



Response to Request for Proposal

eProcurement Solutions and Services

RFP# 202102021- File 3 – Proposed Solutions and/or Services

Submitted by **Infosys Public Services**

August 04, 2021

Infosys[®]
Public Services



Contact Information

For further information and discussions, please contact	
Name	Sandesh Shetty
Designation	Director, Strategic Accounts
Address	800 King Farm Boulevard Suite 505 Rockville MD 20850
Phone	301-354-8600
Fax	301-354-8601
Email	sandesh_shetty@infosys.com

Table of Contents

1. Section III – Proposed Solutions and/or Services (File #3).....	10
1.1 Exhibit 1 (RFP 202102021 - Requirements Traceability Matrix (RTM)).....	15
1.2 Narrative Responses to all “Inline Narratives” as stated in Part II	16
1.2.1 Guiding Principles and Requirements	16
1.2.1.1 Key Solution Functionality Elements.....	16
1.2.1.2 User Experience	23
1.2.1.3 Bidder Best Practices and Roadmap	25
1.2.1.4 Innovations and Value-Added Features/Services	29
1.2.1.5 Customizations/Extensions.....	34
1.2.1.6 Alternative Funding Models	35
1.2.1.7 Contract Transition and Flexibility.....	35
1.2.2 Functional Requirements	36
1.2.2.1 General Functionality.....	36
1.2.2.2 Supplier Portal.....	38
1.2.2.3 Supplier Enablement/Management.....	42
1.2.2.4 Buyer Portal.....	44
1.2.2.5 Need Identification.....	46
1.2.2.6 Request through Pay.....	49
1.2.2.7 Catalog Capability	51
1.2.2.8 Sourcing/Bid Management	54
1.2.2.9 Contract Management	58
1.2.2.10 Vendor Performance	63
1.2.2.11 Purchasing/Data Analytics.....	64
1.2.3 Technical Requirements.....	65
1.2.3.1 Availability	65
1.2.3.2 Accessibility Requirements.....	68
1.2.3.3 Audit Trail and History	68
1.2.3.4 Browsers Supported.....	70
1.2.3.5 User Accounts and Administration.....	71
1.2.3.6 User Authentication	78
1.2.3.7 Federated Identity Management.....	83
1.2.3.8 Data Conversion.....	85
1.2.3.9 Interface and Integration.....	92
1.2.3.10 Office Automation Integration	95
1.2.3.11 Mobile Device Support	96
1.2.3.12 Mobile Applications.....	97
1.2.3.13 Data Ownership and Access	97
1.2.3.14 Data Retention, Archive, and Purge Considerations	98
1.2.3.15 Disaster Recovery Plan	98
1.2.3.16 Solution Environments.....	103
1.2.3.17 Solution Technical Architecture	103
1.2.3.18 Solution Network Architecture	112
1.2.3.19 System Development Methodology	118
1.2.3.20 Service Level Agreement.....	120
1.2.4 Security Requirements.....	120
1.2.4.1 Cloud Security Alliance (CSA) Compliance.....	120
1.2.4.2 Security and Privacy Controls.....	124

1.2.4.3	Security Certifications.....	135
1.2.4.4	Annual Security Plan	143
1.2.4.5	Secure Application and Network Environment.....	147
1.2.4.6	Secure Application and Network Access	156
1.2.4.7	Data Security.....	164
1.2.4.8	Personally Identifiable Information Protection	176
1.2.4.9	Security/Privacy Issue Occurrence	184
1.2.4.10	PII Data Actual/Attempted Access or Disclosure	186
1.2.4.11	Security Breach Reporting.....	189
1.2.5	Implementation Requirements.....	193
1.2.5.1	Project Management	193
1.2.5.2	Project Implementation Methodology.....	228
1.2.5.3	Catalog Support Services	264
1.2.5.4	Data Conversion Services	266
1.2.5.5	Interface/Integration Development Services	270
1.2.5.6	Organizational Change Management (OCM) Services	274
1.2.5.7	Training Services.....	283
1.2.5.8	Help Desk Services	289
1.2.5.9	On-Site System Stabilization Support.....	300
1.2.6	Managed Services Requirements	303
1.2.6.1	Solution Support.....	303
1.2.6.2	Organizational Change Management (OCM) Services	338
1.2.6.3	Training Services.....	340
1.2.6.4	Catalog Support Services.....	340
1.2.6.5	Help Desk Services	341
1.2.6.6	Transition Out Assistance Services	341
1.2.7	Other Available Services.....	346
1.3	Video Demonstrations (Team Infosys Proprietary Content).....	348
1.4	Annexure 1 - Service Level Agreement for SAP Cloud Services	350

Table of Figures

Figure 1.	Our Scope Understanding	10
Figure 2.	Ariba Dashboard Template.....	22
Figure 3.	SAP Ariba Dashboard Example.....	23
Figure 4.	Ariba Mobile Application Sample	25
Figure 5.	Monthly and Quarterly Release Plan	27
Figure 6.	Leading Technologies in the Ariba Roadmap	27
Figure 7.	Benefits.....	28
Figure 8.	Benchmarked Performance Metrics.....	28
Figure 9.	Sample Process Workflow.....	33
Figure 10.	Workstream Conceptual Model	36
Figure 11.	Hybrid Cloud Solution.....	37
Figure 12.	Hybrid Cloud Components.....	38
Figure 13.	Ariba Network Supplier Landing Page	39

Figure 14.	Supplier Dashboard on Mobile	41
Figure 15.	Casual User Landing Page.....	47
Figure 16.	Guided Buying Catalog Tiles	48
Figure 17.	Guided Buying-Configurable Tiles	48
Figure 18.	Solicitation Project Management	56
Figure 19.	Supplier Proposal Review	57
Figure 20.	Ariba Redundant System Architecture.....	67
Figure 21.	Integration A Integration Architecture of States Azure AD IAM and ICAM Solutionrchitecture of State's IDP and ICAM Solution.....	75
Figure 22.	Integration Architecture of States Azure AD IAM and ICAM Solution.....	75
Figure 23.	Proposed Reference Architecture of Saviynt IGA Solution	76
Figure 24.	Azure AD Authentication and Conditional Access Policies	83
Figure 25.	On-Premises AD, AAD Connect and Azure AD Federated SSO Solution.....	84
Figure 26.	Data Migration Approach.....	85
Figure 27.	Ariba data load	87
Figure 28.	Data Conversion landscape.....	88
Figure 29.	Data Testing Mock Dry Runs.....	89
Figure 30.	Oracle Integration Cloud Model	93
Figure 31.	High Level Integration architecture	95
Figure 32.	High Level Solution Architecture.....	104
Figure 33.	Data Exchanges between Cloud and On-Premise ERP system	106
Figure 34.	Ariba High Level Architecture	108
Figure 35.	Portal High Level Architecture	110
Figure 36.	OIC High Level Architecture	111
Figure 37.	OIC and On-Premise Integration	111
Figure 38.	Helpdesk High Level Architecture.....	112
Figure 39.	Logical Network Architecture	114
Figure 40.	Logical Deployment Architecture	115
Figure 41.	SAP Data Centers	116
Figure 42.	Data Center Components.....	116
Figure 43.	Infosys Approach for NIST compliance approach.....	124
Figure 44.	SOC 1 Report.....	137
Figure 45.	SOC 2 Report.....	138
Figure 46.	SAP ISO/IEC 27001 Certificate	139
Figure 47.	SAP Ariba Regulations and Standards Compliance.....	141
Figure 48.	Stages of Security Control Implementation.....	144
Figure 49.	Infosys Overall Security Controls.....	145
Figure 50.	Saviynt Cloud Deployment Model.....	151
Figure 51.	Service Now Deployment Topology.....	153
Figure 52.	Risk Management Process.....	169
Figure 53.	Infosys Approach for IT Security, Privacy, & Data Protection Service.....	171
Figure 54.	Privacy and Data Protection Methodology	171

Figure 55.	Data Privacy Gap and Impact Assessment Services	172
Figure 56.	Lifecycle of Infosys managed PII Data.....	184
Figure 57.	Privacy Breach Notification Process	186
Figure 58.	Critical security incident response plan.....	190
Figure 59.	SAP Ariba Support policy	191
Figure 60.	Infosys IMPACT™ “Lead and Manage Transformation” tools, techniques and accelerators for effective project management.....	193
Figure 61.	Project Management Key Tasks	195
Figure 62.	Illustration of Infosys Strategy.....	197
Figure 63.	Example Accelerators.....	197
Figure 64.	Examples that could materially affect the plan	198
Figure 65.	Mock-up of SaaS Tool.....	199
Figure 66.	Proposed Organization Chart	201
Figure 67.	Stage Gate Process	207
Figure 68.	Phase Gate Criteria Examples	207
Figure 69.	Example Status Report.....	208
Figure 70.	Status reporting Using Business Intelligence.....	209
Figure 71.	Risk and Issue Lifecycle	210
Figure 72.	Example Risk and Issues Dashboard	210
Figure 73.	Onboarding and Offboarding Process	212
Figure 74.	Infosys Quality Management Framework.....	213
Figure 75.	Example of Audit Process	213
Figure 76.	Planned structure for the Infosys PMO team and Staff roles for Participating Entity ...	217
Figure 77.	Sample PMO Accountabilities	218
Figure 78.	Governance Framework.....	227
Figure 79.	Governance Schedule (Illustrative).....	228
Figure 80.	IDEA-Activate™ Methodology	229
Figure 81.	Advantages of Infosys’ Approach for SAP Ariba Transformation	230
Figure 82.	SAP Activate phases.....	231
Figure 83.	Infosys Hybrid Agile Methodology.....	232
Figure 84.	Agile Life Cycle Phases.....	233
Figure 85.	Agile Phases – Activities	238
Figure 86.	Continuous Assessment.....	238
Figure 87.	Agile during Explore Phase	243
Figure 88.	Best Practices and Toolkit for EPS Implementation	244
Figure 89.	Design Confirmation Framework	245
Figure 90.	Day in a Life Illustration during Realize Phase.....	248
Figure 91.	Testing methodology	251
Figure 92.	Progress report.....	255
Figure 93.	Defect Dashboard	256
Figure 94.	Requirement Dashboard	256
Figure 95.	Stages of Deployment	259

Figure 96. Cutover Activities.....	259
Figure 97. Infosys' Change Process.....	262
Figure 98. Risk and Incident Management Framework.....	263
Figure 99. Example Risk and Issues Dashboard	263
Figure 100. Data Migration Approach.....	267
Figure 101. Infosys NIA ETL Tool.....	270
Figure 102. Infosys Integration Execution Methodology	270
Figure 103. Change Experience Approach.....	275
Figure 104. Stakeholder Mapping Chart.....	278
Figure 105. User Persona	278
Figure 106. Measurement and Evaluation Hierarchy.....	281
Figure 107. Training Approach	283
Figure 108. Employee Engagement Strategy	286
Figure 109. Training Plan Summary.....	287
Figure 110. Service Desk Proposed Solution	290
Figure 111. ADSL team Structure and Experience	293
Figure 112. ESM Café Entry.....	295
Figure 113. Service Now ESM Café Model	296
Figure 114. Performance Metrics Dashboard	297
Figure 115. Service Desk Operating Model	298
Figure 116. Onsite System Stabilization Support Plan.....	301
Figure 117. Knowledge Transfer-Preparing from Day-1	302
Figure 118. Transition Plan with Gating process	303
Figure 119. Support as the Final Step	304
Figure 120. Approach to Managing Ongoing Change.....	305
Figure 121. Panaya Enabled UAT Process	307
Figure 122. IT Service Continuity Plan Development Approach	309
Figure 123. ITIL Best Practice Model	311
Figure 124. ServiceNow High Availability Overview.....	313
Figure 125. Infosys Risk Management Process.....	314
Figure 126. Risk Management Process.....	315
Figure 127. Issue Resolution Communication Process.....	318
Figure 128. Meeting Management Plan.....	319
Figure 129. Escalation Process.....	320
Figure 130. Decision Making Process	321
Figure 131. SaaS Security Reference Architecture	326
Figure 132. Infosys Support Monitoring Process	327
Figure 133. Problem Management and Post Incident Resolution Model.....	330
Figure 134. Process Quality Assurance Model.....	331
Figure 128. Internal Users Process Flow.....	335
Figure 129. External Users Process Flow.....	336

Figure 130. System Admin Process Flow	337
Figure 131. Continuous Learning Process.....	339
Figure 132. Transition-Out Methodology	342
Figure 133. Infosys Inflight Project Transfer Approach	342
Figure 134. 4 Step Managed Services Transition Out	343
Figure 135. Infosys Knowledge Transfer Approach	344
Figure 136. Example Transition Out Plan	346

Index of Tables

Table 1. In-Scope Items	11
Table 2. Key Metrics Considered by Infosys.....	12
Table 3. Technology In-Scope.....	13
Table 4. Optional Scope Items	14
Table 5. Proposed Solution for the State of Maine	16
Table 6. Kits and Templates By Phase.....	33
Table 7. Availability Design Considerations.....	66
Table 8. eProcurement – Overall Solution Availability	67
Table 9. SAP Ariba Audit Log.....	68
Table 10. SAP Ariba Audit Log Event Types	69
Table 11. Ariba Administrator Tasks	71
Table 12. SAP Ariba Password Policies	81
Table 13. Reconciliation responsibilities.....	89
Table 14. Data Migration Tools and Accelerators.....	90
Table 15. Data Conversion RACI Matrix.....	91
Table 16. Oracle Integration Cloud Guiding Principles	92
Table 17. Oracle Integration Cloud Integration Patterns.....	94
Table 18. Solution Environments.....	103
Table 19. Key applications and platform.....	105
Table 20. Core Data Exchanges	106
Table 21. Logical Components and Tools	107
Table 22. eProcurement Layers	108
Table 23. ServiceNow Application Layers	112
Table 24. eProcurement Network Features.....	116
Table 25. Data Residency & Data Center Locations.....	118
Table 26. CSA Compliance	120
Table 27. Security Control.....	122
Table 28. Support Activity Model.....	122
Table 29. Technical, Operational and Management Security Controls for Infosys assets and locations	125
Table 30. Vendor Certifications	141
Table 31. System and Associated Transmission Components	156

Table 32.	High Level Security Procedures	159
Table 33.	GDPR Aspects of SAP Ariba	182
Table 34.	Key Tasks across Process areas.....	195
Table 35.	Factors Impacting Scope.....	198
Table 36.	Proposed Organization Role Descriptions – Infosys Team	201
Table 37.	Table 4. Proposed Organization Role Descriptions – State of Maine Team.....	204
Table 38.	Example reports details – Illustrative purposes only	208
Table 39.	Major risk areas for eProcurement Solutions implementation	211
Table 40.	Project Deliverables	214
Table 41.	PMO Roles based relevant PMO Accountabilities	218
Table 42.	Roles and Responsibilities and Skills	219
Table 43.	Scrum Roles and Responsibilities	234
Table 44.	RACI Definition.....	235
Table 45.	RACI Matrix.....	235
Table 46.	Key Activities and Roles	244
Table 47.	Different Types of Design Workshop Accelerators and Enablers.....	245
Table 48.	Key Sub-Tasks for the Build Major Task and Associated Deliverables	249
Table 49.	Testing Entry-Exit criteria	251
Table 50.	Sample Test Strategy Document.....	257
Table 51.	Common Risks from Prior eProcurement Programs by Infosys	264
Table 52.	High Level Approach for Open Transactions	268
Table 53.	Contract Migration rule	268
Table 54.	RACI Matrix.....	268
Table 55.	Integration Methodology Activities and Deliverables	271
Table 56.	Master Data Interfaces	272
Table 57.	Transaction Data Interfaces.....	273
Table 58.	User Group Training and Regenerative Needs.....	284
Table 59.	Service Delivery Parameters	290
Table 60.	Operations Services RACI Matrix	294
Table 61.	eProcurement UAT Entry/Exit Criteria	307
Table 62.	Proposed IT Service Continuity Management (ITSCM) Plan aligned to ITIL Processes 309	
Table 63.	Risk Management and Control	314
Table 64.	Governance and Communication Meeting Cadence Details	322
Table 65.	SAP Ariba Monitoring Service Key Components	328
Table 66.	Areas of Optimization	332
Table 67.	Transition Out Approach.....	343
Table 68.	Transition Out Assistance.....	343
Table 69.	Value Add solution	347

1. Section III – Proposed Solutions and/or Services (File #3)

Our understanding of the scope

Infosys Public Services (Infosys) understands the demands and expectations of the State requirements and how this program will significantly transform the procurement experience for citizens, suppliers, and internal State users. As one of the largest and most diverse professional services firms, Infosys brings knowledge and experience gained from successful implementations of similar programs across the Public Sector domain.

Our response provides not only the vision of a best practice eProcurement solution based on our past public sector transformational experiences, but also a fully implemented and long-term supportable cloud-based solution.

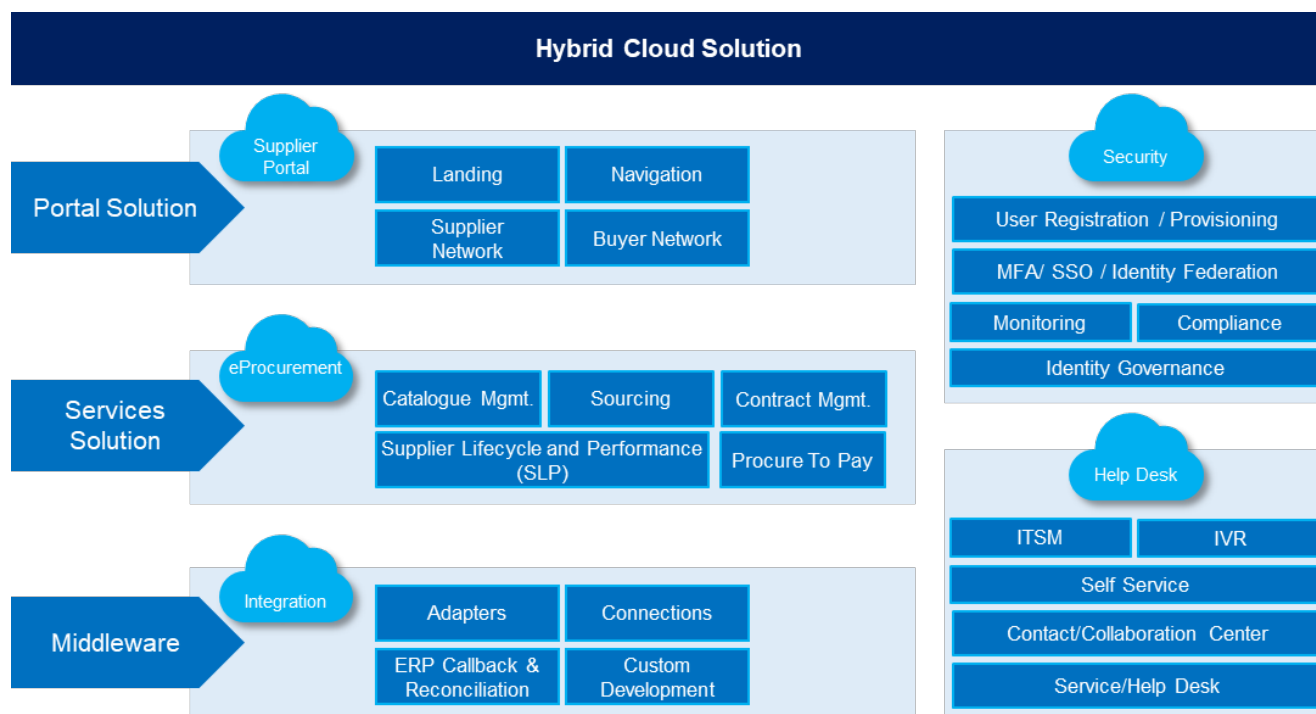


Figure 1. Our Scope Understanding

Our solution leverages the industry leading SAP SaaS technology - SAP Ariba, and offers an end-to-end, scalable, and feature rich e-Procurement solution, a proven Cloud implementation approach, and expertise that best meets the State of Maine's requirements. The solution and business-led proposed approach provides significant value, including a faster implementation and a focus on process improvements and value realization. All of which will contribute to the successful and timely completion of State of Maine's new world-class e-Procurement Solution.

The proposed solution's technical architecture is designed as a highly flexible SaaS and PaaS stack, easily configurable to handle innovative programs or changes in government or partner operations with reduced Total Cost of Ownership (TCO). The operational efficiency and cost-effectiveness are achieved via less paper usage and refined business processes.

In scope

The following table defines the scope coverage of the eProcurement Solutions and Implementation Services across different dimensions:

Table 1. In-Scope Items

Scope Area	Description
Functional Requirement Fulfillment	• Cloud Based electronic procurement solution ○ Supplier Portal ○ Supplier Enablement/Management ○ Vendor Performance ○ Sourcing / Bid Management ○ Contract Management ○ Buyer Portal ○ Request through Pay ▪ Purchase Request Development ▪ Purchase Order Generation & Management ▪ Workflow Management ▪ Payment Card Functionality ▪ Receiving ▪ Invoicing ○ Catalog Management ○ Purchasing Data Analytics
Technical Requirement Fulfillment	• Cloud Based electronic procurement System ○ Integration & Interfaces ○ Near 100% availability ○ Audit trail and history ○ Supported by Leading Browsers ○ User account and administration support ○ Mobile Device Support and Applications ○ Dedicated Solution environments for Dev, Test, Prod, and Training
Security Requirements	• Cloud Security Alliance (CSA) Compliance • Secure Application and Network access • Data security
Implementation Services	• Project Management and Standard implementation services ○ Project Kick Off ○ Requirement Validation ○ Application Design ○ Application Development and Integration Build ○ Unit Testing ○ System Integration Testing ○ User Acceptance Testing ○ Performance Testing ○ Application Deployment ○ Hypercare Support
Data Conversion	• Preparation of Data collection template • Fit Gap Data Analysis • Preparation of Data Mapping

	• Data Migration – Loading transformed data from PeopleSoft, and/or Other Source system ○ Procurement Master data ○ Relevant transactional data • Data Validation
External System integrations	• PeopleSoft ERP • Active Directory for Identity and Authorization Management (as required) • State of Maine Portal for Transparency of Procurement (as required)
Training	• Training Content preparation • Train the Trainer • Training for End Users (up to 25% per RFP requirement) • Supplier training
OCM	• OCM Strategy development • Stakeholder Analysis/Assessment • Readiness Assessments, Organizational and Staff • Impact Assessment • Communications Plan development • Coaching Plan development • Resistance Assessment and Management Plan development
Help Desk Services and Managed Services	• Services (Level 1) to support users and Suppliers in the use of the eProcurement solution • Level 2 and 3 application support services for incidents resolutions and services requests • Catalog Support Services • Supplier onboarding and enablement support • On-going maintenance of the SaaS eProcurement application
Geographic Coverage and Language	• North America • Languages: English

Note: The scope defined in the table above is at high level. Scope for each workstream is further defined and clarified in the respective sections in the proposal.

Based on our experiences in similar projects in public sector and metrics provided by the State, the following are key matrices included in our proposal per respective state category.

Table 2. Key Metrics Considered by Infosys

Considerations	Large State	Medium State	Small State
# of weeks for implementation including hypercare services	50	47	46

Considerations	Large State	Medium State	Small State
Sourcing templates in Ariba	Project: 2-3 templates RFx: 2-3 templates	Project: 1-2 templates RFx: 1/2 templates	Project: 1 template RFx: 1 template
Contract templates in Ariba	Project: 2-3 templates	Project: 1-2 templates	Project: 1 template
# of Custom fields/Extensions in Ariba	15-20 fields	5-15 fields	< 5 fields
Integrations	PeopleSoft ERP Up to 40-50 Integration touch points	PeopleSoft ERP Up to 40-50 Integration touch points	PeopleSoft ERP Up to 40-50 Integration touch points
Data Conversion	~5k contracts Open PO's ~60k supplier	~3k contracts Open PO's ~50k supplier	~2k contracts Open PO ~40k supplier
Help Desk Contacts Per Month for Support	~ 1,250	~ 700	~ 500

Technology in Scope for Core Solution

Table 3. Technology In-Scope

Logical Components	Solution Platform	Solution Component/Version
eProcurement	SAP Ariba (SAAS)	SAP Strategic Sourcing Suite • Ariba Supplier Lifecycle Management • Ariba Sourcing Professional • Ariba Contract Professional SAP Ariba Buying and Invoicing • Ariba Buying • Catalogs • Invoices • Contract compliance
Middleware	Oracle Integration Cloud (PAAS)	Oracle Cloud
Help Desk ITSM Tool	Service Now (PAAS)	ServiceNow Cloud

Optional Scope

As each state/participating entity has a different technology landscape, we offer a few optional solutions to tailor for individual State's situation, and to ensure that our solution is fully compliant with the State's business and operational requirements. These services are summarized in the table below and are further elaborated in subsequent sections of this proposal.

Table 4. Optional Scope Items

Phase	Description
Identity and Access Management	- Infosys plans to integrate SAP Ariba and other platforms with the State of Maine's Identity Access Management solution for ease of operations - However, if the State of Maine IAM solution is not compatible with SAP Ariba and other eProcurement platforms, or the State wishes to leverage a new SaaS based tool, Infosys offers an ICAM (Identity Credential and Access Management) Solution which has native integration with eProcurement and many more advanced security features - Saviynt component of ICAM will be used for Users Lifecycle Management along with identity governance for State of Maine Users (Employees/Contractors):
Transparency Portal	It is important for public sector entities to be transparent about procurements and make award notifications available for public access. As SAP Ariba has the native ability to push award information to external applications such as State's government portal, Infosys has a tailored Transparency Portal readily available that is fully integrated with SAP Ariba to be used by the State if required. This solution is based on Drupal technology built on Acquia PaaS platform.
SAP Fieldglass	- As the eProcurement solution proposed is based on SAP Ariba, it can fulfill the State's service procurement related requirements as specified in the RFP. - Infosys also offers another SaaS solution SAP Fieldglass, which provide enhanced service procurement capabilities. SAP Fieldglass has advanced features that automates the entire process of finding, procuring, and managing external talent. Its Services Procurement module simplifies how external services providers are engaged, ensuring greater compliance, quality, and cost savings. Its Contingent Workforce Management module automates the entire process of procuring and managing flexible labor, from requisition through invoice and payment.

Out of Scope

The following key items are out of scope for Infosys service delivery:

- Changes and customization required in the State's legacy system (such as Peoplesoft ERP) to integrate with the eProcurement system.
- To support data migration, legacy data extraction, transformation, cleansing and enrichment are assumed to be the State of Maine's responsibility. The State of Maine will provide data in upload-able format as per defined by Ariba. Our conversion team will support this process and will also be responsible for the automated translation and loading of cleansed data into the target Ariba platform.
- Major application upgrades or business transformation activities after eProcurement has been deployed. Such upgrades will be managed as separate projects instead of as part of the

managed services.

- Any processes and technologies not covered as part of the scope defined in this proposal.

Key Assumptions

- We assume that each participating entity will be deploying the eProcurement solution independent from other entities. There exist many opportunities to further optimize our proposed solution in case multiple entities decide to collaborate and jointly deploy a transformational program.
- A global delivery model is assumed for the implementation of this eProcurement solution, to ensure accelerated deployment and to control delivery cost.
- The participating entity will provide necessary systems and accesses in a timely manner for team members to work effectively.
- The participating entity will ensure availability of Business and IT SMEs for workshops, meetings, discussions and for review / approval of deliverables.
- The participating entity will ensure appropriate stakeholder communication and management buy-in for the timely reviews and signoffs of all the deliverables.
- The participating entity will deliver corresponding business and technical changes in State's owned legacy or other third-party systems to facilitate eProcurement system integrations and data migrations in accordance to the established project timeline.
- It has been assumed that the participating entity stakeholders will take up to 3 days for review and feedback, and up to 3 days for final review and approval of the deliverables from the date of submission of the same by Infosys team. Up to 2 rounds of reviews are assumed before final approval.
- Since eProcurement is based on a SaaS platform, it will be configured and set up for meeting the State's business and operational requirements. We will adopt the best practice of leveraging out-of-the-box capabilities in SaaS to minimize business operational risks and stay aligned with SaaS vendors' product roadmap. Customization will only be performed within the restriction of SaaS, for items such as adding additional State's specific fields to the sourcing templates.
- Deployment included in Infosys' proposal consists of a single deployment of eProcurement solution to agencies of participating entities. Subsequent rollouts to other relevant agencies and departments are assumed to be State's responsibility.
- The participating entity accepts EULA (end-user-license agreements) from SaaS and relevant software vendors.
- Deficiencies related to SaaS products will need to be addressed by the respective product vendor, with Infosys providing necessary supports.
- Relationship and dependencies with 3rd party vendors/contractors of the State will be managed by the participating entity.

1.1 Exhibit 1 (RFP 202102021 - Requirements Traceability Matrix (RTM))

Infosys has completed the Exhibit 1 - Requirements Traceability Matrix (RTM) and included it as part of our response package. The name of the attachment is – "File 3 Infosys Public Services – Exhibit 1. RFP 202102021 RTM.xlsx"

1.2 Narrative Responses to all “Inline Narratives” as stated in Part II

1.2.1 Guiding Principles and Requirements

1.2.1.1 Key Solution Functionality Elements

As identified in the narrative provided in **Section III – Proposed Solutions and/or Services**, the SAP Ariba solution we propose is a one-product, completely integrated solution. There is no custom integration required among various Ariba modules such as Supplier Management, Sourcing and Contracting, and Procurement Management. It is a seamless, full function, best-in-class industry-leading SaaS procurement solution. In addition to Ariba which covers end-to-end procurement management processes, the solution we propose for the State of Maine includes some additional components that complement Ariba’s capabilities in order to fully meet requirements stated in this RFP. The overall solution includes the following components:

- SAP Ariba Cloud-based eProcurement solution covering Sourcing to Contracts and the Procure to Pay solution footprint.
- Oracle Integration Cloud (OIC) will be used to integrate SAP Ariba/eProcurement solution with the State of Maine’s existing backend ERP system. OIC is a Cloud-based secured tool and will act as the middleware layer for our proposed solution. Alternatively, we can leverage the State’s existing middleware tool and standard as required.
- Identity, Credential and Access Management (ICAM) is a cloud-based security management solution which has an out of the box single-sign-on feature to support Kerberos, LDAP, and other SAML-based identity and authentication processes for our eProcurement solution to enable user id and security integrations with various State’s back-office applications including ERP. This ICAM solution is considered optional in case that the State does not have a SAML-compliant user management system that can integrate directly with the eProcurement system proposed. This ICAM tool has been adopted and deployed as part of eProcurement solution for our public sector clients and has provided significant business values to our clients beyond eProcurement.
- A Cloud-based Transparency Portal acting as a public portal for general/anonymous users> This portal complements SAP Ariba buyer and supplier portal and can be used by public users to easily navigate around the eProcurement system and looking for procurement information such as award details. This Transparency portal has been deployed for our public sector customers and is a good alternative/replacement if the State has limited transparency portal capabilities in its current landscape.

The table below provides an overview of key capabilities and features of respective solution components.

Table 5. Proposed Solution for the State of Maine

Areas	Proposed Solution for State of Maine	Key Features as Required by RFP
SAP Ariba Solution	Our proposed solution will provide seamlessly integrated source to contract to procurement management capabilities including following solution components: • Ariba Network - Connects buyer with product and service suppliers utilizing supplier search functions, RFx management, centralized award	• Portal • Smart routing - Guided Buying • Compliance • Open marketplace environment • Workflow

Areas	Proposed Solution for State of Maine	Key Features as Required by RFP
	management, facilitated collaboration, and configurable dashboards. • Ariba Supplier Lifecycle and Performance Management – This module is a comprehensive solution used for managing supplier performance and minimizing risks. The module allows entities to create performance metrics (scorecards and key performance Indicators (KPIs)) for their suppliers and then allows entities to measure, aggregate, and act upon supplier performance as they deem necessary. This also gives suppliers visibility into their own performance issues and quality problems so that they can proactively address them. • Ariba Sourcing: This module is used to source goods across different categories. This module allows entities to conduct their sourcing event from start to end, including creating and posting a solicitation document, receiving electronic responses, and selecting the winning supplier. The sourcing events include forward and reverse auctions, Request for Information, Request for Proposals, etc. Through the sourcing module, entities are also able to leverage the Ariba Network and Ariba Discovery to increase and promote competition among more suppliers. Once the entity selects a supplier proposal, it can then create a contract in the Ariba. • Ariba Contract: Contract Management encompasses functionality around complete lifecycle management of contracts, including contract creation, renewal, expiration, repository maintenance and integration with requisition and purchasing processes. The contract management process includes what happens to a contract as soon as it has been signed, through reporting on a contract's performance, to the managing and resolving of contract disputes. The process then concludes based on one of the following events: a contract that has reached its expiration date, a contract has exhausted its usefulness or dollar and / or quantity limits, or a contract has expired or is terminated.	• Document management • Integration • Configurable • Reporting, dashboards and data visualization

Areas	Proposed Solution for State of Maine	Key Features as Required by RFP
	• SAP Ariba Buying and Invoicing ○ Is a web-based procurement and Invoicing module. It streamlines the procurement process and drives compliance between vendors, contracts, regulations, buyers, and finance organizations. The entity can use this module to control the procurement process from requesting a purchase through ordering, receiving and finally to invoice reconciliation for payment. This module can also be configured to enforce proper approval flows and ensure compliance. P2P also offers the ability to exchange documents with suppliers connected to the network. Documents may include purchase orders (POs), order confirmations, ship notices, supplier invoices, and payments. This module also allows entities to perform budget checking and advanced contract compliance to ensure a properly executed process for procuring goods and services.	
Oracle Integration Cloud (OIC)	Oracle Integration is a fully managed service that allows you to integrate your applications, gain insight into your business processes, automate processes, and create visual applications. It works on the following guiding principles: • Service Based Integration • Loose Coupling • Separation of Concerns • Minimize Impact • Faster time to Market	• Integration • Configurable
Cloud Based Portal Solution	Our proposed cloud-based Portal will provide the ability to publish award details for external users (Vendors, Suppliers, Other partners) to search and view awards published by State of Maine, as well as many public-facing features such as eProcurement support As some states may decide to leverage existing state portals to support certain portions of the procurement requirements in order to gain unified user experiences, this portal solution proposed to support transparency is	• Supplier/Citizen Portal • Transparency

Areas	Proposed Solution for State of Maine	Key Features as Required by RFP
	considered optional.	
ICAM (Identity, Credential and Access Management)	As a part of our solution, we propose to integrate all the solution components with the ICAM solution to adhere to security and compliance across various regulations including FISMA. We have identified and will implement a handful of single sign-on technologies out of the box to allow fast integration with our portal; however, the technique is customizable to allow for flexibility in the different SSO environments the State of Maine may have. The pre-built integrations that are made available out-of-the-box will include the most common integrations observed and proven within the State of Maine-base. Below is the compendium of Security control and practices Infosys follows for Technical Security, Operational Security, Management Security, and controls. These control families are the basis of securing the application and data. • Technical Controls ○ Access control ○ Audit and accountability ○ Identification and authentication ○ System and communications protection • Operational Security ○ Awareness and training ○ Configuration management ○ Contingency planning ○ Incident response ○ Maintenance ○ Media protection ○ Physical and environmental protection ○ Personnel security ○ System and information integrity • Management Security ○ Security assessment and authorization ○ Planning ○ Risk assessment ○ System and services acquisition As the State of Maine may decide to leverage the existing identity management solution to be integrated with the eProcurement solution, the ICAM solution proposed here is considered optional.	• Secured • Single Sign-On • MFA • Identity Federation • Identity Governance • Monitoring • Compliance
ServiceNow	Although not part of eProcurement core solution,	• Workflow

Areas	Proposed Solution for State of Maine	Key Features as Required by RFP
	ServiceNow enables our eProcurement operational support functions. Our ServiceNow solution leverages an industry leading SaaS-based ITSM tool to effectively manage incidents and service requests from various user groups and provides service level reporting and dashboards to help the State of Maine effectively manage user expectations. Infosys has deployed ServiceNow eProcurement support for many of our clients. We have preconfigured ServiceNow's ESM Café processes based on our eProcurement best practices and our past experiences from various public sector service engagements. Our ServiceNow solution is readily available to the State of Maine for service management functions such as procurement incident and service request management, problem resolutions, solution change and release management, knowledge management, and user self-services.	• Integration • Configurable

Single Point of Entry- The State of Maine envisions a single point of entry to procurement processes via a “Front Door.” Infosys has for many years and continues to provide an integrated source to settlement solution that will provide users with a single place to interact and complete the source to settlement functions using SAP- Ariba Procurement Suite. SAP- Ariba Procurement Suite is a cloud-based solution that supports end-to-end procurement functionalities from source to pay and can be accessed and initiated anywhere through a common URL for Single-Point-of-Entry.

Smart routing – The Ariba Guided Buying solution provides a smart, easy, and intuitive user interface for State of Maine to create any type of procurement request. These requests can include buying, contracting, sourcing, and making services and non-catalog requests, as well as other types of requests. The built-in smart guidance will use the State of Maine’s policies to direct users to the correct path. Our solution provides a fully integrated platform, the State of Maine can achieve zero-touch processing and invoicing, eliminating the more non-value-added work for Accounts Payable (AP), finance, invoice managers, etc.

Compliance – Ease of use and compliance are cornerstones of a successful eProcurement transformation. Compliances in Supplier Management, Sourcing, and Contract are ensured by enforcing business rules via configurable questionnaires and templates. Mandatory fields and data entries such as certificates are enforced to ensure completion and compliance. Compliance for procurement is enforced at each step by leveraging Guided Buying which will deliver State of Maine users with an Amazon-like shopping experience that provides access to catalogs, State of Maine Contracts, and guidance within the context of the procurement process to ensure compliance, while maintaining user satisfaction. Workflows are defined and executed based predefined business rules such as approval thresholds to allow proper governance and controls. Contract Compliance module of Ariba ensures that users can manage contract compliance for requisitions, orders, and invoices. The result, happy users, compliance to State of Maine policies, more spend under management, and reduced maverick spend.

From solution compliance perspective, SAP Ariba supports HTTPS with TLS mutual authentication to secure web applications. SAP Ariba scans files uploaded using the user interface. SAP Ariba ensure

secure file uploads using the anti-virus scanning. Encryption is an important part of SAP Ariba's data protection strategy. SAP Ariba uses both encryption-at-rest and encryption-in-transit to secure your data as it flows into the cloud environment of SAP Ariba solutions. And also provides X.509 certificate-based authentication.

Portal – For Suppliers: SAP Ariba Business Network (SBN) a unified supplier portal that provides a single point of entry (front door) for all supplier facing functions associated with the electronic procurement solution. The SBN will allow suppliers to manage a complete choreography of business collaboration with their customers. The SBN delivers an intuitive user experience that supports self-service supplier registration and maintenance, onboarding, solicitation / bid management, contract lifecycle management, and e-procurement and payables (PO, OC, ASN, Inv. etc.).

For Buyers: SAP Ariba Buying and Invoicing (B&I) solution will be the buyer portal for the State of Maine which will act as a personalized single point of entry ('front door') to initiate the full life cycle of procurement activities for State of Maine's users. Our B&I solution will help the State of Maine's front-end procurement process operate with maximum efficiency while integrating seamlessly with State of Maine's enterprise resource planning (ERP) system for requisitioning, purchase orders, receiving, invoicing and payment processing. This unique software-as-a-service (SaaS) solution also provides a fast, guided buying experience, streamlined catalog maintenance, and a configurable interface which all help in delivering a quick ROI.

In addition to the SAP Ariba native portal, Infosys also offers an optional Transparency Portal capability using Drupal technology. It is a Cloud-based transparency portal that complements SAP Ariba for the public announcements, bids and proposals, which can be accessed by the general/public users. This Transparency Portal integrates seamlessly with the SAP Ariba native portal and gives users a coherent web experience.

Open Marketplace Environment – Spot Buy is a capability within the SAP Ariba Cloud procurement applications which delivers a business-to-business (B2B) marketplace that provides a “catalog of catalogs” like shopping experience and will help State of Maine to find and buy non-sourced goods, those goods that have not been previously put under contract and likely never will be. With Spot Buy, the State of Maine can purchase goods within the procurement application without the requirement to source the supplier, with competitive price and delivery options.

Integration – SAP Ariba suite of applications do in fact come with native out of the box integrations between each solution without need for customer development. For instance, Supplier Master data defined in Ariba Supplier Lifecycle Management is shared and used across the whole Ariba platform including sourcing, contract, and procurement management, and Contracts defined in Ariba Contract Management are utilized throughout the procurement management cycle to ensure proper compliance and full end-to-end traceability. SAP Ariba is one of a few, if not the only one, SaaS procurement solutions that has achieved such high level of native integrations among its application modules.

In addition to native build-in integrations, SAP Ariba supports standard and secure methods of integration that support real-time and/or batch integration. The standard integration options available are:

- HTTPS using a CSV interface (batch integration, and depending on the data volume this can be scheduled to run frequently to achieve near real-time integration)
- SOAP Web services that use an XML payload (real-time integration suitable for transactional data)
- REST APIs (supports both synchronous & asynchronous calls)

Workflow – SAP Ariba modules provide easy to use workflow designs that do not need customization by experts. It provides pre-configured workflows based on best practices that the State of Maine can use right away. With the use of drag-drop functionalities, the State of Maine can easily modify rules and with the use of workflow builder, users can easily build, test, and deploy workflows.

Document Management – Ariba Contract Authoring provides the feature to manage the documents in the Contracts module. Ariba Buying & Invoicing module provides feature to create, store and manage all the transactional documents. SAP Ariba provides a My Document tab where users can access all the created transactions and all the transactions for approval will be in To Do list.

Reporting, dashboards, and data visualization – Standard dashboard templates can be rolled out to all the State of Maine's users belonging to a specific region. SAP Ariba provides standard tiles for accessing different transactions or documents on which user has worked. The information includes status, document id, creation date etc. and is available as a hyperlink which allows user to click and access the transactions from user's homepage. It also provides graphical/numerical representation of different transactions that requires user actions on dashboard as shown in the graphic below:

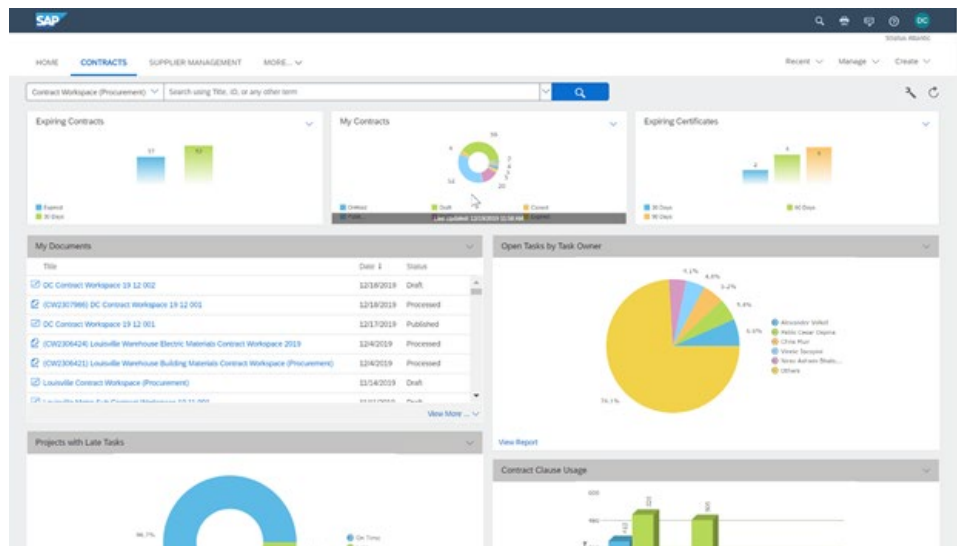


Figure 2. Ariba Dashboard Template

Note: Each Power Users landing page will be a configurable and personalized dashboard that contains relevant reports, to-do lists, actions to support the users' job functions.

Configurable – SAP Ariba solution is highly configurable and can be configured according to the State of Maine needs.

Transparency – The State of Maine can track all actions on any approvable document internally by clicking on the History tab of SAP Ariba application, which captures a complete Audit trail and gives users and key stakeholders full transparency of relevant transactions.

From public procurement transparency perspective, All RFx released by the State, except for those sole-sourced or limited-procurements, can be made available to SAP Ariba Network/Discovery for public user accesses. By default, outcome of the RFx procurement is shared with participating vendors. Such data can also be exported from SAP Ariba via APIs and made available to general public via State's existing portal. Infosys also offers an optional Transparency Portal capability using Drupal technology. It publishes the public announcements, RFP's & awarded supplier information to the general/public users.

1.2.1.2 User Experience

For a procurement transformation to be successful, user adoption is imperative. User adoption is optimized when people can seamlessly process workflows, with the least number of obstacles. Our solution, SAP Ariba, meets today's demanding user experience standards, including dashboard personalization, intuitive navigation, wizard driven capabilities, custom forms, and supplier enablement.

Dashboard Personalization

SAP Ariba has configurable dashboards to meet each of the different types of the State of Maine's user's needs. The Dashboard is a tabbed screen on which the State of Maine users can organize and access key tasks, actions and information from each application that is available to the company. Rather than switching between applications to work with items such as purchasing requests, solicitations, contracts, or analytical reports, users can simply add the items to the dashboard and then monitor and access the items from one convenient location. As shown in the graphic below, users can create multiple dashboards that cover different strategic areas, such as one dashboard for analyses, one for project management, one for supplier management, etc.

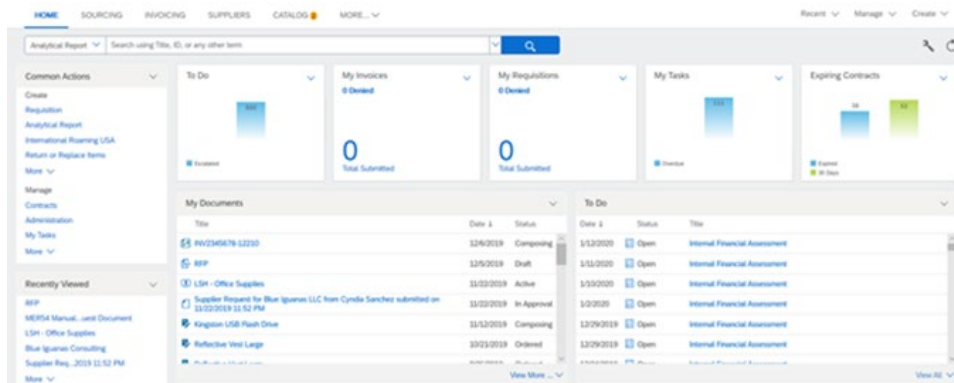


Figure 3. SAP Ariba Dashboard Example

Intuitive Navigation

The solution follows the latest principles of design to deliver a fast and ergonomic user experience minimizing end user training. In-context help and intuitive process flows help users achieve tasks quickly. The interface has been designed with special attention to:

- Minimizing clicks and number of steps
- Seamless transition from mobile app to desktop with "follow-me" process from one another
- Community help
- Visual workflows, reminders, and notifications
- Bulk actions over many items (i.e., bulk receive purchase orders)
- Integrations to facilitate multiple catalog search (items in the material master, inventoried items, MRO Supplies, and contracted supplier catalogs), cost accounting and more.

Wizard-driven Capabilities

With SAP Ariba "Guided Buying" capabilities, SAP Ariba provides a single system for both occasional and frequent buyers to buy goods and services. SAP Ariba differentiates between multiple buying channels to cover the right buying processes and will guide the State of Maine user to the appropriate path. The Guided Buying solution provides a smart, easy, and intuitive user interface for State of Maine users to create any type of procurement request. These requests can include buying, contracting, sourcing, and making services and non-catalog requests, as well as other types of requests.

User work management in portal

SAP Ariba supports user work assignment and reassignment by leveraging pre-configured business rules in respective forms, templates, and workflows. For instance, buyers or buyer groups for procurement requests can be automatically assigned based on product category selected, and approvers for contracts can be automatically assigned based on authorization matrix established. All these capabilities are accessed and realized via a common SAP buyer portal when respective business transactions are created. In addition, SAP Ariba provides an Approvable Role Assignments feature that will allow the re-assignment of work to another user.

SAP Ariba supports work-order based requisitions. Users can import work-order based requisitions using either the file channel method or web services and then process those requisitions in a combined setup involving the buying solution and procurement operations desk.

Work-order based requisitions imported from ERP can include goods or service items. These requisitions enter the approval flow in the buying solution and automatically flow to procurement help desk for approval by procurement help desk agents. This process provides the advantage of leveraging the expertise of procurement operations desk agents to validate the details of line items on requisitions.

Functionality optimized for mobile access and use

SAP Ariba also provides mobile procurement tools to review and approve requisitions anytime, anywhere. We understand when your demanding schedule has you tied up in meetings or traveling. Ariba's mobile app helps you to make even more timely and effective decisions when using our procurement solutions by keeping you connected to your business, all of the time. Whether you use SAP Ariba Buying or SAP Ariba Buying and Invoicing, this new mobile app makes it simple to search catalogs, order items, manage requisitions, monitor progress, send approvals, and conduct other procurement processes in any location and at any time. Consistent 24/7 visibility into pending tasks and the ability to respond rapidly allow you to keep critical workflows processing and boost procurement productivity. The friendly, intuitive interface helps you engage more users, driving up compliance and improving procurement.

Mobile app User Interface

The user-friendly interface provides mobile access to SAP Ariba procurement, sourcing, and contracting solutions so that users can be effective and productive anytime, anywhere. The advanced mobile procurement tools make it easy to:

- Track and act on sourcing and contract tasks
- Get notified when a sourcing or contracting task is assigned, or when a task initiated is acted upon
- Shop and order from company's catalog
- Track and approve requisitions

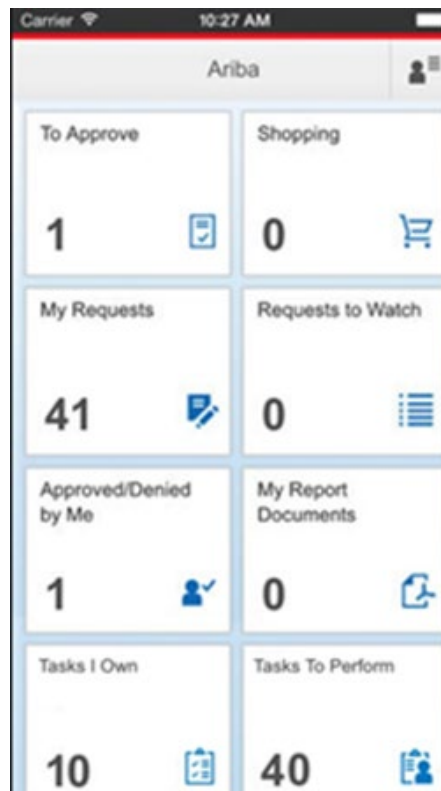


Figure 4. Ariba Mobile Application Sample

Workload Management Functionality

Workload management functionality is supported in SAP Ariba. SAP Ariba provides an Approvable Role Assignments feature that will allow the re-assignment of work to another user. This feature will help in changing the ownership of documents such as Requisition, Receipt, Invoice, Contract Request, Advance Payments, Service Sheets and Charge (purchasing card charge reconciliation (PCCR) documents).

Role-based functionality for drafting, review and approval, evaluator, and other processes

Access to SAP Ariba for State of Maine users is based upon a user profile that is created in the solution. The solution maintains a unique user profile for each user. Profiles can be created directly within the application or via integration from an external HR management solution. Profile sections can be maintained by an administrator using the User Manager Workspace. When users log into the solution, they are provided access to only the functionality that is specified by the groups to which they belong. A super user will be granted broader access to the solution by assigning multiple groups that allow the user to access functionality across the solution. A super-user may also be assigned groups that provide administration capabilities across the solution, or for specific functional areas (sourcing, contracting, etc.). The approval flow is designed and configured in Approval Processes. In summary, with the combination of security profile and workflows, SAP Ariba has native capability to support role-based functionality for drafting, review and approval, evaluator, and other processes

1.2.1.3 Bidder Best Practices and Roadmap

Incorporating New Features/Tools

As a subscriber to a cloud solution, the State of Maine will consume functional enhancements and fixes without a local implementation effort. Like on-premise software products, functional enhancements are provided on a regular basis and called releases. The key difference is that these solutions are implemented centrally.

Ensuring Use of Latest Technologies

SAP Ariba has continued to transform these offerings and more with input from its customer base to provide regular updates to all customers so they can access the latest innovations. Production quality metrics are tracked continuously to determine areas for improvement. All releases are fully documented, covering requirements, design, and test approaches for all features.

Ensuring Timely Updates

Quarterly Releases – Releases are delivered every quarter in February, May, August, and November each year. Individual products may be released on any or all of the quarterly dates. You should expect to receive advance communication of features and should allow time to prepare for impactful changes to your systems.

Monthly Feature Deliveries – Major products may have an optional, no-impact release on harmonized monthly feature delivery weekends. As with the quarterly releases, each product has the option to release during any or all of these windows. You should not need to prepare for or act on the monthly feature deliveries. Changes delivered in a feature delivery should be virtually invisible to the end users. Many of our largest cloud products follow a harmonized release calendar.

SAP Road Maps support the journey to SAP's future product portfolio and the Intelligent Enterprise.

SAP Ariba offers the SAP® Ariba® Best Practices Center service that provides business commerce professionals with access to our process expertise to help ensure greater adoption and sustainable results from your SAP Ariba solutions. SAP Ariba Best Practices Center team members leverage their knowledge of best practices within each solution area to provide strategic advice, allowing you to make the most effective use of all features of your SAP Ariba solutions:

- Best Practice Center Benefits:
- Best Practices Center service provides the following benefits
- Flexible, as-needed support tailored to your specific needs and projects
- Single, named point of contact who understands your unique situation
- Access to a world-leading commerce process and solution expertise and experience
- Proven processes and best practices for all SAP Ariba solutions
- Faster ROI from software initiatives

The primary focus of SAP Ariba Best Practices Center is the use of methodologies that advance the implementation and adoption of SAP Ariba solutions, while enabling you to build internal skills and capabilities. With SAP Ariba Best Practices Center, you have access to solutions experts who have business backgrounds and can offer strategic guidance. Our remote support model is designed to be flexible so you can get the support you need when you need it. Tap into the expertise of our experienced consultants to help you to get the most out of SAP Ariba solutions.

SAP Ariba is committed to supporting customers with innovative features that deliver compliance, efficiency, and process and price improvement. This is done via quarterly release cycles. New features and functions are developed based upon industry trends, best practices, and customer feedback. Each quarterly release is delivered in the second month of each quarter (Feb, May, August, and November). Monthly service packs occur to address defects in the existing features/functions. Releases are scheduled outside of business hours, typically on weekends. Each release is communicated to our customer base on a predictable quarterly cadence. This is done three weeks in advance for each quarterly feature release. Release materials include a high-level overview of each feature, as well as a deeper dive on each feature. This allows SAP Ariba customers to review the features and research those of which are of interest. The State of Maine may designate a point of

contacts (DSCs) who will receive release related information. The DSC will also receive information related to planned and unplanned downtime.



Figure 5. Monthly and Quarterly Release Plan

Ariba Product Roadmap

Emerging technology, changing workforce demographics, and the growing power of business network ecosystems will redefine how goods and services are sourced, purchased, and tracked across every spend category. Procurement roles and organizational structures will change as a result.

Without a doubt, digital technologies will revolutionize how goods and services are procured, tracked, delivered, and managed. Advancements in real-time connectivity, 3D printing, drones, and other innovations have exciting potential to disrupt existing supply chains. Four technologies, however, have the greatest potential impact on procurement. Together, these technologies (see below fig.) will extend core procurement solutions across secure cloud architectures to drive business innovation and customer value while improving productivity.

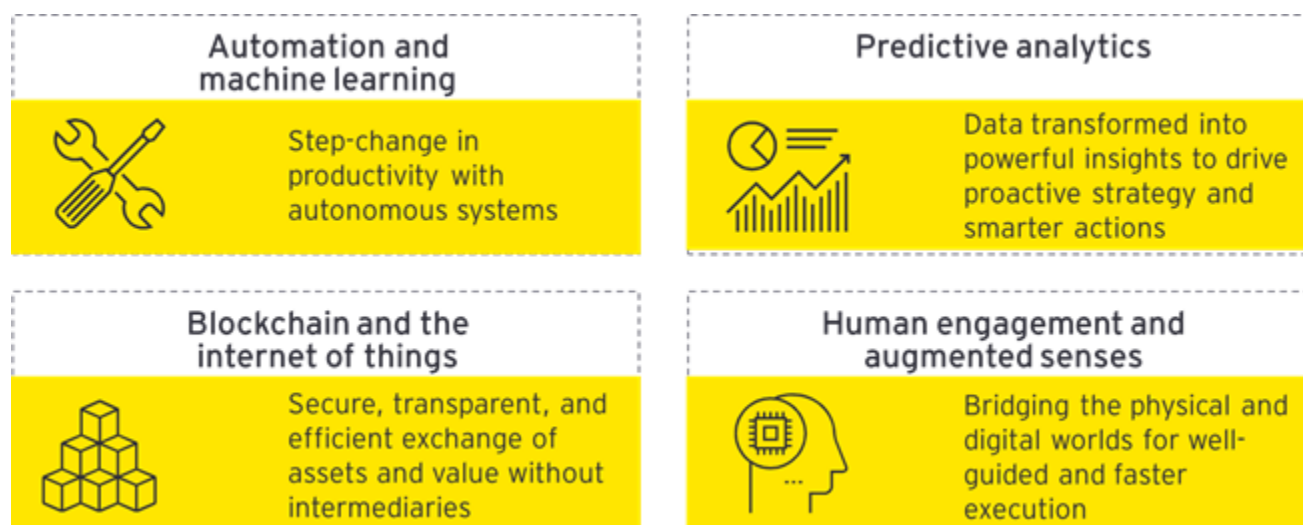


Figure 6. Leading Technologies in the Ariba Roadmap

Best practices for procurement transformation program and Continuous improvements: Infosys follows below mentioned guiding principles to ensure that best practices are delivered as a part of the transformation journey.

- **Simple & Modern UI:** Simple, easy to understand and navigate the UI is an important step that Infosys ensure which Simplification of UI is the key consideration that Infosys
- **Increase spend under management:** One of the key aim of procurement programs is to get all the spend under one tracking system. This helps in planning costs, identifying risks, Automation in P2O Process
- **Future ready solution:** With digital advancement and Industry 4.0, the procurement landscape keeps evolving rapidly. Our solution guidelines ensure that the end system is scalable, robust and future ready.
- **Increase Supplier Relationship Management:** One of the key drivers for any eProcurement system is the ability it provides the supplier to provide real time information. The prerequisite

for this is enabling suppliers to easily adopt to the procurement platform. The Infosys team will setup a strategy for supplier enablement such that buyers as well as

- Continuous improvement: As a part of implementation program, the Infosys team ensure that philosophy of continuous improvement is embedded into the program DNA.

Cost Reduction: Success of any transformation program depends upon the metrics. Most of the KPIs for Procurement transformation programs like the one at the State of Maine are achieved over a period of time. There are some immediate benefits and some benefits that are incremental in nature brought in by virtue of continuous improvements. For the State of Maine implementation, we envision the following benefits:

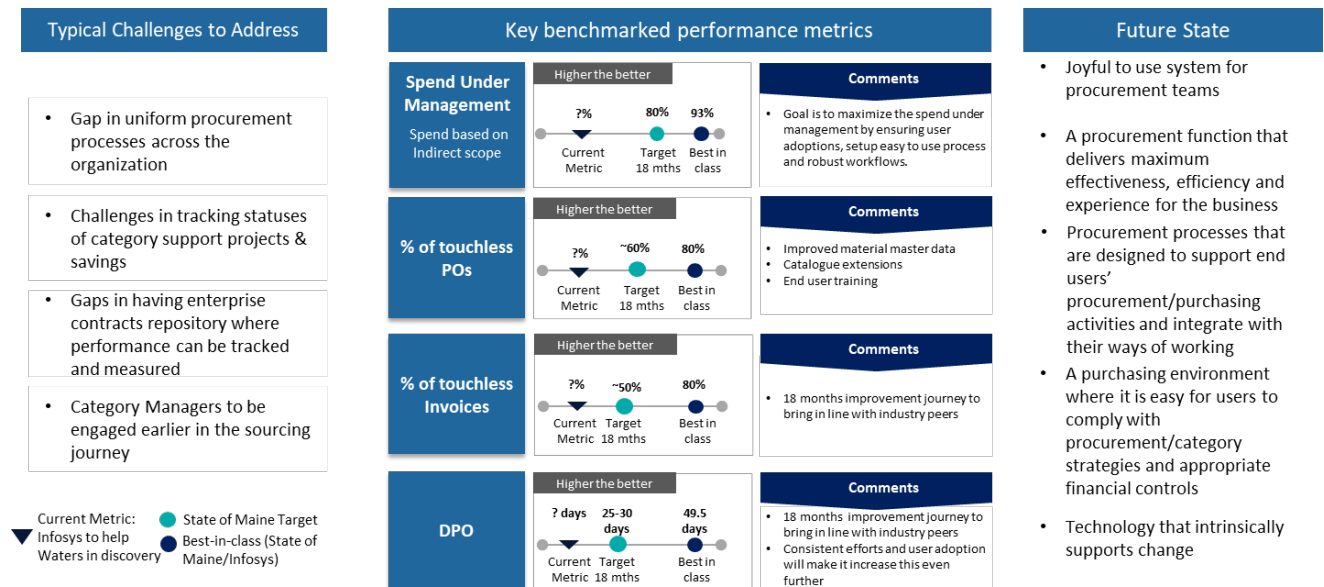


Figure 7. Benefits

Infosys will help in benchmarking current levels and setup target levels for the project duration. Our experience of delivering outcomes to S2P clients in life sciences, and across other industries provides proven benchmarked performance metrics and means to achieve the targets.

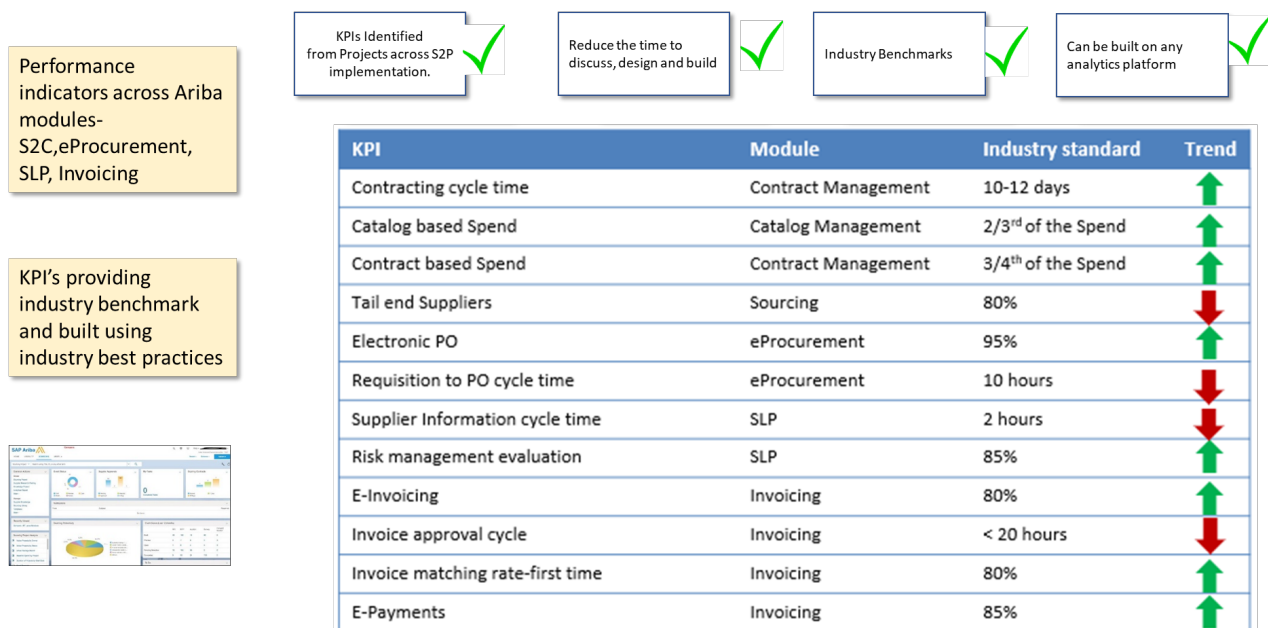


Figure 8. Benchmarked Performance Metrics

Extensible/API Strategy

In addition to releasing new features and functions directly within the proposed applications, we are committed to delivering an extensible solution. The intent is to allow Team Infosys and the State of Maine to leverage SAP Ariba's solution and extend it as required to meet the unique business requirements the State of Maine may have. One example of this in the proposed solution is the Public Posting/Transparency Portal. The portal will expose Solicitations, Contracts, and Analytics to the public. The portal will surface data and documents created and stored within the SAP Ariba solutions. Another example of leveraging the extensible nature of the solution is enabling end users to visualize budget consumption (graphically) at the time of purchase requisition creation. This is a critical requirement for the public sector, and the standard solution supports the budget check. This graphical view shows the leveraging of extensible technologies.

Transparency Portal (Drupal-based /Public Posting Portal)

In addition to the SAP Ariba native portal, Infosys also offers an optional Transparency Portal capability using Drupal technology. It is a Cloud-based transparency portal that complements SAP Ariba for the public announcements, bids and proposals, which can be accessed by the general/public users. It is a responsive web application that gives rich experience in procurement activities for general public, and it scales effortlessly between different screen resolutions on laptops and mobiles, providing the required functionality and meet the security, performance, availability, and accessibility (WCAG Level AA) requirements. This Transparency Portal integrates seamlessly with the SAP Ariba native portal and gives users a coherent web experience.

1.2.1.4 *Innovations and Value-Added Features/Services*

Innovations – Value added Services

In line with the State of Maine's request, the RFP response team spent time studying the State of Maine's policies and regulations to bring forward the best combination of solutions and innovations to help the State of Maine become Best-in-Class. Infosys also understands that sometimes budget is a constraint, so these solutions can be deployed in stages without losing any value.

High performing organizations have found the perfect balance between three key levers: Process, People and Systems. With the ever-changing environment, that balance can be challenging to find and maintain, but with the correct tools it is possible.

Below, we present the optional tools that we believe would bring enhanced value to the State of Maine. During the implementation phase, we will evaluate the fitment of the tools at the State of Maine. Please note that some of these tools and services are not included in the core scope of the eProcurement project and are considered optional where additional fees will be required.

1. SAP Fieldglass

SAP Fieldglass is a cloud-based, open vendor management system (VMS) that helps organizations find, engage, and manage their external workforce and services procurement resources – from temporary staff to statement of work-based consultants to freelance workers, gig workers, contractors and more. This is the only solution in the industry that offers a direct candidate website within our core application enabling contingent workers to apply directly for temporary roles.

Potential Opportunities

- Hiring contingent workers to perform services via SOW.
- Leveraging the same resources across the State of Maine agencies.
- Hiring the right resource for the job.

- Assessment of the candidate credentials for the hired position.
- Saving opportunities for hiring contingent workforce or procurement.

Benefits

- SAP Fieldglass External Talent Management automates the entire process of procuring and managing flexible labor, from requisition all the way through invoice and payment.
- SAP Fieldglass Services Procurement can handle the management of a variety of Statement of Work (SOW) engagements including projects, offshore/offsite, independent contractors, managed programs, business services and Business Process Outsourcing (BPO) models.

2. SAP Ariba Spend Analysis

Ariba Spend Analysis is the only solution that combines internal spend classification, supplier information and market dynamics to give organizations the strategic insights needed to identify and prioritize sourcing opportunities.

Potential Opportunities

- Spend data is tied up across so many systems that organizations do not know how much they are spending with which suppliers or on what products.
- Organizations fail to take advantage of supply market trends which results in high-cost sourcing.

Benefits

- Ariba will capture all the spend data from all systems and ERPs across the company then cleanse and aggregate it using the world's largest classification knowledge base, so that organizations get accurate spend data.
- Select the right suppliers negotiate more effectively and make better business decisions.

3. ICAM - Identity, Credential and Access Management

The comprehensive and proven solution for centralized user identity, credential and access management leveraging industry-leading cloud-based identity solutions that are FedRAMP compliant. Key to the ICAM solution is Saviynt's Identity Governance and Administration product. It combines traditional identity management features with advanced usage analytics, data or infrastructure access governance, behavior analytics, real-time threat detection and compliance controls to secure an organization's critical assets. Azure Active Directory (Azure AD) is an identity and access management-as-a-service (IDaaS) solution from Microsoft that combines Single Sign-on to cloud and on-premise applications with advanced protection.

The ICAM solution can manage the full identify lifecycle and

- can stand on its own or easily integrate with a state's user identity directories and identity management solution
- enables secure authentication and authorization through multiple channels
- ensures compliance to security standards around single sign-on, password complexities, user provisioning, assurance levels, etc.
- provides policy-based controls, inbuilt identity monitoring and reporting.
- is supported by a dedicated helpdesk

Benefits

- Application Access Governance
- Enterprise Role Engineering
- Enterprise Privilege Access Governance

- Identity Access Administration & Governance
- Complements Saviynt's access governance capabilities with granular permission management and risk-based governance
- Supports native integration with SAP Ariba, ServiceNow, Office365, etc.
- Provides customizable conditional access controls and built in Multi-Factor Authentication
- Self Service capabilities around password resets, application access requests, etc.
- Robust AI based analytics and monitoring

4. Transparency Portal / Drupal CMS based Portal (Electronic Procurement System)

In addition to the SAP Ariba native portal, Infosys also offers an optional Transparency Portal capability using Drupal technology. It is a Cloud-based transparency portal that complements SAP Ariba for the public announcements, bids and proposals, which can be accessed by the general/public users.

Infosys has recently, successfully developed and launched a custom Electronic Procurement System, for another public sector client. It is a state of the art solution to enhance the user experience and modernize the public procurement practices, making them simpler and less burdensome, administratively. The portal is developed using the Drupal Digital Experience platform. It is a responsive web application that scales effortlessly between different screen resolutions on laptops and mobiles, providing the required functionality and meet the security, performance, availability, and Accessibility (WCAG Level AA) requirements.

Potential Opportunities

- Public view of the solicitation and contract information through a portal.
- Search capabilities of the procurement data by the public.
- Notifications/Alerts to be shared to the users
- Secure login to the portal where business users should create and manage the tenders and awarding of the tenders.

Benefits

- It is integrated with core procurement systems via middleware using web services and offers a public view for tenders, awards and contract history data. It has integrated Solar search module for enabling the search capability for the users.
- It provides the business users with a secure login and the capability to create and manage tenders and awards per a custom workflow and approval process.
- It also, has an extension module to publicly expose procurement data to approved agencies via JSON APIs, in compliance with the Open Contract Data Standard (OCDS).

5. Celonis Process Mining

Celonis Process Mining makes business processes 100% transparent to uncover inefficiencies, bottlenecks, and compliance violations. These insights are used to increase the efficiency and quality of processes dramatically. Infosys has developed strong competency across the procurement value chain to deliver value to our customers using Celonis.

Potential Opportunities

- High Volume of Price Change from out-of-date master data -
- Manual Errors in 3 Way Match
- Long Tail Spend

- Maverick Buying
- Incorrect plant delivery for dangerous or regulated substances.
- Unfavorable supplier contracts.

Benefits

- Increase in Purchasing Productivity
- Optimizing purchasing spend
- Reduce risk & Compliance.

6. Power Approver

Power Approver mobile application is one stop shop for all approval requests. It provides the ease of access & comfort to users to approve various approvable documents at one place. App sends approval notifications to the approvers. This makes it very convenient and easy for managers to approve the requests on the go. Infosys team developed a customized mobile app “Power Approver” which would be the One Stop Shop for all approval requests. Managers (Approvers) need to install single app, which would integrate with multiple applications (e.g., Ariba) at the back end.

Potential Opportunities

- Multiple enterprise applications sending approval requests to managers
- Managers (Approvers) need to login to enterprise network to see the approval requests and approve them
- Some applications have their own mobile apps; however, this means managers need to install various. Impact is delays in getting requests approved in time, delaying ordering process, which could impact operations.

Benefits

- The Power Approver app is expected to provide quicker approval cycles for various approval requests.
- One stop shop for all approvals. Approve on the go. Integrated with enterprise SSO
- Faster approvals mean more efficiency.

7. Other Tool and Accelerators:

a. Source to Pay Best Practices – A Complete ready set for all Source to Pay process (Accelerator that will be part of the project as a value add)

- eProcurement best practices end-to-end process flow diagrams built based on our experience in Source to Pay for over 17 Years
- Provides a blueprint for Process and functional design based on best practices
- Team can accelerate understanding with process design workshops
- There are ready made 50+ processes available and will be used as reference process to start the discussion. An example below:

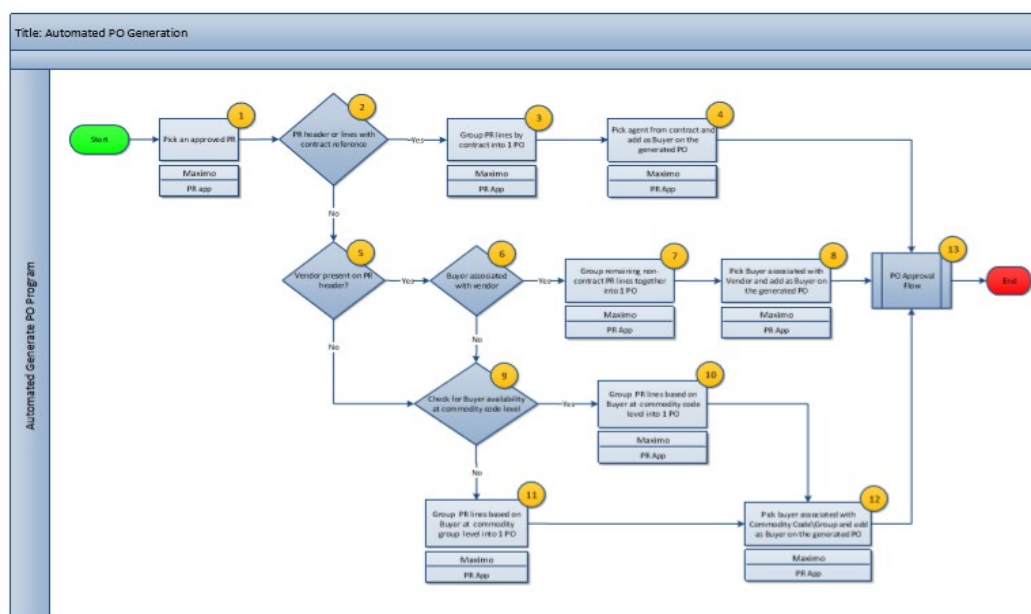


Figure 9. Sample Process Workflow

a) Kits and Deliverable Templates by Phase: Below are the kits/ templates that will help in accelerating the respective phases:

Table 6. Kits and Templates By Phase

SI	Phase	Kit / Deliverable Template
1	Mobilization and Planning	- Kick Off Deck - Detailed Project Plan - Risk Mitigation Plan
2	Process Workshop	- Business Process Master List (BPML) Fit-gap template: capture every L1- L5 process level activities details in Source to Pay functions. - Data Conversion Strategy - Source to pay Standard process flows and user stories for each functionality - Explore Phase Kick-Off Presentation Materials
3	Design	- Change Impact Action Plan - Functional Specification Documents - Configuration Workbook - Key Decision Documents
4	Build	NFR Catalog deliverable-integration channel (API/CSV/web Service) (OIC,SAPArriba)
5	Testing kit	- Testing strategy - End to end SAP Arriba test cases
6	Training Kit	- Train the trainer Plan - SAP Arriba training material

7	Cutover Kit	• Cutover Plan • Cutover activities Checklist
8	Knowledge Transition (KT)	• KT Topics Planning • Satisfactory KT Sign off checklist
9	Hypercare	• Hypercare Overview presentation • Hypercare issue tracker template
10	Data Migration	• Open PO migration template • Contract migration template • Migration reconciliation [load validation report and reconciliation script]

1.2.1.5 Customizations/Extensions

Customizations/Extensions:

- Most of the requirements provided by the State in RTM can be addressed by out-of-the-box Ariba functionality. A few requirements would require customization/extensions for achieving the State of Maine's desired functionality. The deviations are addressed in the RTM.
- Since the primary platform of the proposed eProcurement solution is based on SAP's Ariba SaaS application, Customizations/Extensions will be performed within the SaaS framework to allow fit-to-standard and minimize operational costs and risks.
- Examples of Customizations/Extensions include customized fields for respective participating entities to meet specific business requirements, and custom reports and dashboards for users and key stakeholders.
- Interfaces can be built to facilitate data exchanges between eProcurement system and external applications. Although SAP Ariba has provided a variety of APIs required by typical procurement processes which can satisfy most if not all clients' need, the capability of these interfaces are bound by the SaaS platform and product. For the proposed eProcurement solution, Oracle Cloud Integration platform will be used.
- For those Customizations/Extensions that require SaaS product vendor's involvement, service requests/enhancement requests can be submitted. Acceptance of such requests and timing of solution development will be determined by the respective product vendor.
- Customizations/extensions will only enhance the Infosys suggested procurement processes and would not create any performance issues or processing delays. It is ensured that optimal solutions are suggested as customizations/extensions to enhance the procurement process.
- Customizations/extensions will not invalidate, negate, or minimize any warranty or maintenance requirement as agreed to between the participating entity and their current third-party providers as the extensions are supported within SAP Ariba.
- We ensure the customizations/extensions will reduce the bottlenecks present in the current processes while adjusting the SaaS solution as per the State's requirement. Customizations/extensions timelines and complexity would be shared with the State of Maine and implementation decisions would be made by the State of Maine.
- The change management impacts due to customizations/extensions would be shared with the State of Maine.
- All customizations/extensions which are identified in the RTM would be implemented during

the implementation period and if any customizations are extended beyond the implementation period, then those will be documented in the product roadmap.

1.2.1.6 *Alternative Funding Models*

Infosys is flexible on considering an alternative funding model based on the State's funding requirements. One potential option is to levy per usage fees for procurement related transactions such as RFX fees or invoice processing fees, etc. Such fees can be levies for suppliers as well as for buying agencies. Such a model can provide benefits to participating entities by reducing the upfront capital investment required, converting capital expenses to operational expenses, and improving cash flows during operations. As the business and/or technology solution involved for such funding model may become quite complex based on individual participant State's situation, this can be discussed in more detail with the respective participating entity at the time of order negotiation. Product vendors for eProcurement such as SAP also need to be engaged in order to support such a model. Infosys has supported similar alternative funding models for other client services but has not used this kind of model specifically for the eProcurement solution in the past.

1.2.1.7 *Contract Transition and Flexibility*

Infosys Public Services will work with the State of Maine or the participating entity to manage the transition of the MSA to incorporate the changes present in the new MSA. This assumes that the previous MSA is with the State of Maine/Participating Entity and Infosys Public Services as an entity.

We have 2 potential approaches that we could follow:

1. The Current existing MSA With the State of Maine/Participating Entity will be treated as the master.

In this case the MSA with the State of Maine/Participating Entity will not be modified. Instead the MSA will be amended to cover additional clauses in areas such as:

- Business needs
- Financial needs
- Regulatory /SLA needs

This will be created with clear language that will ensure the precedence of execution.

2. The new MSA (Signed as part of this proposal) will be the Master MSA with the State of Maine/Participating Entity.

In this case there are two ways to approach this:

- a. We can have a sub-clause called the "Legacy agreement" in this MSA and capture all of the clauses that the State of Maine deems necessary that are not covered as part of this MSA. If there are additional clauses that need to be changed, then both the parties will mutually consult and agree upon the clauses.
- b. We can create an addendum and capture the Legacy clauses that need to flow down to this contract. This will have to be mutually agreed upon to ensure fairness with respect to the priority and coverage.

1.2.2 Functional Requirements

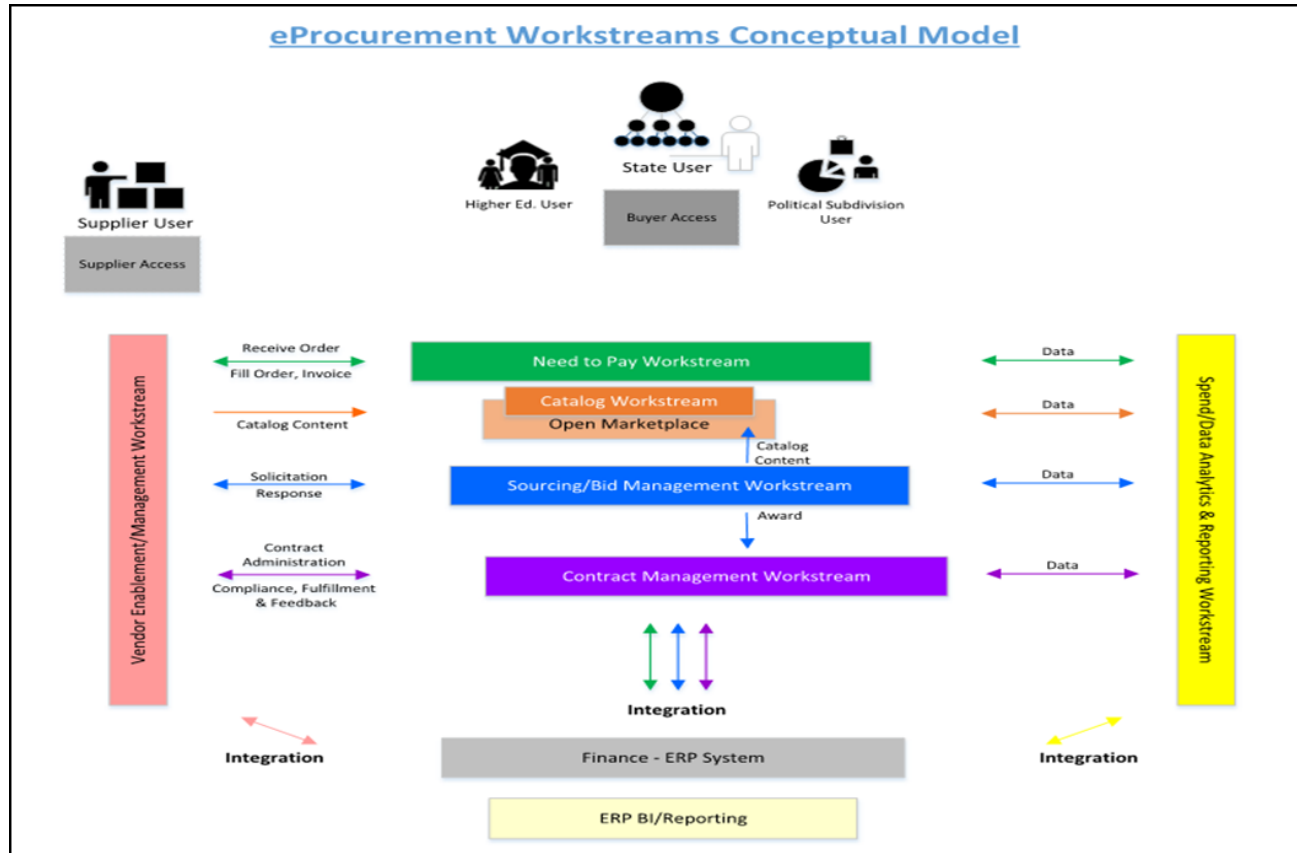


Figure 10. Workstream Conceptual Model

1.2.2.1 General Functionality

Figure "Workstream Conceptual Model" above depicts key procurement related business processes supported by the eProcurement solution proposed by Infosys, and respective data flows. Our solution supports the following procurement processes as required by this RFP:

- Supplier Portal
- Supplier Enablement/Management
- Vendor Performance
- Sourcing / Bid Management
- Contract Management
- Buyer Portal
- Request through Pay
 - Purchase Request Development
 - Purchase Order Generation & Management
 - Workflow Management
 - Payment Card Functionality
 - Receiving
 - Invoicing
- Catalog Management
- Purchasing Data Analytics

To support the State of Maine's vision for a cloud-based, modern, robust, secure, and comprehensive eProcurement solution, we have carefully reviewed all business and technical requirements presented

in the RFP for the State of Maine, and have assembled a solution, approach, and implementation team that aligns with the RFP needs and is based on our proven experience with similar projects.

Some of the key value drivers based on the State of Maine's requirements for the new eProcurement solution are listed below:

- Achieve better value for citizens through improved procurement outcomes.
- Improve client service by providing easy, web-based access to procurement information and services to Departments and Agencies.
- Provide easy, web-based access to information and services that reduce Supplier's burden of participating in the procurement process.
- Achieve an integrated approach to the management of government spend.
- Enable procurement professionals with new tools, technology, and processes to deliver effective client services.

From a technology standpoint, our solution:

- Avoids unnecessary integration for the eProcurement Solution modules – full functionality in one product.
- Contains components that we have already integrated, saving project time.
- Allows other capabilities and modules to be easily added in the future.

Based on Infosys' experience in executing large scale projects in the public sector domain, Infosys proposes the below hybrid cloud-based SaaS model architecture using SAP's Ariba Cloud applications as our core procurement solution to cater the needs of the RFP request. In addition, Infosys will bring other solution components that are extendable to the RFP requirements to allow for future expansion.

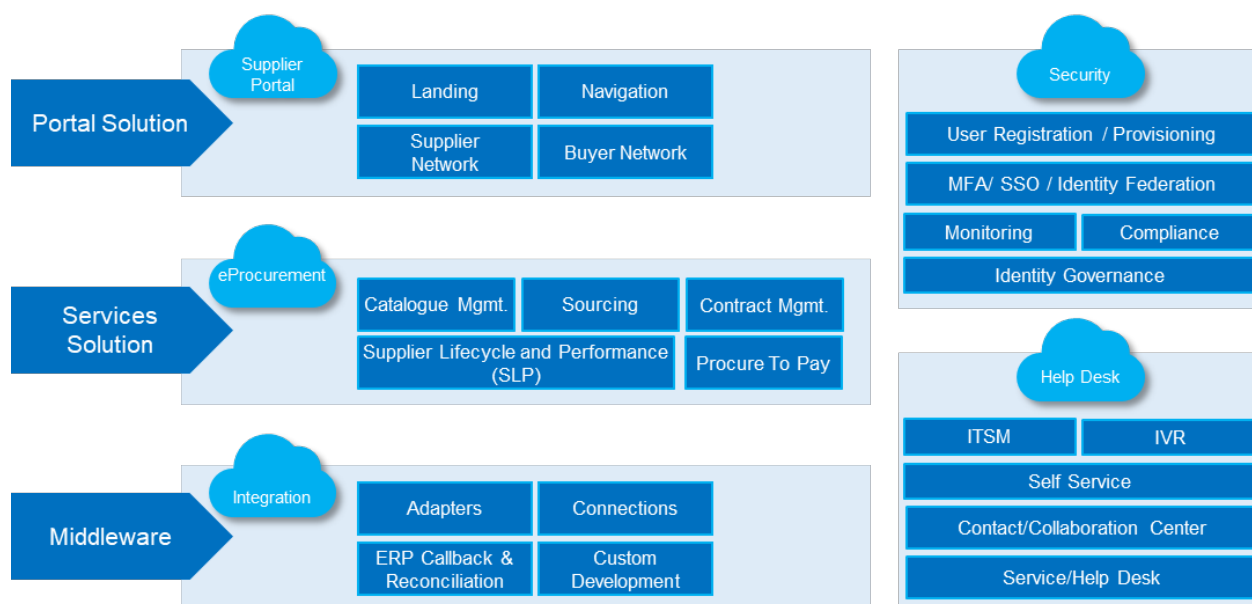


Figure 11. Hybrid Cloud Solution

Infosys has extensive experience in implementing the proposed solution and has delivered value and benefits to clients in similar procurement transformation projects. With the expertise of the experienced the eProcurement team that we have in-house and partnering with our strategic alliance partners SAP and Ernst and Young, we can define and design an eProcurement solution that meets and exceeds the State of Maine's business and technical requirements.

The diagram below illustrates and summarizes the core components of our proposed solution and how it fits with existing architecture and technical standards, meeting the need as well as integrating with the State of Maine's existing ERP systems.

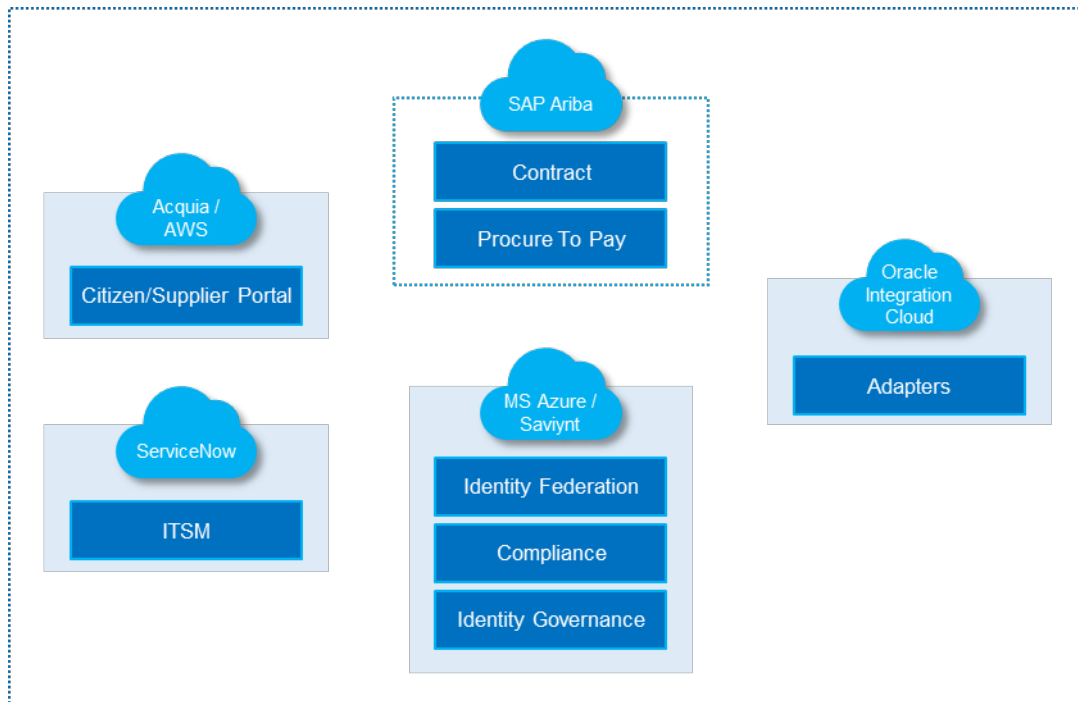


Figure 12. Hybrid Cloud Components

All the chosen and recommended products and services addressing the State of Maine's requirement are best in class and have Leader's standing in Gartner's Magic Quadrant.

1.2.2.2 *Supplier Portal*

Infosys is proposing the Ariba Network a part of 'SAP Business Network (SBN)' as a solution that addresses all of the objectives and requirements of the Supplier portal. SBN acts as a single point of entry (front door) for all supplier facing functions associated with the electronic procurement solution. The SBN will allow suppliers to manage a complete choreography of business collaboration with their customers. The SBN delivers an intuitive user experience that supports self-service supplier registration and maintenance, onboarding, solicitation / bid management, contract lifecycle management, and e-procurement and payables (PO, OC, ASN, Inv. etc.).

The SBN meets objectives and requirements in the following ways:

e-Portal: For State of Maine Suppliers

The SBN delivers an intuitive user experience that supports self-service supplier registration and maintenance, onboarding, solicitation / bid management, contract lifecycle management, and e-procurement and payables (PO, OC, ASN, Inv. etc.) which are discussed below.

Electronic procurement solution:

The State of Maine has an opportunity to successfully leverage the SBN as a component for their procurement needs. Your existing supplier community may already be deeply familiar with the SBN, which dramatically reduces the overall change management effort and will significantly accelerate the transition to the next generation eProcurement solution.

Ariba Network Supplier Landing Page: Below is a screen shot of the SBN landing page that provides a dashboard with overview of records and key performance indicators (Spend, Invoice aging etc.)

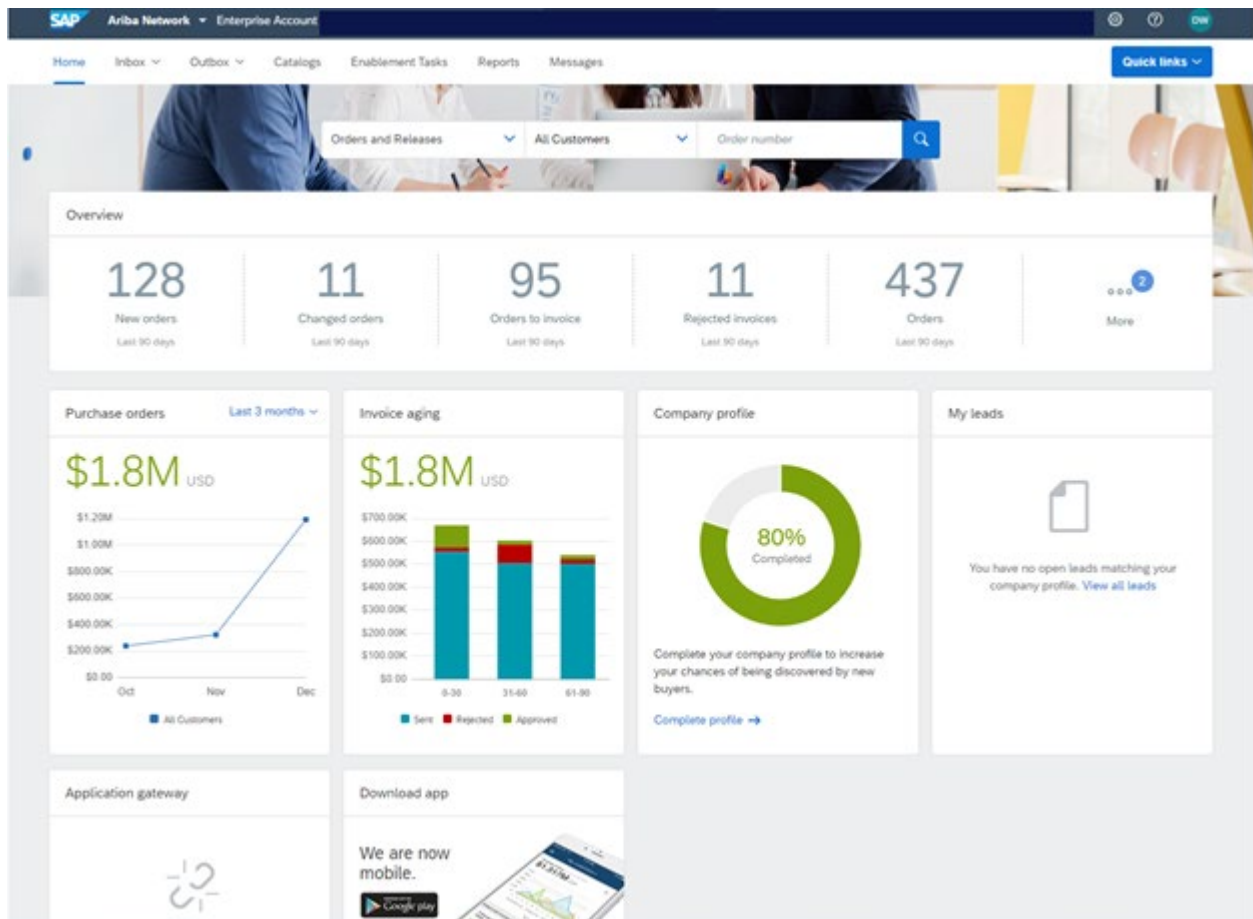


Figure 13. Ariba Network Supplier Landing Page

The SBN provides suppliers the access to support all procurement related transactions between their organization and the State of Maine. This ability is called the supplier unified seller experience. SBN is open, smart, and simple.

Ariba offers a modern many-to-many approach to suppliers, which makes it different from portals and other older technologies. Modern many-to-many provides open options for all trading partners whether they want to respond to you via mobile, or use a portal, or link directly to their backend systems.

Supplier Portal Functionality Enabled by the Ariba Network aka SBN:

Onboarding, registration, and connectivity features help buyers and suppliers get started easily and begin transacting in minutes. Key capabilities include:

- Simple registration and intuitive onboarding through a single, easy-to-use interface
- Entry-level connectivity options such as Web UI, fax, scanning, e-mail, and CSV upload
- Support for a consumer driven buying experience through direct integration of back-end systems using cXML, EDI, or SAP Ariba Integration Adapters.

Order collaboration features help users expedite and enhance order management. Key capabilities include:

- End-to-end automation and collaboration on orders, change orders, confirmations, cancellations, immediate receipt, and one-click confirmation of orders via rapid response purchase order e-mails
- Centralized, streamlined customer communication via a consolidated order collaboration dashboard

- Order task reminders and rules-based order routing for fast, accurate order delivery
- Collaboration with customers on key supply chain planning and execution processes

Solicitation & Contract Collaboration features allow suppliers to locate and respond to solicitations and participate in contract negotiations. Key capabilities include:

- Publicly posted solicitations via Ariba Discovery and the State of Maine's Public site
- Simple solicitation response via user interface or file upload
- Contract collaboration and redlining via the Ariba Network and/or email

Catalog collaboration features help increase PO accuracy and drive online procurement compliance. Key capabilities include:

- Support for CIF, cXML, and Excel e-catalogs, plus integration of online commerce storefronts via the Punch-Out feature
- One-step CIF catalog validation and publication
- Comprehensive catalog dashboard for managing all customer catalog activity
- Visibility into customer catalog update status
- Increased exposure to buyers via public catalogs on the SAP Ariba Spot Buy Catalog solution

Invoice collaboration features help accelerate payments and increase productivity. Key capabilities include:

- Flexible e-invoice options, including:
 - Multi-document and multi-level invoicing with the PO-Flip feature to easily “flip” POs, ASNs, and goods receipts—or specific line items from them—into invoices
 - Non-PO invoicing
 - System-to-system invoicing via cXML, EDI, and CSV upload
- Easy-to-use dashboard and notifications for visibility into invoice and payment status
- Support for multiple languages and over 220 currencies plus compliance with local VAT laws
- Direct access to invoicing wizard via rapid response purchase order e-mails
- Automatic invoice validation and reconciliation

Administration navigation features help lower administrative costs and improve account control. Key capabilities include:

- Single sign-on for centralized management of accounts and Ariba Network profiles across all functions and solutions
- Administrator-defined user roles and ability to assign multiple roles to a single user ID
- Routing by customer group
- Easy-to-use reporting functions
- Accessible, linked documents for every order
- Ability to link accounts, manage Ariba Network profiles, and transfer administrator role

The Ariba Network landing page displays the following user information: user id, user first name, user last name and last log-in of the user. Suppliers can update their user information, link accounts, change their password, and configure their notification preferences. Suppliers use their profiles to centrally create and manage their own users and business contact information.

The on-demand platform helps reduce IT costs and risk. Key capabilities include:

- Availability via iOS and Android mobile devices
- Redundant system architecture, back-up, and recovery procedures

- Industry-leading security measures, including data-at-rest encryption, WebTrust and PCI DSS compliance
- Supplier Support includes 24x7 self-service training tutorials and documentation. Access to phone and chat-based support is also available during normal business hours.

The SAP Ariba Supplier mobile app is a role-based, action-oriented app you can use to get timely notifications and take immediate action on orders and invoices via the Ariba Network. You stay engaged and connected with your customers, boosting productivity by making it simple to collaborate, identify issues, and get business done anytime, anywhere using your iPhone, iPad, or Android device.

The Supplier Mobile App supports:

- At-a-glance updates of orders and invoices with access to details, line items, attachments, and history.
- Configurable, real-time push notifications about orders and invoices that need your attention.
- The ability to confirm customer orders on-the-go.
- Powerful search capability to access 12 months of orders and invoices.
- Intuitive graphs for insights on customer order trends and invoices awaiting approval and payment.
- The ability to pin orders and invoices to your desktop computer for easy access.
- Easy login with your fingerprint or saved username.
- Convenient password-creation tool helps you login on your desktop if you forget your Ariba Network password.

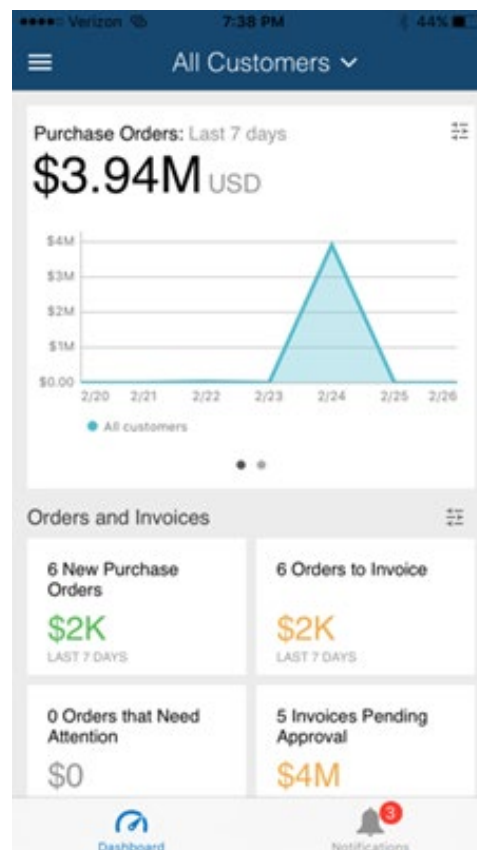


Figure 14. Supplier Dashboard on Mobile

The screenshot above is a dashboard view available for Suppliers to review important transactional

details.

In addition to the above, for supplier access to solicitation results like bid details and award details per the RTM, functional requirements, Supplier Portal #9, we propose an optional custom portal solution. This portal will have the Award Details available for anonymous public view.

1.2.2.3 *Supplier Enablement/Management*

The SAP Ariba Supplier Lifecycle and Performance (SLP) solution along with the SAP Business Network (SBN) (aka Supplier Portal) will meet State's all procurement activities, supplier registration functionality and provide suppliers the ability to establish and maintain their individual account to get business done.

SLP solution supports a full onboarding process, which includes a supplier request prior to an actual registration. This supplier request can be internal or externally initiated, typically consists of the basic information required to determine if adding the new supplier is appropriate.

SAP Business Network (SBN) will allow suppliers to manage a complete choreography of business collaboration with their customers. The SBN delivers an intuitive user experience that supports self-service supplier registration and maintenance, onboarding, solicitation / bid management, contract lifecycle management, and e-procurement and payables (PO, OC, ASN, Inv. etc.)

The State of Maine can manage the entire purchasing process while controlling spending, finding new sources of savings, and building a healthy supply chain. And suppliers can connect with profitable customers and efficiently scale existing relationships by simplifying sales cycles and improving cash control along the way.

Supplier Enablement Services:

Below are specialized services of supplier enablement. Infosys will support the State with Supplier enablement strategy and plan. In addition to this, Infosys will assess the current capability and suggest the State if these services are needed. As of now, the current commercial deal does not include this service.

When you partner with the supplier enablement service team, you have access to a wide range of value-added capabilities that result in effective collaboration. Our proven, scalable methodology supports effective and efficient enablement for an unlimited number of suppliers regardless of size, location, or technical requirements.

We offer the following resources:

- Customized enablement strategy: Use our team's expertise to help you design and develop the most effective enablement strategy for your suppliers based on their profile, purchase order (PO) and invoice volume, and spend. Our approach includes duplicate detection (deduping) and segmentation of your vendor master data to effectively target and onboard suppliers in tiered waves that align with your priorities and objectives.
- The supplier enablement team is comprised of 700+ employees dedicated to enabling procurement transformation projects from all over the globe to be successful.
- Automated verification capabilities for IRS TIN/Name.
- Implementation support, system testing, and project management: We can help you create the processes, infrastructure, and materials necessary to enable and support suppliers. We also implement project management and quality assurance procedures critical to success.
- Comprehensive business process and geographic coverage: Our scalable, end-to-end approach drives supplier adoption across a broad set of business processes, including catalog

management, PO delivery and confirmation, electronic invoicing, payment remittance, dynamic discounting, and payables and receivables financing.

- **Supplier education:** We offer extensive materials for supplier training and support, including user guides, FAQs, technical documentation, and free online seminars that explain the basics of using Ariba Network. We can also deliver your account specific information to suppliers through a supplier information portal embedded in the Ariba Network.
- **Supplier tracking, follow-up, and support:** Standard reports make it easy to track the enablement progress of suppliers throughout the process, and the help desk provides 24x7 application-related customer support and issue resolution.

Supplier Lifecycle

Supplier request projects in SLP allow internal users to request to work with new suppliers. When a supplier request is approved, the supplier is created. An external supplier request allows suppliers who want to do business with an organization to introduce themselves.

After a new supplier is created, a registration manager starts a supplier registration by sending one or more external registration questionnaires to recipients. Registration projects can also include internal questionnaires, and starting the registration makes them available for editing. Approvers review the submitted questionnaires and approve or deny them.

After a supplier is registered, a qualification manager can start qualifying the supplier for one or more specific combinations of commodities, regions, and (optionally) departments by starting qualification projects and sending qualification questionnaires.

Supplier Performance Management (SPM) projects allow to periodically review the performance of suppliers. SPM projects periodically solicit feedback from internal stakeholders based on a standardized set of criteria that is applied to all suppliers.

Procurement Activities supported:

Supplier enablement in conjunction with the supplier portal (SBN) allows the suppliers access to procurement activities like PO delivery and confirmation, electronic invoicing, payment remittance, dynamic discounting, and payables and receivables financing, catalog management.

Suppliers can create and publish catalogs, create catalogs that contain special items or contract prices for specific customers and can control which customers have access to each of their catalogs.

Suppliers can search for and participate in online sourcing opportunities such as a request for information (RFI), a request for quote (RFQ), a request for proposal (RFP), or a negotiation created by buying organizations with the help of SAP Ariba Discovery.

Supplier Enablement and Maintenance:

SAP Ariba SLP provides the ability to establish and maintain supplier accounts. SLP is a set of linked processes for managing suppliers. Defined, template-based processes for managing suppliers that scales easily to bring large numbers of suppliers under management. These processes include Internal and external requests for adding new suppliers to vendor database. Supplier registrations for collecting and managing detailed profile information.

SLP enables to design and develop the most effective enablement strategy for suppliers based on their profile, purchase order (PO) and invoice volume, and spend. SLP's approach includes duplicate detection (deduping) and segmentation of vendor master data to effectively target and onboard suppliers in tiered waves that align with priorities and objectives.

Dun & Bradstreet integration is available in SAP Ariba Supplier Lifecycle and Performance. With D&B integration, questions in the internal supplier request and registration questionnaires can be mapped

to specific fields that hold D&B information. It provides automated verification capabilities for IRS TIN/Name.

Suppliers on the Ariba Network can provide extensive information about their company, from the company address to the specific business policies, to communicate product and service offerings to buying organizations, suppliers can store catalogs on Ariba Network.

Establishment and Maintenance of Pre-qualified suppliers:

The preferred supplier management project feature of Ariba allows the State of Maine to grant preferred category status to suppliers. In SLP, Supplier is qualified for specific commodity/commodities, region, and (optionally) department combination.

In SAP Ariba SLP, qualification statuses can be set for a supplier either automatically using qualification data import, or manually using or qualification projects.

By specifying eligibility criteria, template creators can align a company's sourcing events with their supplier management process to make sure that the suppliers invited to the events are at some point in the registration or qualification process, or to ensure that preferred suppliers are invited.

Qualification and preferred statuses are tied to specific commodity and region combinations and matched to events based on the event's commodities and regions. These statuses are hierarchical and apply to all commodities and regions below the commodity and region in the hierarchy.

Vendor Search:

SAP Ariba SLP module allows user to access Supplier management dashboard and search suppliers by: Name, Country code, ERP Vendor ID or SMID, Supplier first name, middle and last name, Email address, Commodity categories, regions, registration status, ERP Integration status and search results based on certifications.

1.2.2.4 *Buyer Portal*

SAP Ariba Buying and Invoicing (B&I) solution which also includes Guided Buying provide functionality that acts as a personalized single point of entry ('front door') to initiate the full life cycle of procurement activities for Participating Entity users.

The B&I solution helps your front-end procurement process operate with maximum efficiency while integrating seamlessly with your enterprise resource planning (ERP) system for requisitioning, Purchase Orders, receiving, invoicing and payment processing. This unique software-as-a-service (SaaS) solution also provides a fast, guided buying experience, streamlined catalog maintenance, and a configurable interface which all help to deliver quick ROI.

The SAP Ariba "Front Door" with Guided Buying landing page enables all casual users to land in the application and view a dashboard with relevant tiles. Conversely, power users (buyers/analysts) require a configurable dashboard to view the status of critical tasks, to-dos/inbox, and manage the processes they are responsible for (solicitations, supplier on-boarding, contracts, etc.).

To satisfy the unique requirements of the distinct groups of users, we propose directing casual users (Bill the Maintenance Guy) and buyers/analysts to their preferred view of SAP Ariba from the existing State of Maine's site. The State of Maine can create a url/launch button/tile on their website/intranet to launch the Ariba application thus directing casual & buyers to their respective home page.

Each group will be logged-in leveraging a single sign-on (SSO) and carry out the processes as required by their unique role within the State of Maine. Leveraging SSO/LDAP and SAP Ariba security groups each user will have tailored access to functionality based upon who they are and what they are required to do on behalf of the State of Maine. SAP Ariba supports SSO with Corporate

authentication, where-in the user will be able to login to different applications present on State of Maine's website including Ariba applications without reentering the credentials again.

Once logged in Users (casual user & power user) can maintain their preferences and complete their required work. Below are lists of some actions that may be taken by user type:

Casual Users may:

- Leverage Need Identification support
- Purchase via State of Maine Contracts, Catalogs, Open Marketplace
- Complete forms (solicitation request, contract request, supplier request, complaint to vendor, etc.)
- Be linked to other relevant solutions (Service Now, Travel & Expense, etc.)

Power Users may:

1. Configure dashboards
2. Leverage pre-packaged reports
3. Create ad hoc reports
4. Manage and review supplier records, solicitations, contracts, and other documents stored in the solution
5. Create notification tasks within the appropriate process to communicate internally and externally
6. Post solicitations/opportunities

On the Homepage, a user can view user ID, last name, first name, last login details (Date and Time) details.

Life cycle of procurement activities:

SAP Ariba provides cloud-based procurement solution will assist State of Maine users throughout the life cycle of procurement activities that involves demand identification, supplier selection, setting up contracts with the chosen suppliers, placing orders, purchase order processing, receipt handling, invoice creation and payment processes.

REPORTING:

Using prepackaged reports, users can run the reports (standard and non-customized) and extract the required metrics. Additionally, users can also create customized reports using analytical report feature.

Alerts and Notifications:

An alerts and notifications feature for each transaction is configurable and users have an option to turn them on or off. These alerts and notifications are sent to users via email and/or a mobile app.

When a user logs into the application, under "To do" title on Ariba homepage, documents which require action are presented to the user.

Access to Different Modules:

Based on the business role, each user is assigned with groups that grant access to perform specific activities in SAP Ariba. For example, a purchasing user's role is to execute procurement and thus this user won't be given access to upstream (Sourcing/Contract Management) modules.

Vendor Search:

The SAP Ariba B&I allows users to search suppliers in supplier manager by name, address, ERP Vendor ID, ANID, Email, Preferred Ordering Method, Preferred currency, System ID, PCard Compliance level, Change Order restrictions, Contact, Organization ID value/Domain, Active and Is

Network Enabled. Licenses and insurances fields can be introduced as custom fields that involve customization. All of these fields are searchable and reportable in an excel format.

1.2.2.5 *Need Identification*

The Need Identification component of SAP Ariba Guided buying (GB) provides functionality for a user to initiate any type of procurement action with configurable business rules to support Participating Entities custom business needs.

GB provides a smart, easy, and intuitive user interface for employees to create any type of procurement request thereby making low-dollar, high-volume requests completely self-service.

Support Participating Entities custom business needs:

Ease of Use and Compliance are cornerstones of a successful eProcurement transformation. By leveraging Guided Buying, the State of Maine will provide its users with a consumer like shopping experience that provides access to catalogs, State of Maine contracts, and guidance within the context of the procurement process to ensure compliance, while maintaining user satisfaction. The result, satisfied users, compliance to State of Maine policies, more spend under better management, and reduced maverick spend.

Initiate procurement action:

Whether a casual user, or experienced department administrator, or anything in between, you will have access to a solution that allows for an easy completion of required purchases. Guided Buying will truly be the front door to the State of Maine's procurement activities. Guided Buying has tiles which are dedicated to a specific purpose and based on the URL configuration, the user is taken to desired page upon clicking without additional login efforts. Navigation from Guided buying to Ariba Sourcing or buying and invoicing is based on user assigned groups (roles and permissions) is effortless. Users with required groups can access different modules directly from Guided buying.

Users can also be redirected to other solutions (ServiceNow, travel and expense, etc.), complete request forms (supplier, solicitation, contract etc.), and complete other required tasks (complaint to vendor, quick quotes, etc.).

Casual User Landing Page (Need Identification):

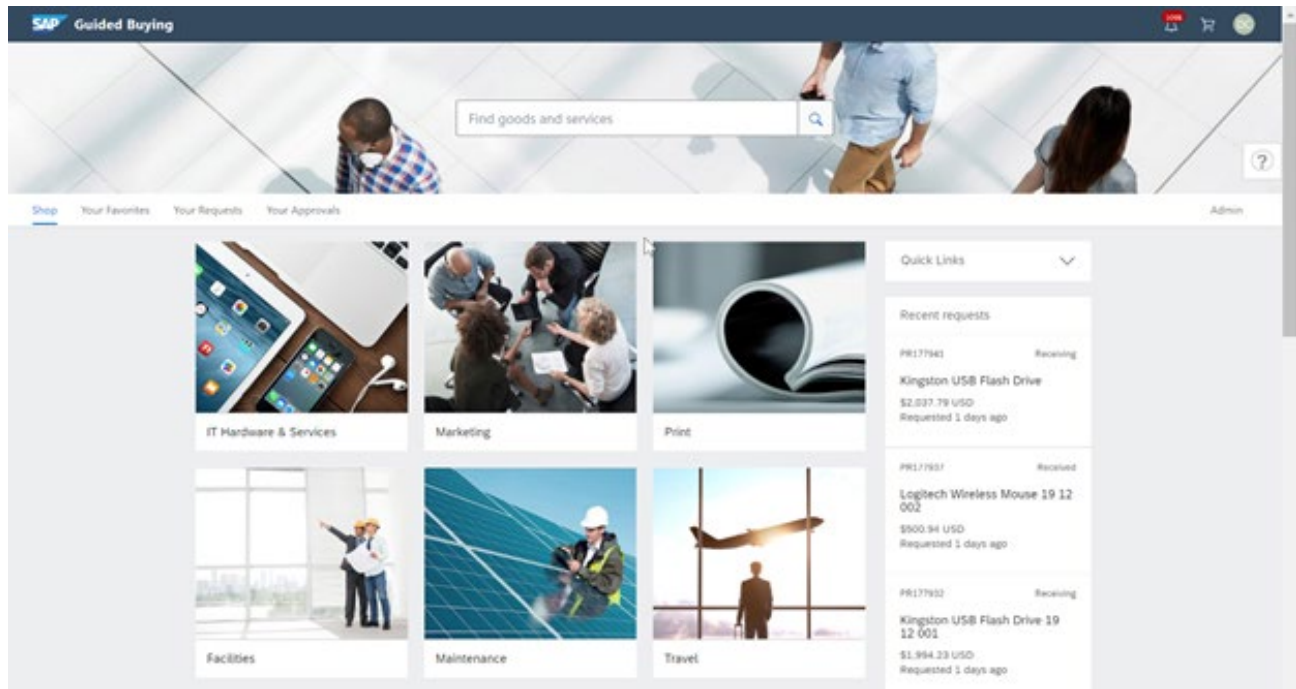


Figure 15. Casual User Landing Page

Note: Need Identification is a component of the Casual Users landing page and will provide guidance to the appropriate buying channel.

User-friendly, intuitive, flexible and adaptable UI:

SAP Ariba believes that Guided Buying is the perfect solution to need identification. The GB solution can be flexibly configured to align forms, permissions, and system behavior for each user, presenting them with customized tiles and categories to streamline purchasing. Rather than build an additional solution for need identification and direct the user to the procurement application after completing a process, it is suggested to place the user directly in the solution and provide in-context guidance based upon the State of Maine policies and procedures. Policy warnings can be configured and displayed to the user as they “shop.” Highly configurable approval workflows can place the right person/group into the requisition approval process. By leveraging all that Guided Buying offers, the State of Maine can streamline its procurement processes. The result, satisfied users and compliant spend.

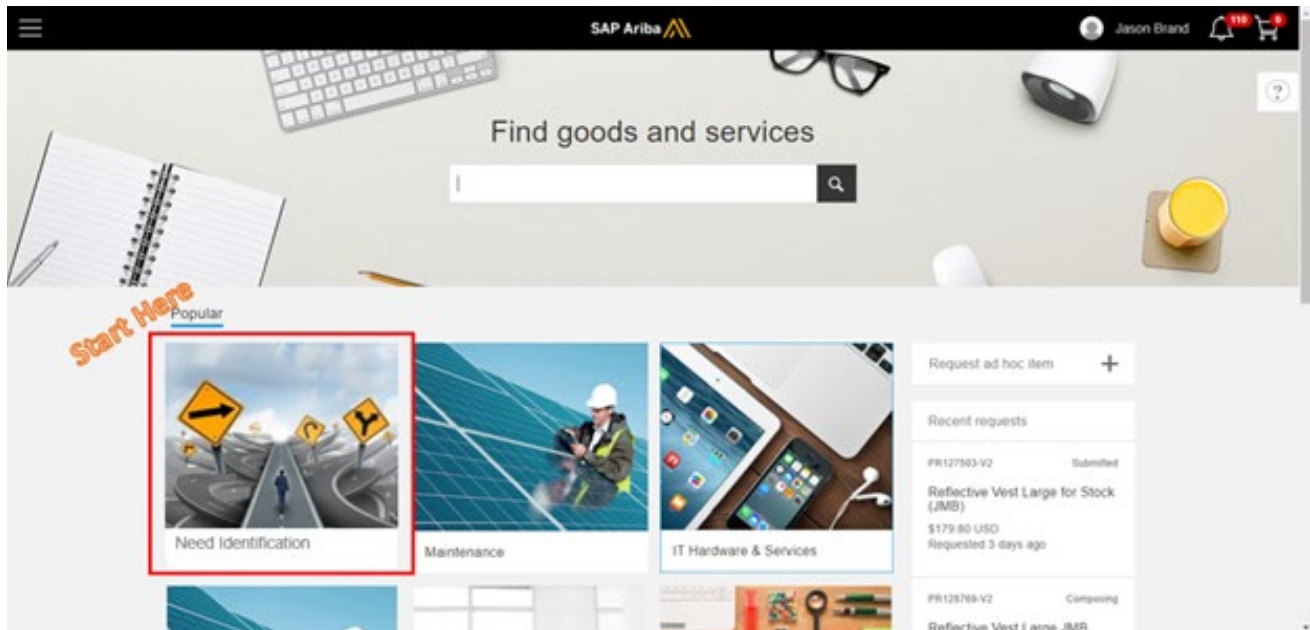


Figure 16. Guided Buying Catalog Tiles

Sample landing page including a “Need Identification” tile that will provide the user guidance to the correct procurement process.

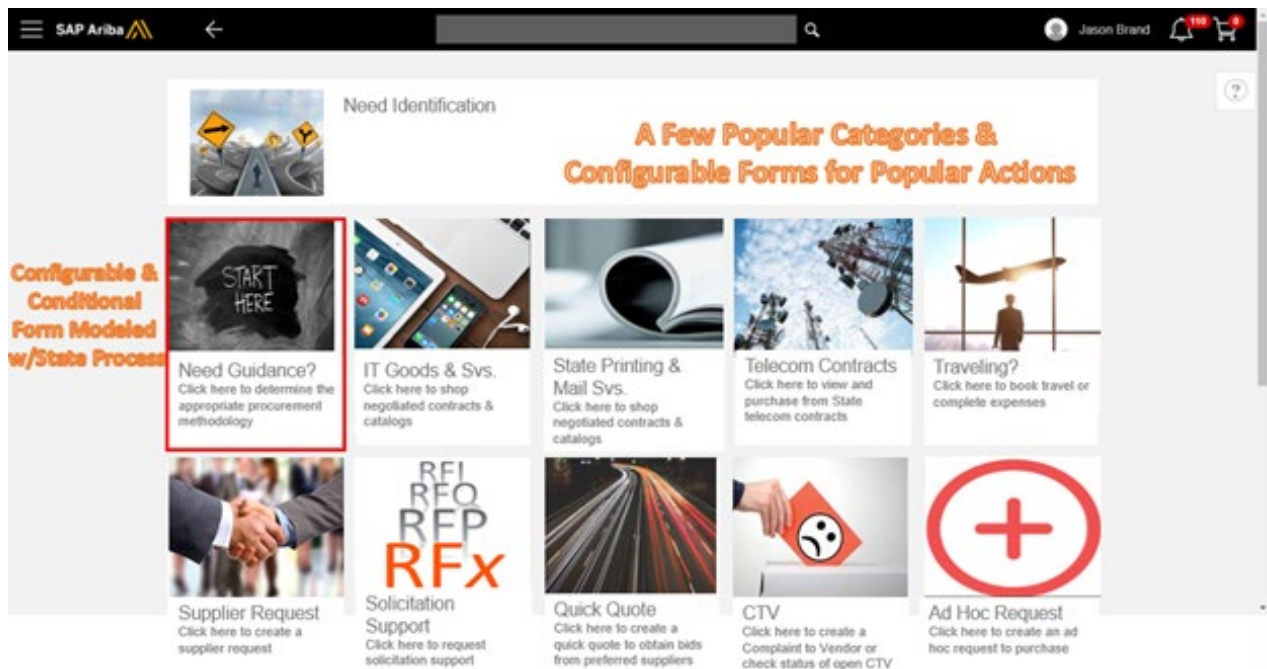


Figure 17. Guided Buying-Configurable Tiles

The “Need Identification” tile will provide the user access to the relevant actions available. If the user is not certain what action to take, they may leverage a decision tree/policy via the “Need Guidance” tile in the upper left. The actions available to the user are configurable and would be defined during deployment.

In Guided buying, users can select procurement specific action either via tiles (configured for specific action) or by search engine. Every tile is designed in such a way it reduces the user's efforts and makes easier way of achieving the desired outcomes.

Guided buying allows an organization to have department specific landing pages and tiles and users can only perform confined level of actions. Procurement policies can be configured and will be in effect when user checkouts the shopping cart.

Guided buying alerts users by posting error/warning messages based on the severity if the shopping cart does not fulfil the policy. Most of the fields present on a procurement document are available either in the form of drop-down menu (PU specific data can be made available) or auto-populated based on user profile.

SAP Ariba uses business rules to trigger approval flow for requests that are created in Guided Buying. For each type of transaction, based on business requirements, approval flow is configured. In Ariba, each process has a separate approval flow which is configured based on business requirement. The approval flows are editable, tested and is deployed in no time. Any changes made to the flow under approval processes will be in effect for new transactions.

1.2.2.6 *Request through Pay*

The SAP Ariba Buying and Invoicing module will provide State of Maine with the Request through Pay services. Through SAP Ariba Buying and Invoicing, the State of Maine can automate, improve, control and monitor procurement to realize immediate process efficiencies and cost savings. Automation of the source to settle process is critical to achieving contract compliance, realizing sourced savings, and delivering value to the State of Maine. Built on robust and highly scalable architecture, SAP Ariba Buying and Invoicing provides full source to settle functionality for all users and commodities so you can quickly locate and collaborate with suppliers for all goods and services and process every purchase from requisition to reconciliation.

Purchase request:

Guided Buying will be the front door to procurement and will serve as the solution to create purchase requisitions. Ariba has the functionality to create requisition for Goods/ Services by referring to the Contracts, Catalog, or non-catalog items as well for single/ multiple suppliers. Each requisition has a unique ID assigned to it for identification (Ex. PR1234). Only members of Purchasing Group will be able to create requisitions and will be able to make amendments to the submitted requisitions. Ariba has a robust search functionality that allows for search of already created requisitions and to be copied into a new requisition.

Ariba allows users to add comments/ attach attachments to the requisitions both at header and line-item level. Purchase orders are created automatically after the requisition is fully approved. The approval workflow is highly configurable and will be configured to meet the State of Maines requirements. Purchase orders will be sent to suppliers via the SAP Ariba Business Network. Subsequent change orders will be routed to suppliers via the Ariba Network as well. Change orders will be subject to a configurable workflow.

Catalog shopping to drive spend to existing contracts:

Ariba has the functionality to set-up static catalogs and punch-out catalog. When State of Maine users search for goods/service to be requested using keywords, Ariba displays the available catalog items which can be added as a line item to the requisitions. The accounting data and supplier details for the line item is defaulted from the catalog.

Access to external retail marketplaces products:

The Spot Buy capability of SAP Ariba is a new business-to-business marketplace suppliers can use to find new customers, increase sales, and increase revenue among SAP's large base of customers. Spot Buy is a feature that helps you find and buy non-sourced goods, those goods that have not been previously put under contract and never will be. With Spot Buy users can purchase goods within

your SAP Ariba Buying solutions without the requirement to source the supplier, enter the supplier in the vendor master, or even provide the supplier with any payment method, such as a procurement card, or invoice process. If Spot Buy is enabled, when you search for an item in your SAP Ariba, the results page is divided into two tabs: Company Catalog and Spot Buy Catalog.

Intelligent workflow engine to apply entity and enterprise-wide business rules:

The request through pay workstream is the heart of the eProcurement solution starting with a purchase requisition and concluding with the receipt of an electronic invoice via the SAP Ariba Business Network.

SAP Ariba provides a robust approval rule management process through a web-based interface, allowing users to graphically build out simple and complex flows and rules. Specific technical resources are not required to manage the approval process. SAP Ariba provides out-of-the-box conditions for faster rule building, but the user can configure a variety of simple and complex rules. Approvers are identified with each approval and a record is kept of each approval in the "History Tab" of the document. Workflows/approvals/business rules can be configured on any data point on the Purchase request document. Rules for one organization can be driven by the organization/agency/company code value so that a specific rule set applies to that group.

On-line approvals:

Approvers are notified of a required approval via email, on screen notification, mobile application notification, and to do lists. Emailed notifications allow the user to approve directly via email and include a link to go directly to the transaction in the solution to further review and approve it. To-do list on the user dashboard also has the list of documents that are awaiting the user approval and user can act upon it from the UI.

Electronic order dispatch:

Orders and releases generated by the Ariba procurement applications are sent electronically to Supplier Ariba Network as cXML documents. The Ariba Network functions as a hub to receive order documents and send (route) them to suppliers for review and order processing (fulfillment) using a supported order routing method. The State of Maine can select order and release routing methods when you set up supplier account and can change them anytime afterward. If there is a change on order routing method, the change takes effect immediately.

Invoice matching for payment authorization:

Ariba allows for both 2-way (PO/Invoice) and 3-way match (PO/receipt/Invoice). In case there is a mismatch in between the data on the matched documents Ariba raises Invoice exceptions which will be handled by the assigned group and once the exceptions are cleared the invoice will be processed for payment depending on the payment method preferred by the State of Maine.

Ariba has the functionality of corporate purchasing card (i.e., PCard) that can be used to purchase goods on SAP Ariba Buying and Invoicing. A PCard can either be assigned to an individual or can act as a ghosted card: Individual cards are physical cards, assigned to users. Only the cardholder can make purchases with that card, and that individual is responsible for resolving any issues that arise. Ghosted cards are assigned to supplier locations, but there is no physical card (only a card number). Any orders sent to the supplier location are billed to the ghosted card.

3-way match for payment authorization:

Ariba has capability of providing 3-way match (PO/receipt/Invoice). Ariba raises invoice exceptions if there is any discrepancy in the data between the matched documents. Once an invoice is fully approved with all (if there are any) exceptions resolved, the invoice is then scheduled to send to the back-end ERP for payment.

Integration with Finance System:

Ariba allows integration with external finance system. The chart of accounts can be maintained in the external finance system and can be sent to Ariba Buying Solutions through scheduled tasks that is set to run at specified intervals. Ariba allows users to define accounting combination validations to define valid combinations of accounting entities. Accounting combinations cause choosers in the user interface to display only valid choices given the values of other accounting fields. They also use choosers to perform validations based on the accounting combinations defined. If the accounting combination for a field is not set up, that field is not used in accounting validation and any value you define for it is allowed on the approvable.

Services contracts:

The Ariba Buying and Invoicing module provides the ability to create contracts for the services procured by the State such as professional services with a pre-determined source. The contract created can be referred to during the creation of the Purchase Requisition and therefore the attributes of the contracts like the accounting details are transferred automatically to the requisition and orders. Milestones can be defined in the contract and successful completion of a milestone typically results in a full or partial financial payment to the supplier.

1.2.2.7 *Catalog Capability*

The SAP Ariba Buying and Invoicing solution which comes with inbuilt Catalog solution will be used to provide catalog capability services to the State of Maine.

The Ariba Catalog solution helps display relevant and current content to the State of Maine's users. It provides a single view of all sources by utilizing cross-catalog search functionality among local catalogs, inventoried items, a spot buy marketplace, and punchout catalogs. With our procurement content solution, the State of Maine can highlight preferred suppliers to drive more purchasing to the State of Maine's preferred buying channels.

Catalog content can be hosted within the system or made available by 'punching out' to the supplier's shopping website. Suppliers hosting content on their sites provide a catalog feed with links to their content as authenticated by SAP Business Network. Both Level 1 Punchout (Site and Aisle/category level) as well as Level 2 Punchout (Aisle, Shelf and Item level for cross-Punchout search experience) are supported.

Creating a Contract with Sourcing Event:

Sourcing Events once completed and awarded to suppliers have the flexibility to generate a contract workspace for future procurement. While creating the contract you can specify whether the State of Maine wants to generate a subscription for non-catalog items to allow purchasing users to search the catalog for the item and to automatically apply the contract terms to the item.

Contract Maintenance for managing contracted items:

The maintenance of contract catalog content throughout the life of the contract/agreement is made by amending the contract workspace, a new version of the corresponding contract is created in the SAP Ariba Procurement solution with the status Open and all of the catalog subscriptions are validated. Catalog subscriptions are only created for items that have any available amount/quantity left must be available through integration with the Contract Management component of the system.

Process for loading, approving/activating catalog content for internally managed and externally created and managed catalogs.

There are 3 channels that catalogs can be updated from:

- Loaded directly by customer via CSV or CIF format

- Loaded by Administrator acting as the catalog management service to the State of Maine user.
- Self-loaded by the supplier via the SAP Business Network.

SAP Ariba provides utilities for suppliers to setup, manage and maintain their catalogs and can upload all of their content using a single, simple user interface. For accessing and managing catalogs the supplier can login into SAP Business Network. Suppliers can create new, update, search and delete catalogs, they have enterprise-grade content management tools to define, validate, and enrich catalog content. By creating catalog rules to cleanse and enrich the data, Suppliers can be rest assured of compliant, error-free catalogs while monitoring content quality with their new dashboard reports.

In all options, the format can either be in CSV or CIF where SAP Ariba will provide the tools and format requirements to easily comply with the formats. The load validation process facilitates all data is in proper order and structure before it is successfully loaded into the catalog processing engine. As an example, if a supplier is self-loading their catalog and there are errors then the SAP Business Network will communicate those issues and require the supplier to fix them before the catalog is successfully loaded. Ariba Administrators can download the catalogs manually from the SAP Business Network or set up AutoSubscriptionSync so that catalogs automatically push to State of Maine's Buying application from the network. AutoSubscriptionSync will also send catalog updates automatically between the SAP Business Network and the State of Maine's Buying Application, including new catalog versions and catalog approval status.

Once loaded, the catalog engine will manage the processing, validation, classification, and approval (robust approval flows can be configured based on business rules which will drive the availability of catalog in the application) of the catalog before it is populated into the active catalog for State of Maine's end user shopping. The catalog approval process provides some unique functionality that allows the user to compare the new catalog with the old catalog. Specific features include the ability to quickly view new items, deleted items, and changed items. For changed items, the user can also view items grouped together based on the amount that the price has changed. For example, the user could specify to see all items that have had a price increase or decrease of 10%. When approving catalogs with hundreds of items, this can dramatically decrease the amount of time it would take to determine what about the catalog has changed.

Open Marketplace:

Spot Buy catalog solution - Spot buy is a capability within the SAP Ariba Cloud Procurement Applications which provides a business-to-business (B2B) marketplace that will help the State of Maine to find and buy non-sourced goods, those goods that have not been previously put under contract and likely never will be. With Spot Buy, the State of Maine can purchase goods within the procurement application without the requirement to source the supplier, with competitive price and delivery options. This will be the solution that will provide an open marketplace environment which will provide access to the aforementioned catalog components and to other non-contract, external internet retail or commercial markets of goods/services, as authorized by the State of Maine.

Here's how it works:

- Find: When an item can't be found in the company catalog, State of Maine users will search the SAP Ariba Spot Buy catalog, filtering results by category, brand, and price.
- Approve: Configurable business rules and spot buy-specific workflow to enforce corporate policies.
- Buy: Approved purchase requisitions trigger checkout, secure payment, and shipment of goods.

When State of Maine searches for an item, the results page is divided into two tabs – Company Catalog and Spot Buy Catalog. The Company Catalog tab displays goods from sourced suppliers,

suppliers that your organization has under contract. If no items are displayed on the Company Catalog tab, a carousel is displayed at the bottom of this tab showing products matching your search description that can be purchased through Spot Buy. The Spot Buy Catalog tab provides additional search results when you are unable to find what you need inside your company catalog. The Spot Buy Catalog tab currently displays filtered content from the eBay marketplace.

Suppliers simply upload a catalog to spot buy and the catalog is searched when Spot Buy buyers search for an item. Suppliers are referred to as "Spot Buy suppliers" when they opt into Spot Buy.

Open Marketplace environment ecosystem:

For Buyers, the Spot Buy for network suppliers feature offers additional choice when searching for non-sourced goods through Spot Buy. Buyers who enable both the eBay Marketplace and the Spot Buy for network suppliers feature can allow users to search eBay and the catalogs of suppliers who opt in to and upload catalogs to Spot Buy. Orders placed to Spot Buy suppliers follow the regular requisitioning process. Spot Buy administrator can control which countries/regions can purchase items through Spot Buy. A custom suppliers list can be created which will restrict users to buying only from specific marketplace suppliers that are approved by the State of Maine.

This Innovative capability provides:

1. An easy way to quickly find and buy what you need from among more than 10 million items.
2. A trusted source of supply from hundreds of pre-enabled suppliers
3. Control, because you customize it according to your policies and procedures, and then receive detailed data for monitoring and reconciling transaction.

SAP Ariba Catalog Features:

- Consumer-like shopping cart with intelligent fuzzy search, parametric refinement, and side-by-side comparison to simplify search, comparison, and buying.
- Rapid supplier catalog enablement to maximize spend coverage.
- Single solution to consolidate management of goods and services, optimizes spend control.
- Automated catalog verification to speed catalog updates, reduce workload, and increase catalog accuracy.
- Advanced contract compliance to address the most complex pricing and deliver maximum savings.
- SaaS deployment for rapid launch, low IT burden, integrated best practices, and fast time to value.
- Level 2 punchout catalogs to simplify ordering and direct buyers to preferred products.
- Relevance ranking and icons to focus buyers on preferred suppliers and products such as MWBE, Green, Local, and other designations.

STATE OF MAINE CATALOG RESPONSIBILITIES:

- Identify catalog Manager—main liaison with Infosys on all things catalogue.
- Identify Suppliers for catalog
- Master data management by State of Maine/buyer should be clearly defined.
- Determine catalog content (this is critical for success). SAP Ariba provides the catalog, but the Customer is responsible for the catalog content for their users.
- Choose catalog types—based on what best suits the products and services you buy.
- Decide who will maintain catalog (generally, this is the Supplier, however, the customer may choose to maintain some catalog).
- Assign Supplier liaison usually by category.
- UNSPSC versions should be agreed upon.

- The State of Maine should provide a dedicated catalog manager for catalog enablement.
- An escalation path should be clearly defined for any issues that arise.

SUPPLIER CATALOG RESPONSIBILITIES:

- Registration on the SAP Business Network.
- Maintaining and uploading catalogues to the SAP Business Network following the Catalog template and requirements provided by the Customer.
- Maintaining and refreshing catalogs
- Working with the customer and Ariba on new features/requirements identified.
- Price, terms and conditions, and desired content should be clarified by the buyer with the supplier.

1.2.2.8 *Sourcing/Bid Management*

SAP Ariba Strategic Sourcing Solution has the capability for the creation and execution of comprehensive sourcing events that lets its customers connect with millions of suppliers across the globe, allowing them to buy the goods and services they need from qualified suppliers offering competitive pricing. With the SAP Ariba Strategic Sourcing solution portfolio, you can manage your entire sourcing, contracting, and spend analysis processes for all types of spend – direct and indirect materials as well as services – all in one place.

Automating the solicitation process (for both buyer and supplier) - SAP Ariba Sourcing will help the State of Maine of Maine improve upon the existing solicitation process. SAP Ariba Sourcing is the most widely adopted and complete strategic sourcing offering in the marketplace used by thousands of customers to create and implement competitive best-value agreements.

By combining best-in-class sourcing and negotiation technology with access to a global network of suppliers and unparalleled strategy and category expertise, SAP Ariba Sourcing enables organizations of any industry, size, or geography to drive fast, sustainable results by automating and streamlining critical tasks across the sourcing lifecycle, including:

- Strategy development – Identify savings opportunities, assess market dynamics, and develop an informed sourcing strategy.
- Sourcing and negotiating – Identify and qualify suppliers, negotiate best-value agreements, derive optimal award allocations, drive project collaboration, and standardize processes and manage knowledge.
- Monitoring and managing suppliers and agreements – Quickly implement supplier agreements, track and realize savings, and manage supplier performance.

SAP Ariba can facilitate the creation of purchase requisitions and solicitation requests and route them to the appropriate State of Maine user to facilitate review/approval and facilitation of the required follow on processes (sourcing, purchase order, etc.). The list of suppliers invited to each solicitation is automatically captured by the system. Furthermore, a record of all solicitation related notifications sent by the system is accessible through the messaging center as well as the event log. The supplier list (group) may be printed in multiple ways, from the supplier tab at the event level, and also via the print event details feature from the solicitation overview tab.

The solicitation can be published automatically upon the complete of creation process. Additionally, the solicitation can be published at a point and time in the future, which is configured by the user at the time of solicitation creation.

Standard templates and libraries

The State of Maine will benefit from out of the box features and functions that can be configured to support the State of Maine's specific requirement. Features include; robust RFx (ITB, RFI, RFP, etc.) creation and management, Reverse Auction, Reverse Auction with Bid Transformation, Forward

Auction, Forward Auction with Bid Transformation, Total Cost Auction, integration to Ariba Discovery supporting public posting, sealed envelope bidding, bid analysis and optimization, scoring and grading, conditional content, communication and messaging internally and externally, direct integration to SAP Ariba Contracts and several other prepacked event formats. Using event templates, SAP has configured a myriad of government procurement methods including sealed and unsealed bids, open market solicitations with the appropriate solicitation notices, intent to bid (ITB) / invitation for bid (IFB), and others.

Benefits that other SAP Ariba customers have achieved leveraging SAP Ariba Sourcing include a price reduction of 8-14%, identification of qualified suppliers via Ariba Discovery, reduction in solicitation cycle times (up to 50%) and reduced administrative costs (up to 15%).

Sourcing templates can be configured for quick quotes. In addition, there are collaborative requisitioning and tactical sourcing (3 bids and a buy) options in the Buying module. SAP Ariba Sourcing also includes a Sourcing Library. Specifications can be managed in the solution and stored in the sourcing library. The sourcing library can be leveraged to add content to a sourcing event. Attachments are limited to 100MB.

"The State of Maine may include a specific document (check list) that the Buyer/Analyst should consult when evaluating proposals. The checklist can be associated with a template and conditionally provided to the user based upon solicitation creation. Conditional logic can be utilized such that the check list changes based on the entity running the solicitation. Alternatively, we would recommend that the State of Maine leverage Sourcing process templates in the solution to replace the checklist. The template would include a series of phases and tasks the user must complete in order to successfully conduct the solicitation. The process can vary based upon Agency/organization, commodity, etc. Capabilities include a project management tool with flexible process management capabilities that help companies model and standardize their own unique sourcing processes. Project Management offers templating of process models for broad organizational deployment, including the ability to auto-configure the "right" process based on project attributes as well as conditional question responses."

Formal or informal, sealed or un-sealed, complex or simple

Two (and multi) Step ITBs can be set up within an event in order to evaluate different parts of a bid or a proposal. For example, a technical proposal may be evaluated in the first step, with pricing to be evaluated in the second step. These steps may also be configured to be "sealed" bids as well; meaning that they are not visible to anyone until the virtual envelope is unsealed/opened.

To ensure a quick turn-around time, the sourcing modules provide sole source, emergency and RFI templates which can be configured using standard sourcing project template functionality.

Suppliers may revise and resubmit their bid at any time until the solicitation closes. All bid communication is encrypted. In addition, sealed bid virtual envelopes can be leveraged to keep bids sealed until the virtual envelope is opened.

Initiating solicitations from a requisition,

Solicitations can be created directly within the sourcing solution, from a requisition, or a sourcing request. Solicitations may be created from a purchase requisition. This may be done directly from one requisition and include content from other requisitions, or from a number of requisitions that are held for aggregation. The solution supports the entire solicitation process inclusive of the electronic solicitation and all the supporting tasks and process that are required to complete a successful solicitation. The State of Maine and its Agencies/Organizations can configure robust process templates tailored to their unique requirements. For example, one agency may configure an RFP process that includes a series of phases, tasks, terms & conditions, questions, reviews, approvals etc.

that are unique to their solicitation process. Another agency may be required to follow a slightly different process. Leveraging configurable templates this will not be a problem, rather it will become a benefit for the State of Maine. Users will have a defined process to follow which will include the appropriate documents and language to complete the solicitation. The result, a streamlined and compliant process.

The solution also supports other critical components of the solicitation process including addendums, amendments, Q&A, supplier notifications, supplier communications, internal communications, document management, etc.

Solicitation Project Management:

SAP Ariba Sourcing supports the entire solicitation process including the “project management” components. Above, you can see the process phases and tasks the user was required to complete as part of the solicitation. The phases/tasks are configurable by the State of Maine and may vary based upon Agency/Organization, commodity, etc. With SAP ARIBA, Prior solicitations can be copied to kickstart the creation of a future solicitation. All content from the prior solicitation is included in the new solicitation, and the user is free to keep/discard or edit content as required. Tasks within a solicitation can be reassigned to another users. This can be done by individuals with appropriate access to the solution and the specific solicitation.

Name	Document	Owner	Status	Due Date
▼ ✓ 1. Analyze & Plan -		Project Owner	Complete	
✓ Analyze Spend Data -	Category Analysis -	Jason Brand	Complete	
✓ Prepare Sourcing Strategy -	Sourcing_Strategy -	Jason Brand	Complete	
✓ Approve for Sourcing Strategy -	Sourcing_Strategy -	Jason Brand	Approved	
▼ ✓ 2. Request for Information (RFI) -		Project Owner	Complete	
✓ Create RFI -	Landscape Services RFI (v2/3) -	Jason Brand	Complete	
✓ RFI Approval Prior to Publish * -	Landscape Services RFI -	Jason Brand	Approved	
✓ Publish RFI * -	Landscape Services RFI -	Jason Brand	Complete	
✓ Review & Score/Grade RFI -	Landscape Services RFI -	Jason Brand	Reviewed	
▼ ✓ 3. Conduct Request for Proposal (RFP) -		Project Owner	Complete	
✓ Create RFP * -	Landscape Services RFP -	Jason Brand	Complete	
✓ RFP Approval Prior to Publish * -	Landscape Services RFP -	Jason Brand	Approved	
✓ Publish RFP * -	Landscape Services RFP -	Jason Brand	Complete	
✓ Review & Select Best & Final Offer Participants -	Landscape Services RFP -	Jason Brand	Reviewed	
▼ ✓ 4. Best & Final Offer -		Project Owner	Complete	
✓ Create & Publish Best and Final Offer * -	Best & Final Offer -	Jason Brand	Complete	
✓ Analyze Best and Final Offer * -	Best & Final Offer -	Jason Brand	Complete	
✓ Approval of Award of Business * -	Best & Final Offer -	Jason Brand	Approved	

* Indicates required task

Figure 18. Solicitation Project Management

Public posting

Attachments associated to a solicitation are available for review via the Ariba Network and can be made available to the public when utilizing a Discovery Posting. Further, the Ariba Discovery API set makes it possible to post SAP Ariba Sourcing solicitations on portals and web sites outside the usual discovery area. What this means for the State of Maine is that certain attachments could be passed back to the public posting site.

In order to make the procurement file and associated attachments publicly viewable, it is integrated to the solicitation public posing site. We would utilize an API built specifically for this use case.

SAP ARIBA has the functionality to hide the identity of the supplier while posting questions and answers in public forum. ARIBA also provides the functionality of cancelling a response or solicitation. This can be integrated with external website to indicate that the process has been cancelled.

Supplier notification

As a seller on SAP Ariba Discovery, if the capabilities of a supplier company match a buyer's project requirements, SAP Ariba Discovery displays the business opportunity on supplier's Leads Dashboard. Such Suppliers which are un-registered in the Buyer application can still choose to respond to Buyer's matched postings after the release of the solicitation. Award notifications to awarded suppliers are available out of the box when during the award process within the tool. These content and structure of these emails are configurable as well.

The user who is submitting the award has the opportunity to select if emails should be sent to awarded and/or non-awarded suppliers, or if emails should not be sent at all. The system-generated communications generate a variety of system messages relating to invitations, notifications of changes to an event, event close, award notifications, etc.

Supplier Proposal Review

The screenshot shows the 'Supplier Proposal Review' interface for 'Doc786179221 - Landscape Services RFP'. The interface includes a navigation bar with tabs: Overview, Content, Suppliers, Discovery Suppliers, Report, Messages, Log, Scenario, and Award. The 'Content' tab is active. Below the navigation bar, there is a 'Pending Selection' status and an 'Actions' button. The main content area displays a table of responses for various questions. The table has columns for 'Name', 'Initial Price', 'Historic Price', 'Direct Tech Industries Price', 'FAB Associates Price', and 'KJB Inc. Price'. The questions are listed in the 'Name' column, and the corresponding prices or responses are listed in the other columns. The table is filtered by 'All Content' and 'Responses'.

Name	Initial Price	Historic Price	Direct Tech Industries Price	FAB Associates Price	KJB Inc. Price
Totals:	\$132,000.00 USD	\$54,000.00 USD	\$129,200.00 USD	\$129,800.00 USD	\$115,650.00 USD
1 Introduction:					
2 Commercial Terms:					
2.1 Will you comply with our standard payment terms of 2%20net60?			Yes	Yes	Yes
2.2 Are you willing to sign the attached Master Agreement? If no, please provide comments and attach any redlines you may have.			Please see attached redlines	OK As Is	OK as Is
3 Pricing:	\$132,000.00 USD	\$54,000.00 USD	\$129,200.00 USD	\$129,800.00 USD	\$115,650.00 USD
3.1 Landscaping Services Questionnaire:					
3.1.1 Has your firm done business with us in the past?	No		No	No	No
3.1.2 Percentage of your customers that you service on a national basis?			1-20%	1-20%	21-40%
3.1.3 What is the typical response time for Snow Removal services?	1 Day or More		1 Day or More	1 Day or More	5-6 Hours
3.1.4 Do you charge extra for bagging and removing grass clippings?	Yes		No	No	No

Figure 19. Supplier Proposal Review

SAP Ariba Sourcing supports the creation of pre-requisite questions which we recommend utilizing in cases where solicitations have a mandatory set-aside. The supplier is responsible for answers in the prerequisite questions, which in this case, would require them to self-attest their MBE certification. In the event they cannot meet the certification or set-aside requirements, the system will not allow them to participate in the solicitation. A Buyer Review of the prerequisite content can be utilized with pass/fail criteria to review vendor certification status prior to allowing the supplier to proceed with a proposal.

Evaluation of bids/proposals

Suppliers can submit alternate bids after submitting a primary bid. There are three alternate bid options:

1. **Supplier Bundles:** Allows participants to submit discounted pricing based on bundles of items they create.
2. **Volume Tiers** - Allows participants to create volume tier structures with pricing at each of the volume tier levels.
3. **Alternative Pricing** - Allows participants to submit different values for the terms included in an

item and adjust their price accordingly. Alternative pricing allows participants to respond to what you are looking for and also provide alternative responses.

Ariba supports a functionality which includes automatic scoring, subjective grading and team member participation. Buyers can add graders from as many different areas as possible while scoring suppliers anonymously. Buyers can also assign a weight to graders on a grader-by-grader basis.

The Sourcing solution offers prepackaged bid response reports that can be viewed through the user interface or exported to Excel or PDF. This includes the responses to questions/requirements as well as the Scoring.

Awarding the event

Design Build (DB) with one entity and a single contract to provide design services as well as construction can be configured within the optimization scenario functionality so that the bid award is limited to a single bidder. Within SAP Ariba's Sourcing Project workspace, the Design Bid Build (DBB) can be organized in three phases such that the steps/tasks within the design phase are completed before the bid is released and awarded; with a build/construction phase to follow.

Leveraging a feature called Scenario Optimization the State of Maine may create numerous constraint-based award of business scenarios. The sourcing award can be created to one or more suppliers across one or many items. The award can also be split by category/region provided the solicitation was setup with the appropriate allotting strategy. Awards can generate a contract workspace for future procurement and a contract release, which once fully approved, becomes a purchase order.

There are two approaches to resoliciting no award bids. One option is to create a new solicitation and use the event copy feature. In this approach, all solicitation content (documents, requirements, forms, etc.) are recreated. In some cases, the State of Maine may prefer to "re-open" a no-award solicitation. If re-opening the solicitation does not require additional or new approvals, this is oftentimes the preferred method.

When granting an award to a supplier(s), the user/admin also can send a notification (via checkbox) to non-awarded suppliers as well. The content and structure of these emails are configurable as well.

Integration with other solution components to automate the creation of catalogs and contracts.

SAP Ariba Sourcing is natively integrated to SAP Ariba Contract Management, this will allow the State of Maine to create state-wide Contracts, Agency-specific contracts, Project-specific/one-time contracts, or Purchase Orders. The resulting contracts will be available for users to review and procure against as required. SAP-ARIBA also allows users to build line items in the User Interface or via Excel and load them into the solution via the user interface. SAP Ariba provides electronic signature through out-of-the-box integration with third-party vendors, DocuSign and Adobe Document Cloud eSign Services.

1.2.2.9 *Contract Management*

SAP Ariba Strategic Sourcing (Product) encompasses the Contract Management module which covers the contract authoring, contract administration, contract development and contract tracking. Ariba Contract Management has the ability to structure the contract hierarchy as master and sub-agreements. The built-in Ariba Wizard feature provides a seamless navigation of the workflow. Contract Administration provides the authorized users to make the amendments or renewals of the published contract workspaces. A detailed contract life cycle is described below. The Ariba Contract Workspace is the legal document between the supplier and buyer agreed-upon the terms & conditions, pricing, discounts & rebates.

A Contract workspace document is created with a supplier and not with a pool of suppliers. Contracting is usually performed after awarding the suppliers in the sourcing process. Creation of the contract can be initiated after awarding the supplier in SAP Ariba. Contract initiation can be done at the bid-view of the Sourcing event. Predecessor project field in the workspace can link the solicitation project to the contract. Also, contracts can be created separately without any RFP/ Proposals. Contract Module provides the feature to setup the agreement between the supplier and buyer. Contract Workspaces can be created for another department or another organization.

Contract Authoring (Automated with Templates)

A standard set of contracts can be created by leveraging the pre-defined templates that are existing in the CLM. These templates can be furnished with set of documents, To-do tasks, approval tasks, Members of the project, groups involved in the project. Members under the team manage the contract workspace. At least one contract owner would be available to manage the contract workspace. Contract Advisors and other team members with designated roles must be under the Team Tab. Contract management has the ability to set the unique numbering format for the contract workspaces which start with CW. This sequence of numbers can be customized in accordance with business requirements.

The Ariba Contract Templates feature enables the reuse of contract information and documents for different contracts. Templates can be designed for business regions, specific area or any other business need. Templates can be accessed by a specific set of users based on specific conditions maintained. Users with contract authoring permissions can create the templates with desired contract documents, tasks and team members. Multiple Contract Templates can be created based on the requirement using Ariba Contract Management Module. Contract Module has the ability to maintain the set of standard documents in the document section of the templates. Published contract templates are used in the creation of the contract workspace. To update or modify the data in the template, the template must be amended. The changes can be tracked using the version history. Contracts can be created for another department or another organization.

Similarly, the changes performed on the contract workspace can be tracked using history. Version changes are recorded in the history of the contract document, with all the changes made to the document. Version control enables you to manage contract modifications and prevent the contract document from being edited by multiple users simultaneously. Using version control, one can check out a contract document to edit it. No other user can edit the contract document while it is checked out. The changes you made are saved and the contract document can be edited by other users. Version controlling for update of templates is suggested. Documents, terms/conditions, and specifications (along with team members and tasks) can be updated on a template as described in EPROC-CNT-7. Each template will need be updated individually.

The updated template version, with updated documents and terms/conditions can be viewed and new contracts can select the latest published templates for use.

Contract Administration

Published contract workspaces can be edited/amended to modify certain details of the document. To perform the administrative changes on the document, we can leverage the administrative amendment, which does not require any approvals. Major changes on the published contract document, which require review, are possible using the Amendment type of amendment. The termination and renewal of the contract document is possible with Termination & Renewal type of Amendments. These are reviewed by the project team members. OOTB functionality allows a user to edit the workspace fields in a draft State of Maine/Draft amendments.

The Ariba Contract has the ability to create the line level, item level, commodity level and supplier level contracts. The Line Level Contract is created for the specific line item(s) with the defined pricing

supplied by the supplier. Commodity specific contracts are created for the specific commodity codes supplied by the supplier. The Supplier level contracts cover all the products& services supplied by the supplier.

Ariba Contracts has privilege to upload additional attachments and documents with a maximum size of 2 GB. The supported document types are MS Word documents (.doc, .dot, .docx), Excel documents (.xls, .xlt, .xla, .xlsx), and .zip files.

Contract Workspaces can be used as the simple repository documents as well as the spend accumulators. The document section of the contract workspace can be leveraged to maintain the documents. And the documents can be restricted the access with access controls. SAP Ariba Contract Management can capture contract metadata, documents, and attachments up to 100MB each, full history/audit trail, notes, etc. All of the information is captured within the contract workspace (electronic folder) and is retained for the duration of the software subscription.

Electronic Signature

Ariba contract management has ability to integrate with the external DocuSign portal to have the electronic signatures on the documents. Signature tasks are an add-on feature for SAP Ariba Contract Management. The E-Signature task is used to carry out the signing process from internal and external signers. Users privileged as Signers perform the electronic signature using the DocuSign portal. Signers can login to the DocuSign portal to review the document that is shared from Ariba Contracts and provide their e-Signatures. The e-Signature Tasks in the Contract Workspace maintains the signed document and other comments/details shared by signers. An electronically signed contract can designate a specific version as the official, agreed-upon version, understood by all parties to be the version that is in effect. After a document has been electronically signed, no one can modify the document without invalidating the electronic signature. If a signed document is modified, it must be re-signed by all required signers.

DocuSign provides the Secure login for the designated signers & admins to access the documents and to provide electronic signatures on the documents. DocuSign can be integrated for the eSignature functionality for internal and external users. This requirement can be covered using role/group allocation to user profile in Ariba. Users need to be available with designated roles and permissions in the DocuSign system.

Ariba Contract Compliance has the ability to track the accumulated spend. Orders/releases against contracts can be aggregated against the contract for spend tracking and analysis purposes. The Contract compliance must be integrated with Contract Workspace to leverage this functionality. Contract Compliance has the Contract Request, which contains the Pricing terms, Line-Item details, Milestones, Payments & functionality to attach the additional documents. Contract (C) with the payment terms & other details gets Open when the contract workspace is fully published.

This contract (C) is used in the transactions and the spend gets accumulated against it. The Milestone tracker is available in the Contract Request to track the targets assigned during the contract setup. Milestone owner tracks and reviews the accomplishments. Additional reviewers can be set up to review the milestones of the contract. Ariba Contract Management functionality allows to attachment any additional document type of size not exceeding 100 MB each.

Ariba Contract Life Cycle Management has the ability to maintain the pricing terms with an excel template. The contents for the contract line-Item documents are specified in a pricing terms excel document, which SAP Ariba converts to a line item document. A line items document can be created with line items from an external system. The inbound web service, import contract line items document, creates a contract line items document after receiving a request from an external system.

Additional fields can be added to the Contract record with valid values (text, numerical, date) and in different formats (list, radio button, checkboxes, text field, etc.) with appropriate permission based editability and visibility.

Contract Workflow & Approvals

The Ariba Contract Management functionality allows users with specific permissions (contract owners) to review the contract after submission for publishing. Additional reviewers can be added in parallel or in serial to the approval flow to review the contract document.

The customer will have specific contract workflow requirements that will be easily configured in the SAP Ariba Contract management solution. Digital contract approval routing is determined by customer rules that are either systematically applied or have been added based on criteria specified by the project team.

For those users with access to the contract, there is full visibility of status, open required tasks, and next steps provide through email notifications, dashboards, and/or reporting functionality. Approvals can be executed through the application or outside the application through our iOS/Android application available on mobile devices.

Ariba Contract Management supports the creation and negotiation of Statements of Work (SOW). The State of Maine can create a standard SOW template including the terms and conditions, associated documents, approval workflows, etc. Once created the template can be leveraged to send the SOW to each supplier for review and acceptance. This is done at the supplier level; contract mass creation is not supported.

Ariba supplier performance management solution can link Performance Management projects directly to contract agreements. Payment information for each supplier can be tracked as well.

Contract Developments

The State of Maine can configure forms to meet your organization's specific business needs to capture payment retainage, withholding and retention amounts or percentages, and descriptions. Notification tasks can also be configured to notify users or groups of users to key dates or follow-on actions.

Supplier profile information from an awarded solicitation is automatically carried over to the Contract record. Additional information specific to that contract (such as a project manager, other stakeholders) can be added as members to the Team tab with corresponding roles.

A validation can be configured on the Create Contract screen that before submission - when the contract workspace is created - there is a validation that checks the contract effective date. There can also be an additional approval for this so that it is not a "hard stop" that prevents the creation of the contract.

At the time of contract creation, the user may indicate the type of contract that is created, and how it may be used (e.g., Mandatory, Optional, Limited or MBE Set Aside). Once the contract is finalized it can be published, and individuals or groups of individuals with appropriate access may purchase against the contract. The contract object supports spend limits, aggregates spend against the contract and can provide notifications to the contract owner.

SAP Ariba Contract Management supports capturing default account codes. Structured contract line item data for pricing and category codes are captured in the "Contract Line Items Document" (CLID). These defaults are leveraged in SAP Ariba Buying & Invoicing, allowing users to purchase against contracts. Reminders can be established through notification tasks as needed.

The State of Maine will have the ability to set up tasks for any contract event. Tasks can be assigned to owners and can have a notification profile that will send email notification to users when tasks are

pending, active, overdue, and completed. Tasks also will be displayed in a portlet on the dashboard for user action."

The State of Maine can configure forms to meet your organization's specific business needs to capture details on subcontractors or dealers. These forms can be made available for the suppliers to update, or the State of Maine can update the data. Data captured in these forms may be reported upon.

Contract Reporting

SAP Ariba solutions come with their own built-in reporting capabilities. A set of over 250 pre-packaged reports are available. Additional reports can be created by modifying pre-packaged reports or creating new analytical reports. These reports can be displayed within the solution on the user's dashboard or exported for inclusion in other reporting applications.

One of the reports available is 360 report that will give all activity (contracts, solicitations, purchase orders, etc.) for a given supplier. In addition, other reports can detail spend by suppliers of a certain type (SWaM)

The State of Maine may configure the solution to allow suppliers to access their contracts via the SAP Ariba network. Data updates for revenue sharing and/or subcontract payments can be completed by the supplier via response to a notification task.

Our approach for making the procurement file and associated attachments publicly viewable is to integrate to State of Maine's solicitation public posing site. We would utilize an API built specifically for this use case.

Contract Tracking

SAP Ariba Contracts provides a very dynamic and configurable search interface and functionality. Users can choose to add or take away fields from the search interface, so that when they conduct searches, they see only the out of the box as well as your custom fields that would be relevant to them. SAP Ariba Contracts supports the search of metadata at the contract level. Full text search is available to include uploaded documents. Users can combine text search criteria with metadata criteria. There is an access control list on each contract to control visibility, in conjunction with publicly available APIs which can extract contract data filters that can be part of the extraction logic.

Contract Workspaces can be displayed with the search functionality and the search functionality is used for both the active and expired/closed contracts. The search criteria can be customized based on the available fields in the contract workspace.

- Contract workspaces can be searched with filter criteria contract ID.
- Contract workspaces can be searched with the supplier fields.
- Customization is required to set up the special contract types search fields.
- Contract workspaces can be searched with the commodity/category.
- Customization is required to set up the usage type search criteria.
- Customization is required to set up the MBE search criteria.
- Customization for the custom field search is required.

Contract workspaces can be searched using different date criteria such as creation date, effective date, expiration date or using date ranges. Search criteria can be customized to search with the Agency/Supplier/ On behalf of Agency. Contract Workspace can be searched with the different contract users. (Contract owner/Contract Advisors). Search criteria can be customized to search with the reference fields that state has added to contract. There is no OOTB functionality that classifies the contracts with catalog hosted or punch out system. Customization is required in the determination of

the contract lines associated with a catalog or not, and to have a variant of internal hosted or punch out.

Contract Notifications

Alerts and notifications can be configured within each contract workspace. Additionally, the message board can be leveraged by the team members of the contract to send out messages and alerts to relevant stakeholders.

System triggers the email notifications as per the settings to the users for the contract updates such changes, spend consumption or expiration or renewal. The settings are configurable.

1.2.2.10 *Vendor Performance*

- SAP Ariba Supplier Performance Management (SPM) enables you to use consistent measurements for supplier performance to identify performance problems. SPM components to measure supplier performance are surveys, which collect input from stakeholders in your organization, scorecards, which provide an overall score for suppliers. A scorecard can include data from surveys and report data. A score is typically based on data about a supplier for a specified evaluation period and key performance indicators (KPIs). KPIs act as containers for data from surveys, reports, or other sources.
- SPM components enable the measurement of supplier performance by capturing vendor performance data such as on-time delivery based on order need-by vs. receipt dates, Other measurements include, order accuracy based on ordered vs. received/rejected quantities, pricing accuracy based on order vs. invoice prices, contract milestone completion, customer surveys, capture/storage of any vendor performance complaints, SLAs and associated damages/remedies, vendor eProcurement fees invoiced, and payments made.
- SPM provides tracking/reporting abilities on vendor performance metrics through scorecards. Performance criteria is translated into key performance indicators (KPIs) that map between SPM scorecards and surveys and prepackaged SPM reports
- SPM enables users to create scorecards, charts and graphs based off the vendor performance data collected. A supplier performance management (SPM) scorecard aggregates information about a supplier to provide an overall score that indicates how well the supplier is performing.
- Supplier performance management (SPM) surveys enable you to record responses from multiple participants, including suppliers. You can run surveys to: 1) Collect qualitative data about a supplier. This data is typically collected from internal stakeholders. Values from text selections (such as Good or Excellent) can be mapped to numerical values (scores). You can also assign weights to survey questions. 2) Collect quantitative data. This data might be collected from either the supplier or internal stakeholders.
- SPM enables the ability to import and export the survey to a spreadsheet. Respondents can also use a Microsoft Excel spreadsheet to respond to a long survey. The project owner can then import the survey responses into SAP Ariba Supplier Management solutions.
- SPM enables the ability to create a new Ariba contract template based on a performance issue of the vendor where performance should be improved. Multiple templates can be created based on the requirements.
- Contract owners, team members with the required permissions and the supplier who is part of a contract can upload multiple documents on the document tab in contract where all documents can be stored by the vendors.
- Purchase order documents can be linked to contracts when the contract number is included and when contract items are procured without the contract number and provide a summary of all spend as the system generates a separate order when requests are created against the

contract and contract details are saved on the line item details of that request. The purchaser can track the spend by opening the contract.

- It allows all users to view vendor performance of all contracts, If a contract is created against Vendor(s) then we can track performance of a vendor from that particular contract.
- It provides the ability to track vendor performance of individual statements of work that are completed from a master agreement (enterprise contract) in the Ariba Master Agreement.
- Buyer/analyst will receive notification when a contractor completes performance but will not provide information about the criteria, it will just notify. The contractor will need to view the project to check performance.
- In SPM, Notifications can be sent to Contractor when they do not meet the performance criteria.
- Supplier performance management (SPM) surveys enable you to record responses from multiple participants, including suppliers and provides the ability to attach documents File size limit is 100MB per attachment to associated vendor performance records.

1.2.2.11 *Purchasing/Data Analytics*

One of the key methods to obtain benefits from the eProcurement system is to identify, track and report on metrics. Our team can help drive benefits through the identification, development, and reporting of key metrics.

The Ariba Strategic Sourcing/Ariba B&I has the capability of reporting. Built-in reporting functionality leverages the procurement transactional data for analyzing and depicting various aspects such as performance, risks and outcomes of the business/suppliers. Buying trends and effective spend management can be done utilizing these reports. Ariba has a set of over 250 pre-packaged reports. Additional reports can be created by modifying pre-packaged reports or creating new analytical reports. These reports can be displayed within the solution on the user's dashboard or exported for inclusion in other reporting applications. The reporting features include the graphical and statistical reporting of the data on the dashboards. The reporting capability is built for ease-of-use and flexibility.

Discussed below are some of the user-friendly features:

- Parameter-based reports to make analysis readily accessible even to new and infrequent users. Creation of multi-measure charts drag and drop capability so users can edit existing reports directly from the field browser or the actual report by dragging and dropping available fields to/from reports.
- Line-level reporting to view line level details.
- Scheduled reports to schedule a report by date, time and frequency that can be cached for performance and quick retrieval.
- Support for alerts and grades to create visual alerts and grades determined by user-defined thresholds and metrics.
- Pivot table user interface, 80/20 filter and flexible grouping of spend across multiple dimensions so users can locate what they need using rapid response analysis, flexible drilldowns, expansion and navigation.

All the Ariba solutions come with their own built-in reporting capabilities. A wide range of pre-packaged reporting on spend analytics is available to track the expenses on supplier, commodity code, organization, particular contracts and orders.

Managing Reports

The Ariba Strategic Sourcing/Ariba B&I has the feature to provide the prepackaged and customized reports as per the user requirement. Authorized users with the designated roles and permissions can run the custom reports in accordance with the required selection criteria.

Browser Based Reporting & Querying

Ariba Strategic Sourcing/Ariba B&I has a browser-based reporting solution for reporting and querying capabilities. Only the authorized users can access and run the various reports.

Reports can be exported from the solution via excel, .csv and .pdf. Reports can also be scheduled to run in the background and emailed to users. The email will include an excel version of the report results.

Ariba Analytics provides the pre-packaged reports for various categories, organizations and suppliers. It includes the spends, detailed reports, contracting details, and anything supplier performance related.

Ad-hoc Reports

Ariba Strategic Sourcing/Ariba B&I provides users the functionality to create personalized reports and save under the personal workspace. Only the authorized users can access the personalized reports. All data captured in the solution and flagged as reportable is available to users Ad-hoc reports. This is true across the source to settle solutions including requisitions, purchase orders, solicitations, contracts, invoices, approvals, catalog usage, etc.

Pre-packaged Reports

Pre-packaged reports provide the feature to track the procurement activities and performance metrics. These reports can retrieve the proposals/responses based on the State of Maine's requirements, including proposals/responses that are related to specific suppliers. These reports can retrieve the contracts with a specific supplier and supplier type. Similarly, for the orders for a specific supplier and supplier type. These reports contain the specific details related to the purchase requests, their attributes, spend details, discounting and pricing details of commodities of the purchase orders and blanket orders. Also, these reports contain the specific reports related to the contracts which are near to expire and whose spend has crossed the threshold value set in the contract. Also, there are contract reports which are about to expire, closed and in published status. These are used to track the contract spend and order spend by organization. Pre-packaged reports provide the ability to track the spend on a supplier work request to P-card and non-P-card.

Pre-packaged reports contain the specific reports related to category specific spend and commodity specific spend commodity specific supplier data, commodity specific contract data, etc.

Analytical Reports

The Ariba Strategic Sourcing/Ariba B&I has access to all of the transactions to run the various analytical reports. Analytical Reporting is a layered reporting feature, a user can have the higher-level reporting and can drill down to get the hierarchical details. Ariba Strategic Sourcing/Ariba B&I also provides the reports on the other non-spend information like commodity codes, procurement types, COA, hierarchies, supplier hierarchies. The spend analysis tool is built on the hierarchical logic. Ariba analytics has the feature to provide the analytical reports in pie, bar and graph representation of the data. These reports can be exported to the external systems. Ariba Strategic Sourcing/Ariba B&I functionality can incorporate federal reporting requirements and can export the files in standard excel, pdf formats and share the reports via email. Ariba Strategic Sourcing/Ariba B&I provides the feasibility to load the external data into the system to have the holistic reports utilizing the available data from the system.

1.2.3 Technical Requirements

1.2.3.1 *Availability*

The core of the eProcurement solution proposed is based on SAP Ariba SaaS application. Ariba Cloud Services are deployed as a true SaaS Model IV solution. Ariba hosts multiple customers on a load-

balanced farm of identical instances, with each customer's data kept separate, and with configurable metadata providing a unique user experience and feature set for each customer. A SaaS IV system is scalable to a large number of customers, because the number of servers and instances on the back-end can be increased or decreased as necessary to match demand, without requiring additional re-architecting of the application, and changes or fixes can be rolled out to thousands of tenants as easily as a single tenant.

As it is SaaS application, the maintenance and upgrade activities are scheduled ahead and would be in non-business hours as per regions. This ensures the maximum system availability during business hours.

The table below maps the key Infrastructure design considerations with corresponding features of the proposed architecture:

Table 7. Availability Design Considerations

Key Design Considerations	Proposed Reference Architecture Features to Satisfy the Design Considerations
Infrastructure Availability	• With our SaaS solution, we have more than 99.5% availability • Redundancy for each system component • Pre-build optimized configuration for performance
Elasticity and Scalability	• Consolidation of instances for better manageability and effective utilization of the resources • Scale-out architecture for Web and App Tier • Scale-up architecture for DB Tier • Use of caching designed to enhance the scalability of applications
Load Distribution	• Load balancer for distribution of workload and instances across availability zones

SAP Ariba uses replication technologies to copy data between data centers within a region. Application of these technologies protects against data loss from a disaster effecting a single site.

Infosys runs redundant copies of all critical software subsystems including application services, enabling automatic fail-over in the event of an error so that there is no disruption of service. Our solution's hardware infrastructure is also implemented with automatic fail-over mechanisms. For further redundancy, the procurement solution is connected to the internet with two different ISPs running through physically separate conduits to the upstream provider.

The following diagram illustrates how redundant systems are maintained in order to achieve high availability desired by State of Maine.

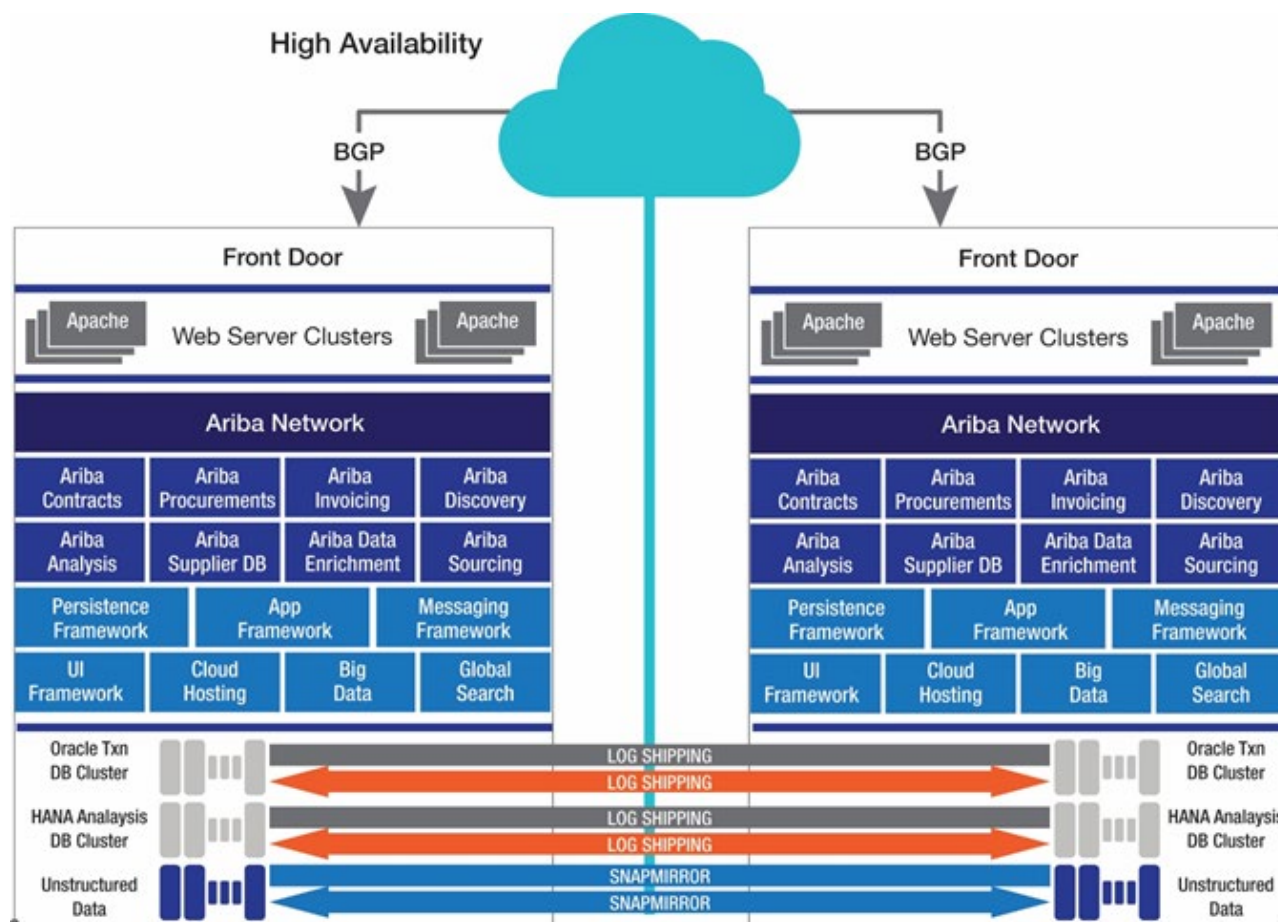


Figure 20. Ariba Redundant System Architecture

Below table provides the overall availability of our eProcurement Hybrid solution components.

Table 8. eProcurement – Overall Solution Availability

Key Components	Availability	Additional Reference
SAP Ariba Solution	99.5%	Please visit SAP website for more details on Service Level Agreement for SAP Cloud Services
Oracle Integration Cloud (OIC)	99.5%	https://www.oracle.com/cloud/iaas/sla.html#aavailability
Cloud Based Portal Solution	99.95%	https://www.acquia.com/products/drupal-cloud/cloud-platform/availability-disaster-recovery
ICAM (Identity, Credential and Access Management)	99.5%	Azure AD – https://azure.microsoft.com/en-us/support/legal/sla/summary/
ServiceNow	99.8%	https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/legal/subscription-service-guide-upgrade.pdf

To ensure the highest availability of the eProcurement solution, we will use best practices such as:

- Frequent systems backup and maintenance

- Redundant systems
- Proactive customer notification of unplanned down-time
- International support coverage

1.2.3.2 *Accessibility Requirements*

The core of the eProcurement solution proposed is based on the SAP Ariba SaaS application.

SAP is committed to delivering software solutions that are accessible to individuals with disabilities and to that end, working towards meeting WCAG 2.0 Level AA. This includes addressing the Electronic and Information Technology Accessibility Standards described in Section 508 of the Workforce Rehabilitation Act. The Americans with Disabilities Act (“ADA”) is a separate law governing primarily Accessible Design for facilities. The Department of Justice home page for ADA (www.ada.gov) Provides a link to Section 508 materials which address, in detail, accessible access to technology. While the solutions proposed implement several accessibility features, they are currently not fully optimized for accessibility. Each of our products has undergone a WCAG 2.0 assessment and at this time most criteria at Level A and AA are either supported or supported with exceptions. Supported accessibility features are provided by SAP solutions in combination with third-party assistive technologies such as the screen reader JAWS. JAWS and most other assistive technologies may require SAP and or customer furnished client-side software.

In addition to SAP Ariba application, the optional Transparency Portal solution provided by Infosys proposed is WCAG 2.0 Level AA compliant.

1.2.3.3 *Audit Trail and History*

Within our solution, specific logging takes place that is viewable by the customer, document owners and users with specific permissions. Audit logs capture information such as the date and timestamp of every action taken on the transaction, user information, content changes, approvals, and rejection of transactions. All this information can be accessed under the History tab of the transaction document and by running the reports. Audit logs produced through use of the solution are considered customer data and are maintained within the customer's instance of the database. These logs are retained so long as the customer has an active contract with us. As a user control consideration, customers are responsible for monitoring the proper entry of data to the solution and reviewing reports generated by the system.

As part of audit compliance requirements, SAP Ariba solutions and the Ariba Network stores information about changes made. Configuration changes, master data changes, and changes related to transactions are recorded for audit purposes. Our solution will use the audit service provided by SAP Ariba to store and retrieve audit information.

Monitor user and supplier activities:

SAP Ariba solutions will track activity for all users, or search for specific users to monitor, in the audit log. To review audit details, a user should be members of the administrator group. The audit log has filters for viewing user activities for specific times, dates, events, or users. SAP Ariba solution comes with the most used filters already enabled including date, effective user, event type, and node. The solution can export up to 10,000 audit log entries to a Microsoft Excel file.

The following table describes the columns on the Audit Log page:

Table 9. SAP Ariba Audit Log

Column	Description
Id	The unique identifier of the action.

Date	The date and time the action occurred.
Event Type	The event type used for categorizing the logged event. The event types are described in the next table. This information is for Ariba internal use.
Real User	The name of the user who performed the action. In most cases, the effective user and the real user are the same user. The effective user and the real user are different users when the real user was acting on behalf of another user when performing the action.
Effective User	The name of the user who performed the action
Description	A description of the action
Customer Site	The name of your Customer site. This information is for Ariba internal use.
Node	The name of the logical node on which the action occurred. This information is for Ariba internal use.
Stack Trace	If an exception occurs, this column shows the part of the code that generated the exception. This information is for Ariba internal use.

The following table describes the types of events tracked on the Audit Log page.

Table 10. SAP Ariba Audit Log Event Types

Column	Description
Admin	Ariba Customer Support administrative actions and events such as site-level administration and service manager functions (for example, User Session and Log Level category)
Admin (tasks/files)	Administrative tasks such as data import and export, file upload and download, and events related to configuration files
Admin AppUtil	Internal solution-level auditing
CDS Sync Verifier	Validation of common data server (CDS) synchronization; provides information about all CDS related activity
Exception	Exceptions that occurred during document processing
General	Events that do not belong in any other event type category listed in this table
Integration	Integration event executions and failures
Parameters	Changes to parameter information
RealmPurge	he RealmPurge task (run by SAP Ariba Customer Service)
SSO	Single sign-on and password adapter activities
SchemaRealmMapping	The scheduled task DBSchemaRealmMappingVerificationTask, which SAP Ariba Customer Service uses to ensure data integrity
Translation	Used for capturing translations for resource names
User Management	Changes to user data, such as changes to group membership or contact information.
User Management (tasks/files)	User management changes made via import tasks.

ICAM Audit and History:

Saviynt provides comprehensive logging and monitoring as part of Audits and History Capabilities. All activities within Saviynt as well as connected applications which share audit data are logged and monitored. The system captures action, timestamp, comments/ business justification in Saviynt database for auditing and compliance purposes. Saviynt also supports versioning of entities (rules, roles etc.) so that owners, administrators, and auditors can closely track the changes and impact. Saviynt optionally provides Identity / Threat Intelligence module to continuously scan for anomalies based on user behavior.

Saviynt application provides an easy way of tracking any changes made to any user record or roles over a period. Any changes made to user records or roles is stored in the Update History for each security object, various versions are maintained for roles that undergo role review / approval process before being formalized. It also enforces 'event-based' triggers where action / review can be automatically invoked as changes are detected. Saviynt also offers Role vs. Actual, Request vs. Actual reports to further determine any disparity of user security between Saviynt and Authoritative Sources

Saviynt Enterprise Identity Cloud (EIC) provides extensive logging of activity in support of a secure information ecosystem. EIC captures every transaction performed by users, privileged users, and administrators, and all data is available for review with out of the box reports and is supported by the analytics module for ad-hoc reporting. Saviynt provides a flexible platform allowing the customer to define what and for how long audit events are stored. Saviynt creates a unique sequence number while generating audit logs that can be used to detect any tampering. Saviynt also supports the ability to send logs to a centralized log management system in real-time for safekeeping.

Audit logs are typically retained online for one year and then archived for six more years. Audit log data is accessible within the EIC using the Analytics module, typically permitted only for Admins, but the retention policy for the logs is only configurable by the deployment team. No EIC user can change the audit trails or order them purged other than on the agreed schedule

1.2.3.4 *Browsers Supported*

The following browsers have more than 10% of the web traffic and are supported by SAP Ariba cloud solutions:

- Apple Safari (64-bit)
- Google Chrome (64-bit)
- Microsoft Edge (32-bit)
- Mozilla Firefox (64-bit)
- Microsoft Internet Explorer (32-bit) until December 31, 2021

The optional custom portal solution for public access to awards will be certified for use with following browsers:

- Apple Safari (64-bit)
- Google Chrome (64-bit)
- Microsoft Edge (32-bit)

Note: Compatibility mode is not supported

SAP Ariba solutions track a user's browser whenever the user logs in. Administrators can view the browser information on the Users page in the User Manager workspace of the administration area. The State of Maine can use the browser information in the search criteria and can export a user's browser information to an Excel file. This will help the State of Maine in analyzing platform trends.

Knowing which browsers are in use helps SAP Ariba work with customers on browser support issues, enabling administrators to prepare for changes. Administrators discover which users are utilizing browsers that SAP Ariba no longer supports.

The SAP Ariba suite is tested for multiple browsers, operating systems, and versions during every release. SAP Ariba shares the details of browsers, OS and versions for every release, enhancement, and fix.

For ICAM Solution - Saviynt Enterprise Identity Cloud (EIC) supports the following browsers/versions:

- Firefox ESR 67 and later
- Google Chrome 75 and later
- Microsoft Internet Explorer 11 and later
- Safari macOS 12.1 and later

EIC also supports HTML5 for compatibility with mobile browsers

For ICAM Solution - Azure Portal Supports the following browsers

- Microsoft Edge (latest version)
- Safari (latest version, Mac only)
- Chrome (latest version)
- Firefox (latest version)

1.2.3.5 *User Accounts and Administration*

The Solution need to manage and authenticate following broad category of users:

1. State of Maine Users – End Business Users
2. Solution Administrators – To manage the solution components
3. Suppliers – Participating Third Party Vendors

Supplier Users will be managed by SAP Ariba Network directly, whereas State End Users and Solution Administrators will be managed by the State's preferred IAM solution.

For Suppliers SAP Ariba User Administration solution will provide for creating, managing, and monitoring the variety of user account types for the State of Maine. This ranges from full access for system administrators to a tiered structure of limited access depending on the user's role. For the user administration requirement, Infosys will leverage the capability provided by Ariba Network administrators, SAP Ariba strategic sourcing and supplier management solutions administrators and SAP Ariba procurement solutions administrators to perform the following:

- Creating new user accounts
- Deleting users when they leave the organization
- Resetting user passwords
- Acting as another user
- Locking and unlocking user accounts
- Monitor user activity

The following table describes the types of tasks that can be performed by different administrators that can create, manage, and monitor user accounts

Table 11. Ariba Administrator Tasks

Administrator Roles	Ariba Network administrators	SAP Ariba Strategic Sourcing and Supplier Management solutions administrators	SAP Ariba Procurement solutions administrators
Tasks	• Reset a user's password • Reassign a user login	• Act as another user • Lock or unlock a user • Generate or reset user passwords	• View user information • Monitor user activities

	• Monitor user access activity • Delete a user • Transfer administration ownership • Assign user management capabilities to users • Prevent Ariba Network buyer users from logging in manually • Track and audit supplier group membership changes	• Deactivate or reactivate a user • Create and manage user delegations • View user activities in the audit log • View or disconnect user sessions • Anonymize personal data for deactivated users • Let non-administrators act as another user	• Act as another user • Lock and unlock a user • Deactivate and reactivate a user • Generate or reset user passwords • Create or end a user delegation • Terminate a user • Anonymize personal data for deactivated users • Let non-administrators act as another user

Access to data and functionality within the modules is based on roles and permissions that determine which features of the solution a user can see and work with, and what data the user can access. The set of permissions for a user is determined from the roles mapped to that user and the groups to which the user may be a member. Permissions are mapped to roles and then roles can be mapped to other roles, to users and/or to groups. Users can inherit roles and their associated permissions by being a member of a group. The combination of groups, roles and permissions allows customers to manage access control in a way that reflects their organizational structures and the roles of users within those structures. The solution provides pre-defined roles and customers can define their own roles.

The solution also provides a single point of integration and administration for users and user profiles, organizations, groups and group memberships, roles, and permission mappings. This common data is shared and synchronized across modules automatically. The User, Group, Role and Permission objects can be managed from the provided UI or populated from a variety of sources, such as corporate systems and/or flat files. For example, the user object can be populated from an external HR system. The application provides capabilities to perform batch upload from the user interface (either through web page based interactive file upload, or via automated (scripted / scheduled) HTTPS push of data from HR and ERP systems. E.g., user profile data (with supervisor hierarchy), user to Group/Role mapping, etc. are accepted.

The user can delegate their approval authority to another user to allow that user to approve requests sent to the delegator. The delegate receives all system-generated email notifications regarding requests that require his/her attention. The user can log in as the delegator and act as the delegator to review, approve or deny requests on the delegator's behalf.

When the delegate receives a notification on behalf of the delegator, the notification mentions the delegation so that the delegate knows why the message was sent.

When acting as the delegator, delegates can approve and reconcile all the documents assigned to the delegator, even if they do not normally have access to those documents. To support audit reporting, if the request is acted upon by the delegate, the name of the delegate is shown in the approval node, followed by the name of the delegator in parentheses.

If you have delegated your approval authority to one or more users, you can stop the delegation manually at any time.

Our solution will leverage Delegation functionality from SAP Ariba Strategic Sourcing and Supplier Management solutions and SAP Ariba Procurement solutions

Our solution can use one of these options to delegate your approval authority:

- Delegating your approval authority to a single user (one-to-one user delegation)
- Delegating your approval authority to multiple users (one-to-many user delegation or multi-user delegation)
- Members of the Customer Administrator and Customer User Admin groups can create delegations on behalf of other users
- Solution can stop the delegation manually at any time

User groups

Groups grant users access to functionality in SAP Ariba Strategic Sourcing and Supplier Management solutions and SAP Ariba Procurement solutions. Roles grant users access to functionality in the Ariba Network. Group membership enables users to perform specific actions in the end-user and Ariba Administrator interfaces. For example, only members of the Customer Administrator group can use Ariba Administrator to import, export, and manage all types of data. SAP Ariba includes several defaults, or system-defined, groups. You can also add custom groups.

SAP Ariba strategic sourcing and supplier management solutions administrators that create and assign groups that reflect the access requirements, job function, and responsibilities of system users. Tasks performed by solutions administrators are: add and modify user groups, view user groups, define subgroups for custom user groups and deactivate or reactivate custom user groups

SAP Ariba procurement solutions administrators create and assign groups that reflect the access requirements, job function, and responsibilities of system users. Tasks performed by solutions administrators are: define custom groups, define child groups for your custom groups, import Punchin groups for catalogs, import user group mappings, define user group mappings, manage groups in Ariba Administrator, rationalizing user and group data in multi-ERP and review your group memberships.

User roles

By creating roles and then adding users to them, administrators can control who can log in to your organization's Ariba Network account and which areas of the service each user can access. Groups grant users access to functionality in SAP Ariba strategic sourcing and supplier management solutions and SAP Ariba procurement solutions. In the Ariba Network, a user with the administrator role can create a role with certain permissions and assign the role to a buyer user. A role defines a user function within Ariba Network, such as purchase order generator. Each role has a unique name and set of associated permissions that specify what users who are assigned to the role can see and do in the Ariba Network. A role can be assigned to any number of users. Ariba Network administrators that create roles that reflect the access requirements, job function, and responsibilities of system users.

Tasks performed by solutions administrators are: create new user roles, modify user roles, reassign users to different roles, change a user's role and delete roles

ICAM Solution (Optional)

The optional component ICAM can be the central dashboard to manage user accounts and related administration. The roles segregation and mapping mentioned above and required by SAP Ariba can be handled by ICAM group mapping. User life cycle including on-boarding, off-boarding, hierarchy can be centrally controlled and enforced by ICAM.

The State can choose to integrate with their existing IAM solution or opt for the optional ICAM solution. The integration connectors will be developed and provided by Infosys. Connectors will enable the Identity's Group to Application role mapping to provide tiered access to SAP Ariba and other applications.

Based on the State's requirement, Infosys visualizes the following Scenarios:

Scenario 1: State IAM Solution:

The State can choose to integrate Solution components with their existing IAM solution directly.

Benefits: Solutions access is in direct control of State IAM Administrators

Assumptions:

1. State's IAM solution supports REST, Web Service and SAML integrations
2. State IAM team will provide required support, resources/servers, and access to configure/enable integration between State IAM and Solution components
3. Infosys will provide connectors and guidance required for integration
4. State will have to on-board Solution Administrators to State's IAM also
5. State IAM team will handle Identity, Credential and Access Management for various applications and instances including Production and Non-Production environments.

Scenario 2: Infosys ICAM Solution:

The State can opt for optional ICAM solution proposed by Infosys for seamless integration with existing identity system but can leverage the same for User Accounts and Administration.

Depending upon State Identity being On-Premises or Cloud, the Infosys ICAM solution is flexible and configurable for both layers.

Benefits:

1. Infosys IAM team will manage the User Lifecycle and On-Boarding/Off-Boarding of Users to Applications
2. Infosys ICAM team will manage the User Access to Applications
3. Solution Administrators will be managed by ICAM solution
4. Infosys will develop, configure, and manage the connectors to onboard users as required including enhancements for the solution
5. Infosys has assumed State IAM Team will provide necessary support for onboarding Users from State IAM Platform to ICAM Solution

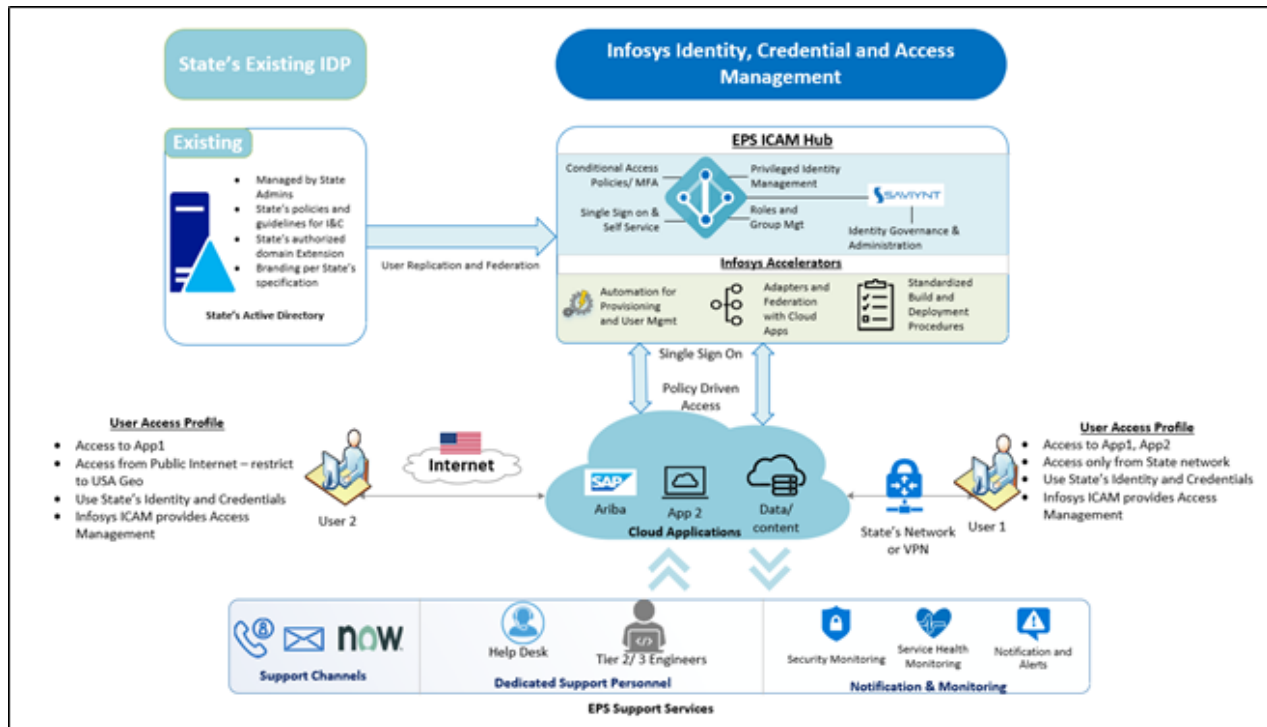


Figure 21. Integration A Integration Architecture of States Azure AD IAM and ICAM Solutionrchitecture of State's IDP and ICAM Solution

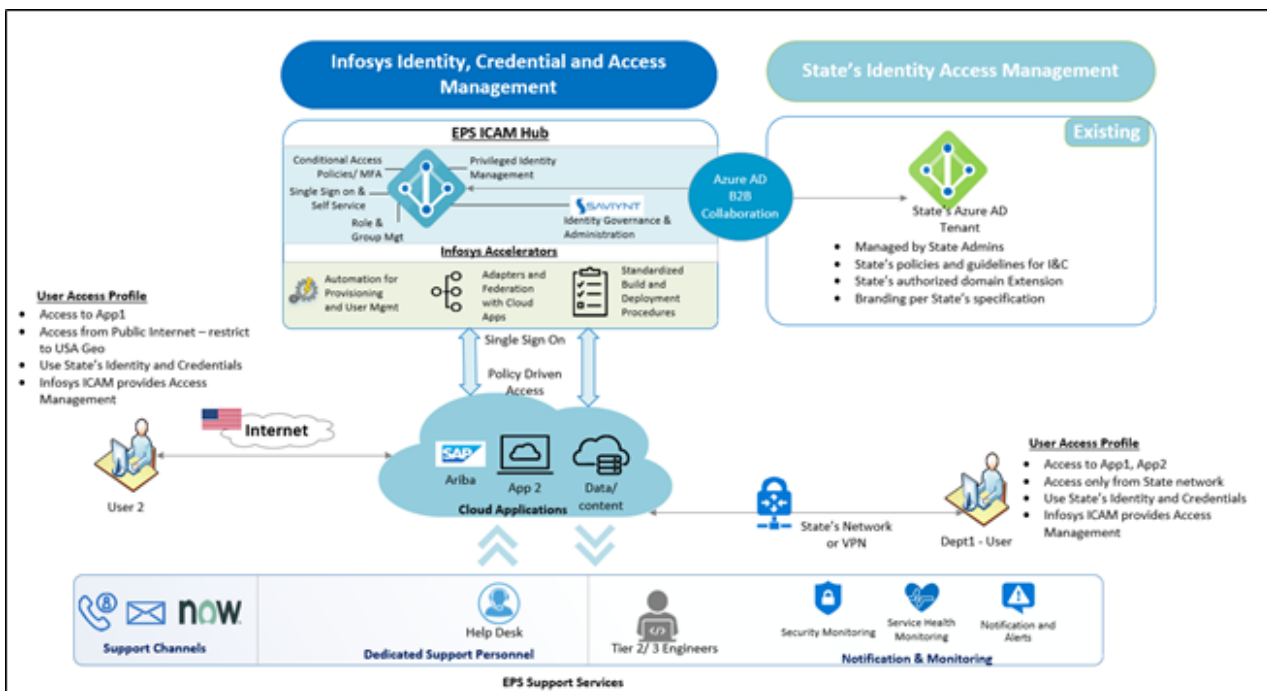


Figure 22. Integration Architecture of States Azure AD IAM and ICAM Solution

Infosys recommendation is to use a SaaS based IGA solution from Saviynt Enterprise Identity Governance for clients that do not have an IAM system for their Users lifecycle management. Saviynt solution provides support for User onboarding, User/Accounts Provisioning/De-Provisioning, Account Reconciliation, and Access Review and Re-certification. Using Saviynt solution, we can achieve comprehensive support for managing multiple User Entities such as State Employees, Agency,

Department, Non-State Entities, and so on. It a robust policy management and governance framework that includes approvals, versioning, SOD analysis and ownership management also, the Identity Governance and Administrations capabilities are delivered out-of-the-box for all the users and include the following services:

- Create account (Ariba, Service Now, Active Directory, other Cloud Apps)
- Enable / Disable Account.
- Modify account (add / remove entitlement, modify attribute)
- Delete Account
- Set password
- Manage AD group lifecycle
- Reconciliation (full and incremental) of applications accounts and entitlement types
- User Access Review and Re-certification
- Audit and Reporting

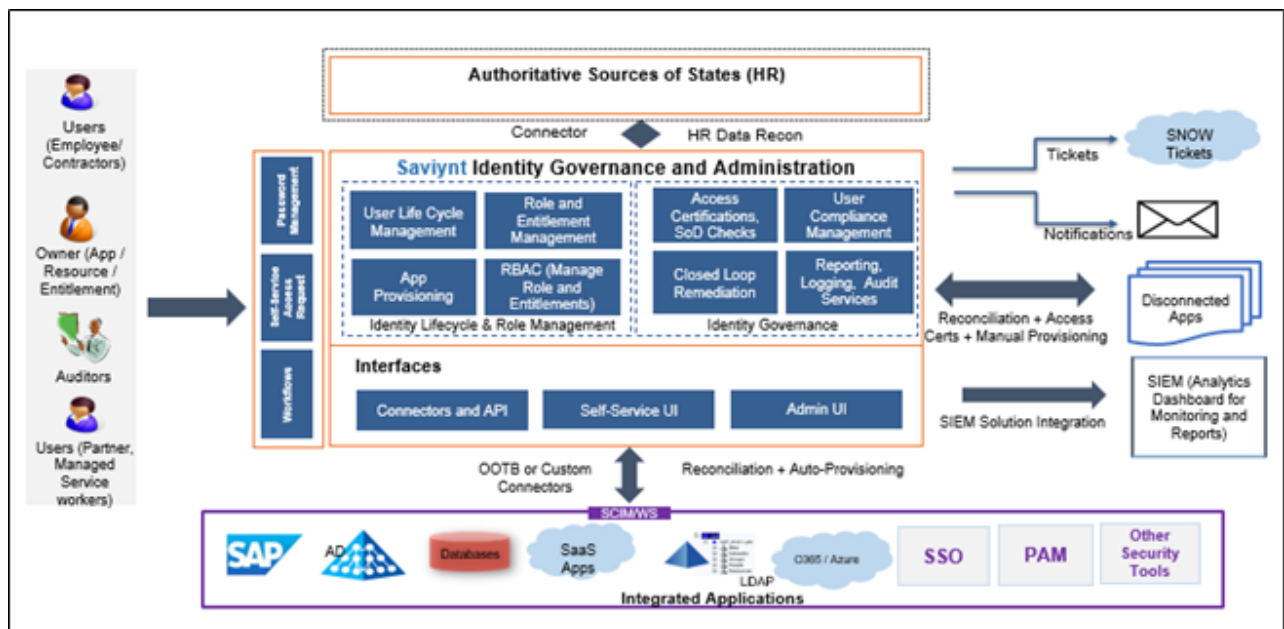


Figure 23. Proposed Reference Architecture of Saviynt IGA Solution

Saviynt - Enterprise Identity Governance Capabilities Includes

- Risk-based Access Certification / Attestation (user manager, role owner, resource / entitlement owner, role content and event-based)
- Enterprise segregation of duty (SOD) assessment and management (risk analysis, risk remediation workbench, mitigating controls)
- Continuous controls monitoring, reports and dashboard
- Out of box compliance controls library and continuous monitoring
- Provisioning / assignment of coarse-grained access
- Task management
- Risk and usage analytics
- Risk-based access certification including closed loop remediation
- Unique active HR identity (employee, and non-employee) common across all applications
- A user can have many 'accounts' in one or more applications

- User will login to Saviynt and perform IGA processes for self and / or others

Saviynt - Enterprise Identity Governance and Enterprise Identity Administration Capabilities Includes

- Risk-based Access Request management (self-service, delegated)
- Automated provisioning / de-provisioning
- Enterprise Role management
- Attribute-based (ABAC) provisioning rules management
- Identity event policy management
- Task Management
- Account and access import / export / reconciliation
- Password management / self-service or delegated password reset
- AD / LDAP group management / governance
- Reporting and dashboard

Identify Proofing

- The Saviynt solution will Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements
- Identity proofing solution will be used for collecting, validating, and verifying a user's identity information for the purposes of establishing credentials for accessing a system. Identity proofing is intended to mitigate threats to the registration of users and the establishment of their accounts
- With Saviynt, the State's users be integrated for identity verification and proofing of their users before allowing users registration or access. Including supervisor or Approver authorization as part of the registration process provides an additional level of scrutiny to ensure that the user's management process and procedures is aware of the account
- Validation and verification of identity evidence increases the assurance that accounts and identifiers are being established for the correct user and authenticators are being bound to that user. Acceptable methods for validating and verifying identity evidence are consistent with the risks to the systems, roles, and privileges associated with the user's account.
- Require that the validation and verification of identity evidence be conducted in person before a designated registration authority.

Manager Approval Workflow

- An approval workflow can then be triggered to perform out of band policy validation, location verification, approvals, etc. prior to creation of the user identity with Saviynt and downstream systems.
- Identity proofing can be handled manually or can be automated in Saviynt through the integration with common Identity Proofing services.
- Saviynt provides out-of-box workflow for managing user life cycle and user access to systems. Also, using Saviynt API's, configuration files, workflows can be customized based on different requirements that State may have for Identity Proofing
- Based on the Saviynt workflow and approval process for Identity evidence, such as documentary evidence reduces the likelihood of users using fraudulent identification

Role Engineering

Saviynt offers the ability to manually create new roles / groups as a self-service function. Group/Role names can be auto created based on a customer defined policy. Saviynt has been built to manage very large volumes of accounts / entitlements / roles / groups and OOTB Analytical controls can help

manage group / role proliferation and can identify unused groups / roles as well as potential duplicate roles and groups.

Access Recertification

Saviynt offers one of the most comprehensive and intuitive Access Attestation/Certification solutions with functionality including closed-loop remediation, integration with usage analytics, dynamic risk/access outlier profiling, and end-to-end auditing with support for various types of certifications listed below:

User Access Certification

- High Privileged User or Critical Access Certification
- Resource Owner Certification
- Role/Group Membership Certification (identities associated with a role or group)
- Role/Group Content Certification (entitlements associated with a role or group)
- Risk-based Certification of outlier access and even activity

Reporting

Saviynt provides built-in analytical and actionable security controls, reports and dashboards which make it easy to deliver the types of information commonly required by auditors, such as how access was requested/granted (birth-right vs access request) and approvals involved etc. The reports are categorized based on managed system (e.g. specific reports for SAP or other ERP system access vs. enterprise access) and type of report (e.g. outlier reports, role reports, SLA reports, etc.) but also by standards such as PCI, CIS, SOC 2 and NIST.

Saviynt provides granular access control on who gets access to various system reports. All reports can be scheduled or executed on demand. Reports can be exported in Excel, PDF and CSV formats. Saviynt roles can be used to grant auditors access to all data or subsets of data in a very easy to use UI enabling them to get the data required easily.

Saviynt provides options to build your own charts based on output derived from various metrics and controls to the report admin. These charts can then be rendered via online dashboards or sent via email on a scheduled basis.

Some of the key analytical and access intelligence report types that are offered include:

- ARS Reports
- Attestation Reports
- Role Management Reports
- SOD Management Reports
- Provisioning/ De-Provisioning Reports
- Specialized Connector Reports
- Entitlement and Account Reports
- Outlier Analysis Reports
- User Risk Reports
- Application Risk Reports

1.2.3.6 *User Authentication*

Suppliers will leverage the SAP Ariba Network native user management. SAP Ariba Procurement solutions support user management tasks including viewing, adding, and modifying users, lock and unlock users, deactivate and reactivate users, terminate users, monitor user activity, reassign user

roles in approvable documents to other users, and manage user passwords and delegations. Every User accessing an SAP Ariba solution is identified by a unique username and will have a valid password. SAP Ariba Procurement Administrators are responsible for actions such as monitoring user activities, resetting passwords, approving user profile changes, and ensures user information is synced between your ERP system and your SAP Ariba solution. Administrators can delegate user tasks in an emergency to another user or prevent a user who has been terminated from accessing your SAP Ariba solution by deactivating the user. Creating users in SAP Ariba Procurement solutions involves a series of definition tasks, which include:

- Importing or manually creating enterprise user information, which includes the user's email address, default currency and locale
- Importing or manually creating ERP-specific user information, which includes the user's default accounting information
- Setting up user and shipping address relationships
- Setting up user and supervisor relationships
- Assigning users to groups which controls which features a user is permitted to use
- Setting up user spend limits (approval limits) per company policies

User information is used in SAP Ariba solutions as follows:

- To uniquely identify the users and authorize them to perform certain tasks.
- To facilitate the automatic generation of approval flows based on approval limits, group memberships, and supervisor information.
- To include contact information such as shipping and billing addresses on purchase orders sent to suppliers.
- To default accounting information in approvable documents so that purchases can be tracked and reported correctly.
- To populate choosers that allow users to search for and easily find other users, for example when adding a watcher or additional approver to an approvable document

The audit log records activities related to user creation, activation, and deactivation. In addition, if there is any change to a user's personal data (contact data such as name, phone number, or email address), the change is recorded in the audit log.

Users can log in using one of two authentication methods:

1. Regular user authentication. Users have configured usernames and passwords that they manually enter on the login page.
2. Single Sign-On. Users log into their corporate network, which automatically logs them in to their SAP Ariba applications when needed. SSO with corporate authentication requires State of Maine's network administrator to enable communication between State of Maine's user authentication system and the SAP Ariba applications.
3. Federated Single Sign-On: SAP Ariba solutions can also be integrated with 3rd Party Identity Access Management solution such as Azure AD for SSO and MFA
4. State of Maine may activate external federated authentications if they use SAML based authentication or ADFS for accessing the SAP Ariba Cloud Services.

Regular user authentication:

With regular user authentication, usernames and passwords will be maintained by the Ariba Administrator. The Ariba Administrator generates temporary passwords for new users and sends new users an email message with instructions for logging in. New users are immediately taken through the password reset process when they log in for the first time

2-Factor Authentication (2FA):

In SAP Ariba, multifactor authentication provides an additional level of security to logins by providing users the ability to authenticate themselves using an authentication factor in addition to their username and password. In SAP Ariba can enable multifactor authentication for both individual users and user groups. When enable multifactor authentication for a group, all users in that group can start using multifactor authentication. Multifactor authentication can be enabled only for accounts that do not use corporate authentication with single sign-on. In addition to enabling and disabling multifactor authentication, you can manage multifactor authentication by performing actions such as unlocking user accounts that are locked due to invalid sign on attempts, as well as sending reminder emails to users who have not set up multifactor authentication, among others.

In addition to enabling multifactor authentication from the user interface, you can enable multifactor authentication for new users by importing the users using the Import Enterprise Users data import task, which has been enhanced to support multifactor authentication. This is useful for enabling multifactor authentication for multiple users simultaneously, without the need for additional administrative action. Similarly, you can enable multifactor authentication for new groups by importing the group using the Import User Group Mapping data import task. All administrative actions related to multifactor authentication are logged. The log entries can be viewed in the Audit Log page of the Site Manager workspace.

After multifactor authentication enabled for user accounts, the users need to set it up the first time they sign on. Once initial setup is completed, users can sign in securely to their SAP Ariba solutions by providing the verification code from their mobile devices during the login process after entering their username and password credentials. Users have the option of choosing to be remembered on a specific device by checking Remember Me on the multifactor authentication page. This will be valid for a limited time period, which can be set.

Single sign-on with corporate authentication

In States where single sign-on (SSO) with corporate authentication is set up, a user can sign in with one username and password to access multiple applications, including SAP Ariba Procurement solutions and SAP Ariba Strategic Sourcing solutions.

SSO systems store user credentials for multiple applications and automatically submit those credentials on behalf of users when needed. Users log in once, rather than re-logging in with a separate set of credentials for each application they access. SSO with corporate authentication can also provide centralized control and enforcement of corporate authentication policies.

To use SSO with corporate authentication, your network administrator must enable communication between your user authentication system and your SAP Ariba solution.

Logging and Monitoring: The customer assigns one or more Customer Authorized Administrators to oversee activity within the system. The Customer Authorized Administrator(s) assigns and maintains login ID's and user permissions and can view and manage administrative tasks within the system. The task and role-based workspace in the administrator console assists in easy and efficient management. Administrators have the authority to terminate a user access to the system as well. Monitoring of account activity and associated reports is a user control consideration.

When Single Sign on is used, password was not stored in the SAP Ariba application, all password rules and changes are maintained and managed by State of Maine change policy.

If Single Sign on was not setup and password was maintained in SAP Ariba solution, then the following password rules are applicable.

Password Policies: A password complexity scheme is in place and mandates case-sensitivity between 12 and 32 characters in length. Passwords can include any Latin characters and punctuation

marks and must include at least one numeral between the first and last character. They must also include at least one letter. The technology is configured to require users to change passwords at least every 180 days. The password complexity scheme applies to all systems. Password complexity and change management is technically enforced where feasible or testing is performed for compliance. The out-of-the-box prior password parameter is that no one password can be reused for four password change cycles. This count can be customized to be more or less than four if needed. Lock out occurs after five failed attempts to log in. Once logged in, session timeout occurs at 120 idle minutes. Both of these parameters cannot be customized.

For authenticated users in the SAP Ariba application, password management involves generating and resetting temporary passwords by the Ariba Administrator. Password settings control password expiration, password expiration notification, how frequently a user can reuse a password, password length, password security questions, and lockout periods. The following table describes the default password parameter settings and indicates which settings can be modified for your site by Customer Support.

Table 12. SAP Ariba Password Policies

Setting	Description	Default	Customer Support Can Modify
Password expiration warning period	The number of days before a password is about to expire that users are sent a warning message.	14	Yes
Generated password expiration period	The number of hours a temporary password remains valid after being generated by an administrator.	720	Yes
Generated password reset expiration period	The number of hours a temporary password remains valid after it is reset by an administrator.	720	Yes
Forgotten password expiration period	The number of hours a temporary password remains valid after a user enters a valid username on the Forget Your Password? page.	24	No
Password reuse limit	Restricts password reuse. For example, when the setting is 4, users are not allowed to reuse any of their last four passwords.	4	Yes
Password pattern matching feature	When set to Yes, passwords must contain at least one uppercase character, one lowercase character, and one digit.	Yes	No
Maximum password length	The maximum length, in characters, for passwords.	32	No
Minimum password length	The minimum length, in characters, for passwords.	12	No
Minimum security answer length	The minimum number of characters users must specify when creating an answer to their password recovery secret question.	5	No

Setting	Description	Default	Customer Support Can Modify
Maximum security answer attempts	The maximum number of incorrect answers users are allowed to their password recovery secret question before being locked out of the site.	5	No
Lockout period	The number of minutes a locked-out account is inaccessible before it is automatically released.	120	No

ICAM Solution (Optional)

The ICAM solution will provide all of the user authentication requirements as mentioned. The ICAM solution can be configurable and customizable as required. MS Azure based ICAM can be integrated with SAP Ariba.

To enable Single Sign-On (SSO) with SAP Ariba, Oracle Integration cloud and others, Applications can be integrated with SAML, and AUTH0 based Identity and Authentication System.

The solution components can be integrated with an IAM of the State's preference to provide authentication to the solution administrators and the State's end users.

Based on the State of Maine's existing setup and preference, we can use the following scenarios during deployment:

1. State of Maine's existing IAM: In this case the applications are integrating directly with State's existing IAM solution. So, the user authentication will inherit the State of Maine's existing authentication policies including password policies, multifactor authentication, logging and monitoring at the IAM level, SSO and identity proofing. User authentication and SSO will be controlled and managed by the State of Maine IAM administrators as per the State of Maine's existing guidelines.
2. Infosys Proposed ICAM Solution: Infosys' recommendation is to use a SaaS based Microsoft Azure AD Solution. Azure AD provides secure user authentication supported by Identity Governance from Saviynt make this a robust and reliable platform to rely on. The ICAM solution will:
 - Develop and provide architectural and implementation configuration standards for authentication and password maintenance with password protection, Azure AD seamless single sign-on (SSO), self- service password reset, password writeback
 - Develop and provide architectural and implementation configuration standards for Azure AD Connect with password hash synchronization (PHS) or pass-through authentication (PTA)
 - Develop and provide architectural and implementation configuration standards for dynamic and self-service group membership, automatic license assignment, access reviews
 - Develop and implement Azure AD identity based conditional access policies requirements to add user accounts to Azure AD security groups

- Leverage existing password policy from the State and authentication will be passed to State's identity solution. Design and configure Azure AD functions to add user accounts to Azure AD security groups for Azure AD password reset
- Provide multifactor authentication. Develop and provide architectural and implementation configuration standards for multi-factor authentication (MFA)
- Develop and provide architectural and implementation configuration standards for dynamic and self-service group membership, automatic license assignment, access reviews.
- Have out of box and custom developed connectors depending on the supporting applications to provide SSO and user provisioning
- Provide a comprehensive view of activity in your environment. The provided data enables you to:
 - Determine how apps and services are utilized by users
 - Detect potential risks affecting the health of the environment
 - Help troubleshoot issues preventing your users from getting their work done
 - Capture and retain logs for required period by moving to supporting storage account or SIEM solution
- Use conditional access policies to identity signals as part of access control decisions

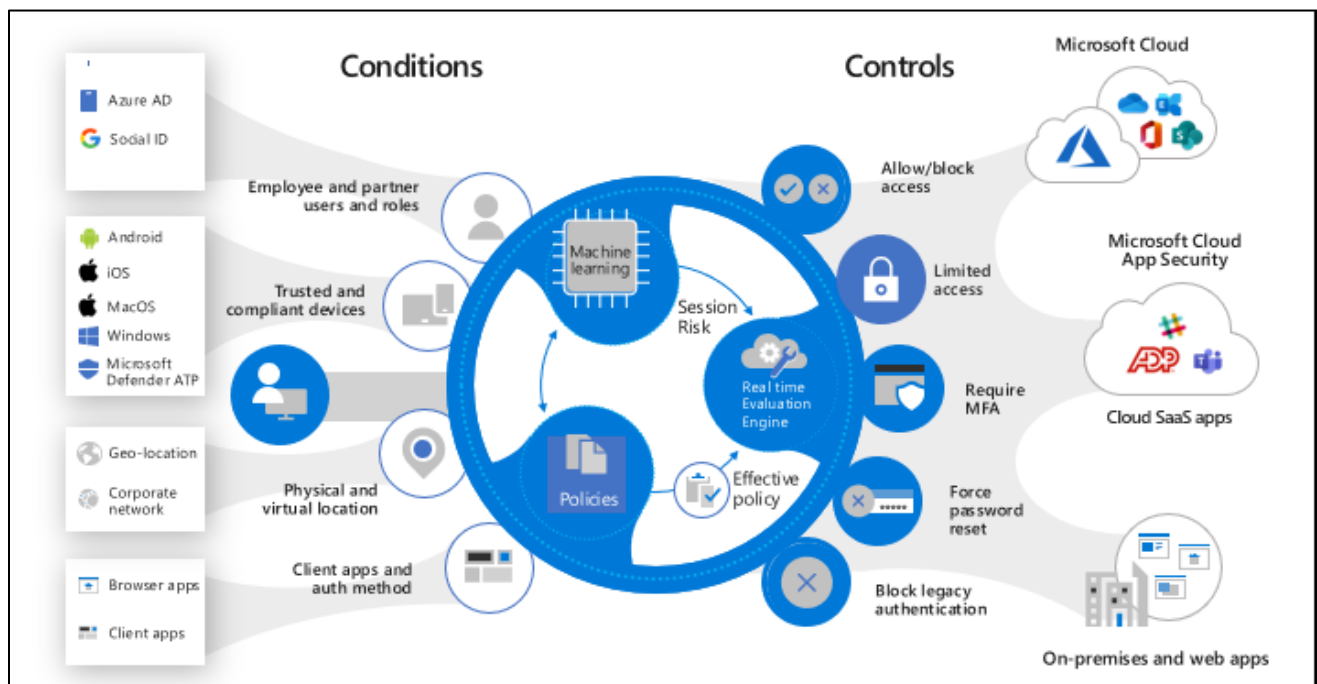


Figure 24. Azure AD Authentication and Conditional Access Policies

1.2.3.7 Federated Identity Management

As mentioned in previous sections, the State of Maine will have the option to choose the IAM solution as in State of Maine's existing IAM or the proposed optional ICAM solution by Infosys.

Option 1: If the State of Maine uses its current IAM Solution: If the State of Maine has own Identity Access Management (IAM) solution, we will leverage State of Maine's IAM solution for Integration with

the SAP Ariba eProcurement Solution (Service Provider) and Other Portal solution (Service Provider) with States IAM IDP (Identity Provider) leveraging protocols such as SAML, OAUTH. Partner states are not part of the State of Maine network, will work using their own corporate devices and access the State of Maine's SAP Ariba eProcurement Solution using own IdP with the trust established via SAML, OAUTH federation that needs to be configured.

Option 2: If the State of Maine uses the new Infosys ICAM Solution: If the State of Maine uses the Infosys ICAM solution, we will leverage Infosys ICAM solution as an IDP for State of Maine Users. With this solution we will integrate the State of Maine's SAP Ariba system (Service Provider) with the Infosys ICAM Solution (Azure AD as an Identity Provider) to provide access to the State of Maine users. For Partner states user's, the same ICAM solution would be integrated with Other States own IdP via SAML, OAUTH federation to enable access to the Partner's States.

The second option proposed, (ICAM solution) is a centralized user identity, credential and access management leveraging industry-leading cloud-based identity solutions that are FedRAMP compliant components.

This ICAM solution will manage the full identify lifecycle and can stand on its own or easily integrate with the State of Maine's user identity directories and identity management solution. It can be federated and will provide the system's centralized administration and synchronization of user identities to enable user provisioning and de-provisioning of identity and access directly from the Participating Entity's systems. The State of Maine's identity authentication will be leveraged eliminating multiple set of credentials for the same user's ID in case of non-federated environment.

Infosys proposes to use Azure AD B2B collaboration that has a new set of capabilities that enable simple and secure collaboration with the business partners. Azure AD B2B collaboration is easy to configure with simplified signup for partners of all sizes even if they do not have their own Azure AD via an email-verified process. It is also easy to maintain with no external directories or per partner federation configurations.

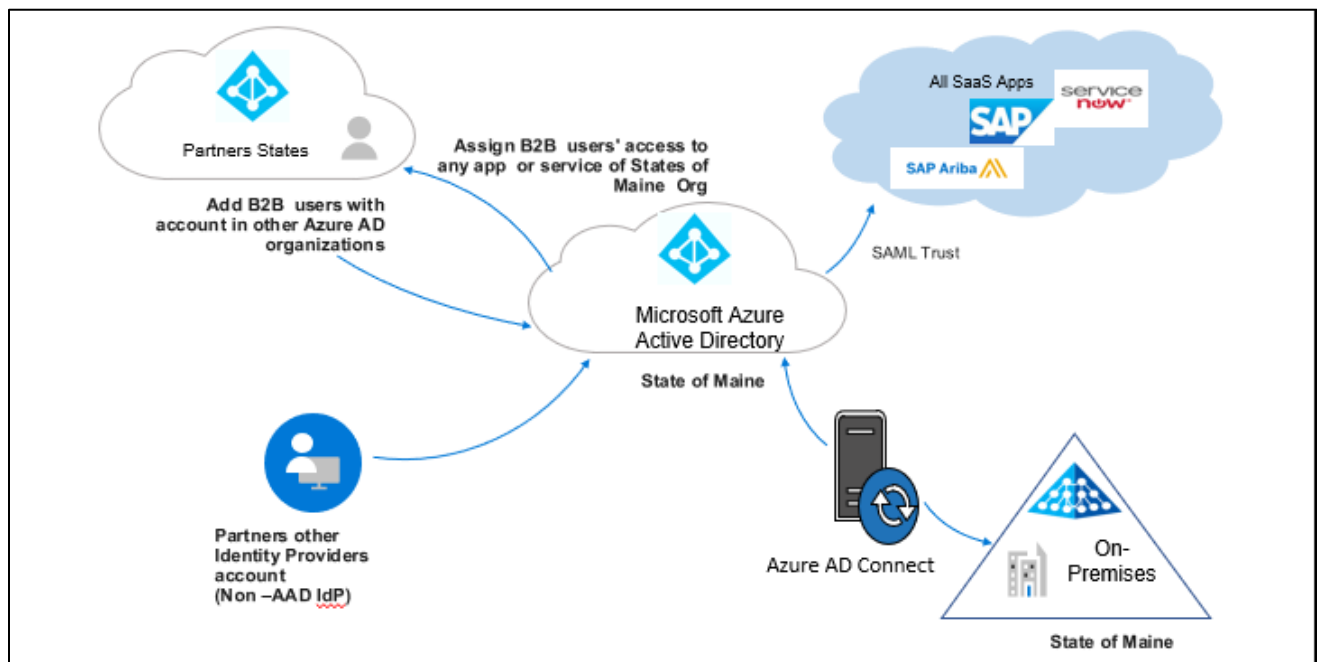


Figure 25. On-Premises AD, AAD Connect and Azure AD Federated SSO Solution

Additionally, the partner companies or people who need access to the State of Maine's applications do not need to have a State of Maine provided User ID. Azure AD B2B collaboration provides a simple

user signup experience to provide these partners with immediate access to the State of Maine applications

Here, each partner user uses an existing Azure AD account or any other IDP. The State of Maine can provide this user with access to the chosen corporate applications (Ariba, ServiceNow, Cloud Apps). The partner user exists in the State of Maine's Azure AD as an external user, where the IT professionals can provision licenses, assign group membership, and further grant access to corporate applications through the Azure portal or PowerShell just like for users available within in the State of Maine. The security team controls all access to the State of Maines applications through the State of Maine Azure AD. When collaboration is terminated, partner users can be removed from State of Maine's Azure AD and their access to the applications is immediately revoked.

1.2.3.8 Data Conversion

The following data migration activities will be followed for the data conversion. This approach is iterative in nature and will be aligned to the overall project plan.

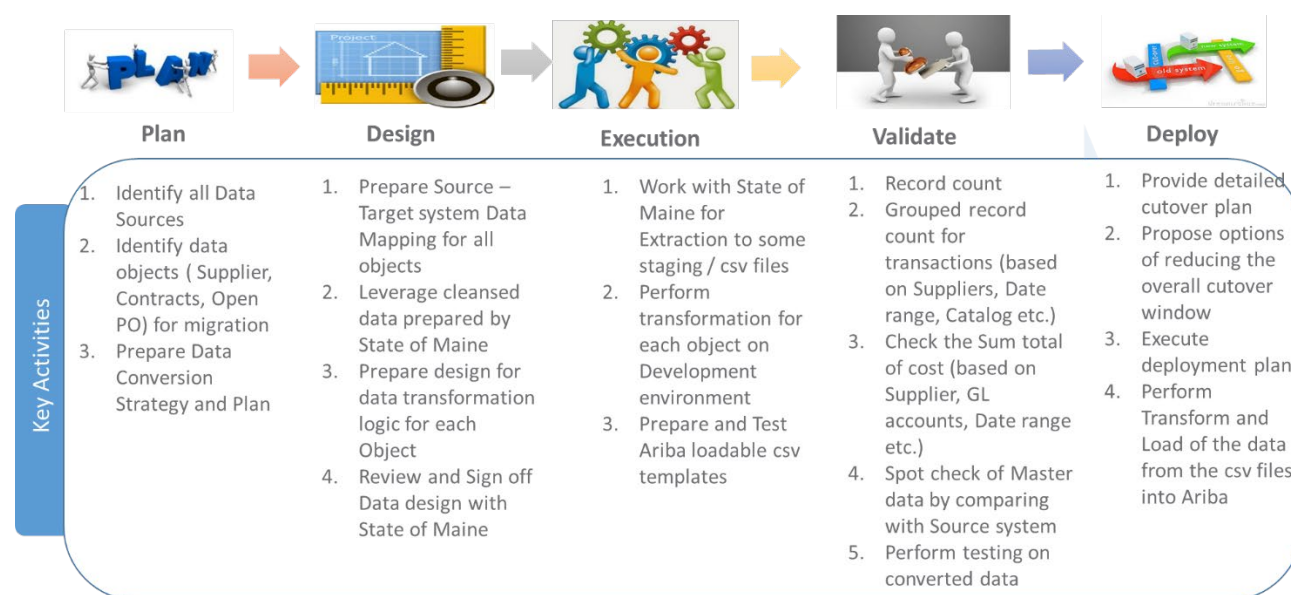


Figure 26. Data Migration Approach

Plan

The project team will conduct a review to understand the minimum acceptable data requirements to operate Source to Pay business functions. The output is a strategy document which will be prepared considering the data requirement, retention policy and legacy system archival strategy to finalize the historical data requirement. After identifying the scope, the next step is to analyze the source data.

The stage involves evaluation of data quality, performing data profiling, identify problem areas, errors and priority of the data requirements.

Infosys will leverage our NIA tool to reduce manual effort and provide quality results. We will also collaborate with State of Maine team and determine the extraction process, cleansing rules (automated / manual).

NIA ETL is Infosys proprietary tool which helps in ingesting, managing, cleansing and transforming data from any source system, this tool will meet the requirement on the data transformation/conversion of any data set (open purchase order, Invoice data, contract meta data and supplier master data) for the State of Maine.

Infosys Nia ETL is an Artificial Intelligence platform which collects and aggregates organizational data from people, processes and legacy systems into a self-learning knowledge base and then automates repetitive business and IT processes, freeing up human effort to solve higher-value customer problems that require creativity, passion, and imagination.

Infosys Nia Data ETL supports an intuitive web interface for building data workflows, enabling data transformation and then publishing the data across on-premise data stores in real time or batch.

Often, one of the main goals of performing a data conversion/migration is to combine multiple data sources into one standardized format. This is referred to as normalizing data. It offers data engineers an integrated environment for scheduling, managing and monitoring complex enterprise data workloads. The platform supports multiple data adaptors like Oracle, Postgres, SQL server and others to connect and ingest data from. You can upload multiple files into the system by creating different data sources.

Infosys NIA ETL can help with the data transformation provided the file is received and given back in CSV/Excel format)

Design

Data Mapping

The data mapping activities will be mainly to map below entities

- Fields in Ariba and can be directly mapped to legacy fields /other legacy data source
- Fields in Ariba, but not in legacy systems. These fields can be derived based on functional discussion and added in the transformation logic
- Fields not in Ariba, but available in legacy systems. A few fields could be relevant based on the new process and would be mapped and non-relevant fields will be left behind/archived

Ariba out-of-the-box fields will be used as the base for data mapping. The advantages of the approach are that it encourages usage of OOB functionality, only relevant fields based on new process and system will be mapped and it will help drive decision to eliminate /purge unwanted data. The high-level steps will be as follows:

- The team will prepare a list of all relevant Ariba fields plus additional fields based on the process.
- With support from the State of Maine team, the data between the Ariba and legacy fields will be mapped.

Development: ETL and Transformation:

The high activities for NIA ETL set up are as below:

1. Once the data is extracted by the State of Maine team, we will import the extracted source tables and fields from the database or file
2. We will create transformation and filter rules. The rules may involve:
 - The date range details from when the data needs to be migrated.
 - The new statuses (open or closed), default data, data enrichment that may need to be considered while migrating.
 - The sequence numbers that need to be generated for any mandatory fields.
 - The default or initial values that needs to be populated for mandatory fields in the target system.
3. The transformed data will be loaded into an Ariba upload able csv format
4. A detailed reconciliation of the source and target data is automatically provided

Execution

Data Load

Once we have Ariba loadable csv templates, SAP plans to leverage SAP's Activate Methodology. Built on our experience from tens of thousands of SAP projects, the SAP Activate methodology provides pre-built implementation content, tools, best practices and migration accelerators that help SAP Ariba deliver consistent and rapid migrations across industries and Customer environments. The SAP Activate methodology for cloud implementations provides an implementation framework to support subscription-based software where the system installation and management occur outside of the project ("Software-as-a-Service" or SaaS). It is less intensive than a traditional project methodology making it ideal for smaller project teams. This methodology is easily integrated with larger, on-premise projects to create a hybrid implementation approach with a single agile methodology.

The data load in Ariba is performed as shown below:

- Files are provided to Ariba in csv file format from the NIA transformation tool;
- Mapping is done to match external files to Ariba fields (target system);
- These files are loaded in Ariba by running import tasks in Ariba that are provided.

The below diagram illustrates the data load approach for Ariba from any external system.

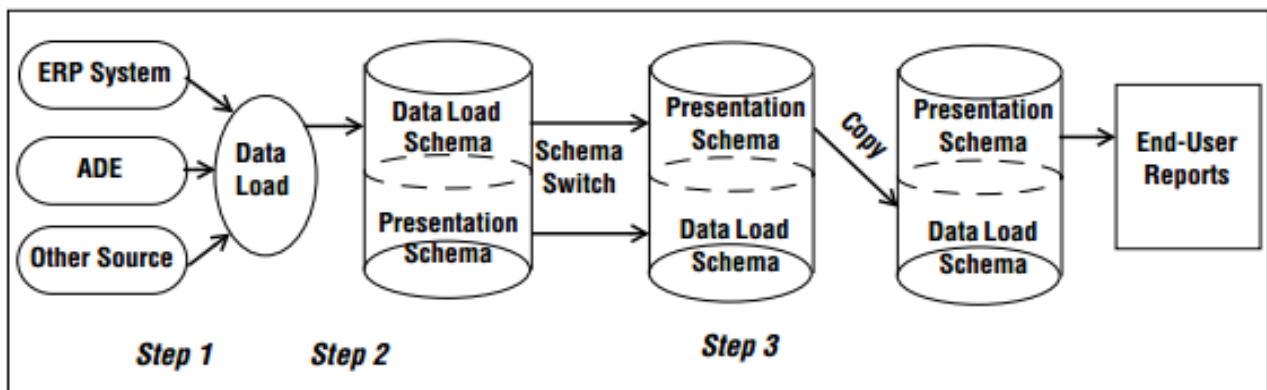


Figure 27. Ariba data load

The high-level Data conversion architecture is given below:

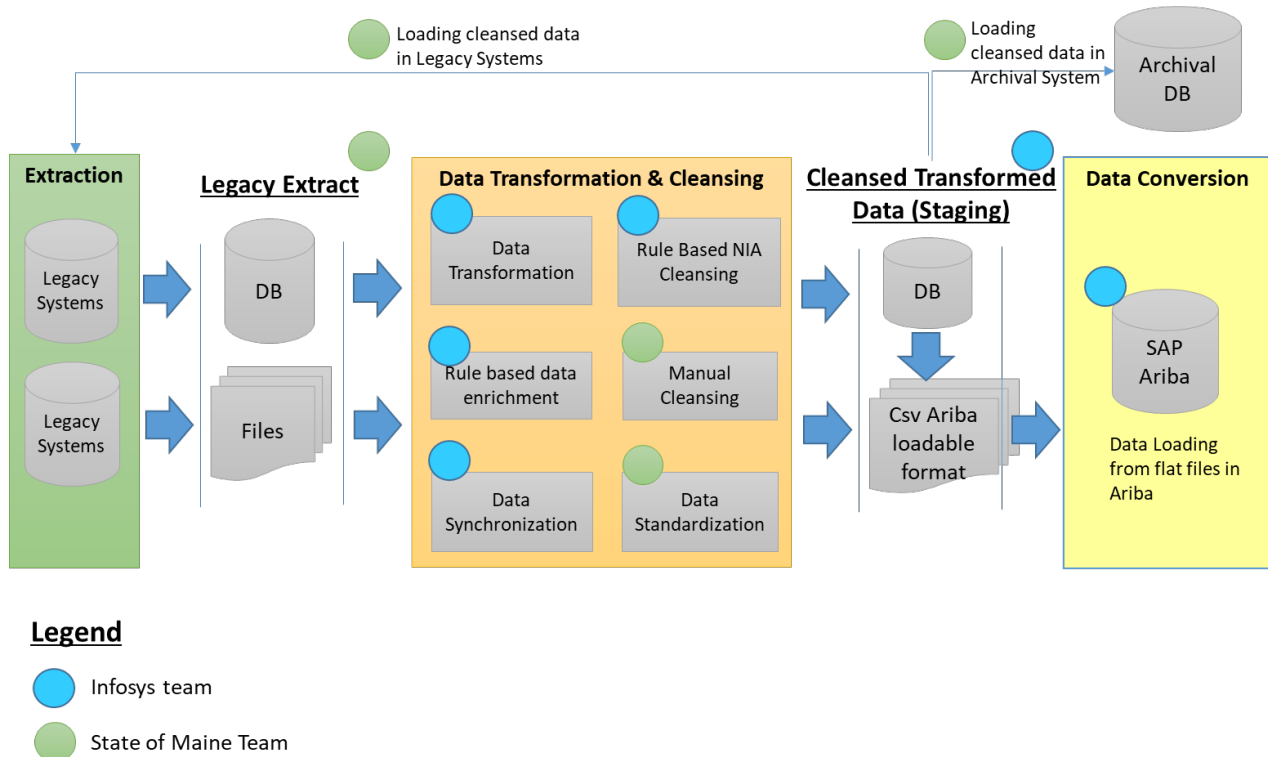


Figure 28. Data Conversion landscape

Validate

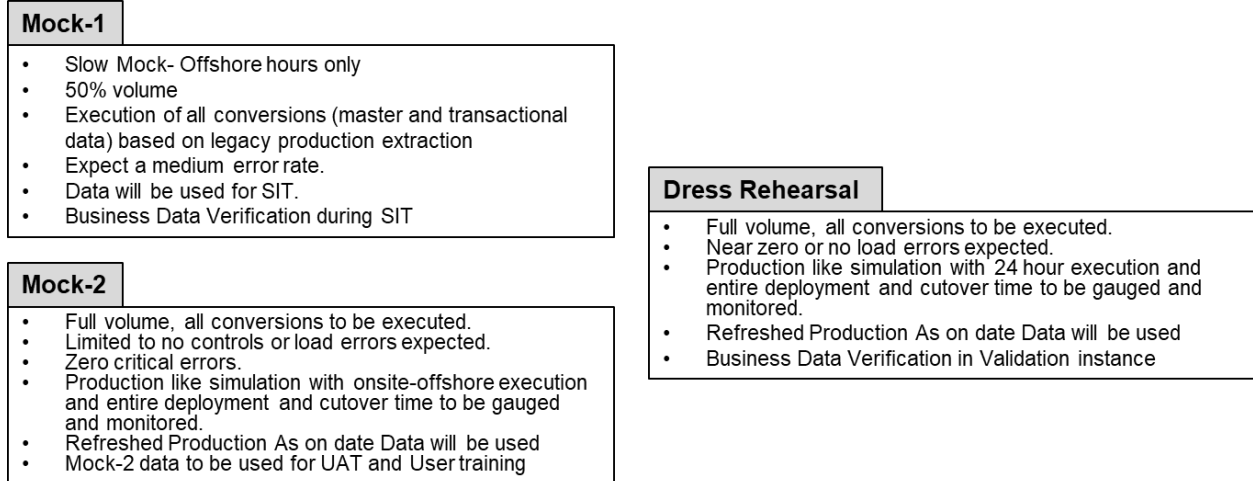
Infosys understands the data involved and has structured our data validation approach to provide an effective validation of the data migration process. The data validation approach followed is focused on early validation. The validation would be performed at the following layers:

- At data extraction from source systems to landing area
- At transformation of data into staging area
- At pre-target area, before the data is loaded into target systems

The following validations are performed at the various stages:

- **Data Comparison:** This involves sample (different variants) data comparison of legacy and Ariba fields.
- **Technical Reconciliation:** This involves comparing source, staging and target count of records migrated, grouping by status, grouping by department.
- **Business Reconciliation:** This involves comparing converted sums like Contract cost, PO Cost, Invoice Cost.
- **Front End Testing:** Unit Testing, System Testing and User Acceptance testing would be performed on converted data during various phases including end-to-end use cases and day in life.

Data Testing Mock Runs/Dry Runs: We will have numerous mock runs of individual objects in development environments before the data can be used for testing. In addition, there will be 3 complete data mock runs, 2 dry runs of data migration before Go-Live. The mock run and dry runs for data migration will be a simulation of cut-over activities. The output data from each mock will feed the system integration testing, user acceptance testing. A complete production run will be performed over a weekend. The electronic production data migration will be targeted to complete in 12 hours or less.

**Figure 29. Data Testing Mock Dry Runs**

Reconciliation roles and responsibilities

Table 13. Reconciliation responsibilities

Activity	Activity Detail	Responsibility
Technical Reconciliation Activities	Identify technical reconciliation points across the end-to-end migration process.	Infosys
	Perform reconciliation checks post the data transformation activities,	Infosys
	Verify the records uploaded to Ariba and produce record counts	Infosys
	Produce count reconciliation reports as agreed and deliver to relevant stakeholders	Infosys
	Should there be any discrepancies in the technical audit and reconciliation reports (record counts), coordinate with data team for appropriate actions.	Infosys State of Maine
	Where applicable data integrity scripts should be run, in particular for assets and locations. These scripts should verify that there are no orphans and that the parent child relationship is intact.	Infosys
Business Reconciliation/ Data validation activities	Data validation through field level comparison of Ariba screens with legacy field.	Infosys State of Maine
	Data Validation through legacy reports comparison with similar reports generated from Ariba	Infosys State of Maine
	Identify the business reconciliation to be used	Infosys State of Maine
	Assist the analysis of discrepancies discovered during dress rehearsals and cutover.	Infosys State of Maine
	Perform business reconciliation checks as defined and agreed for each stream.	Infosys State of Maine
Testing	System testing of migrated data	Infosys

Activity	Activity Detail	Responsibility
	Mock run testing	Infosys State of Maine
	User acceptance testing on migrated data	State of Maine
Sign off and Approvals	Approve the error correction approach during cutover.	State of Maine
	Provide sign-off for each reconciliation report delivered.	State of Maine
	Provide overall sign-off for all the data migrated.	State of Maine
	Provide support to resolve the issues identified during the reconciliation / data validation process.	Infosys

Tools and Accelerators

Infosys will use tools to accelerate the data cleansing and conversion activities. The deployment of these tools and accelerators will help the State of Maine meet the proposed schedule without compromising quality. The key accelerators are described below:

Table 14. Data Migration Tools and Accelerators

Phase	Accelerator	Description	Benefits
Design	Pre-built data Map templates and Questionnaires	Predefined questionnaires and data maps are used to quickly and consistently gather data related information.	- Faster data mapping facilitates - Questionnaire would be tailor made and reused for all Ariba data sources - These are Infosys data map templates that show Ariba on one side and the source database on other. We can use these templates to fill the source side easily
Build and Unit test	Data Transformation = NIA	One Click Tool to transform data	- Reduces the overall data migration and validation effort by 50%. - Data loading can be carried out even by a less skilled resource as no additional scripting is required. Just the data needs to be brought in.
Test	Data validation and reconciliation with NIA	- Data validation scripts helps in expediting the audit and reconciliation - This tool help in finding out record or attribute level differences after data load into target system.	- The data load and pre and post validations results are persistent which can be used to plan for future loads. - Reduction in effort up to 70% in performing data reconciliation after data load into target.

RACI Matrix- Responsible, Accountable, Consulted and Informed Matrix

Table 15. Data Conversion RACI Matrix

Activity	Deliverables	Responsible	Accountable	Consult	Inform
Data Integrity/Quality Issues	Issue tracker	State of Maine	State of Maine	Infosys	
Rule based Data Cleansing	Cleansed legacy data	State of Maine	State of Maine	Infosys	
Manual data Cleansing	Cleansed legacy data	State of Maine	State of Maine		Infosys
Legacy Data Extraction into CSV format	Data extraction	State of Maine	State of Maine	Infosys	Infosys
Mapping sheets for Legacy and Other Legacy/Ariba	Mapping sheets for legacy and other legacy and target Ariba	Infosys	Infosys	State of Maine	
Provide legacy source field information for mapping	Mapping sheets for legacy and other legacy and target Ariba	Infosys	State of Maine		
Provide target Ariba field information for mapping	Mapping sheets for legacy and other legacy and target Ariba	Infosys	Infosys	State of Maine	
NIA Job Mapping, transformation, session & w/f	Job packages	Infosys	Infosys	State of Maine	State of Maine
Migration of Legacy & other legacy system Data into Ariba	List of data issues and streamlining data mapping and job packages	State of Maine	Infosys		
Technical validation (Data)	Unit and system test scripts & results, reconciliation report	Infosys	Infosys		State of Maine
Business validation (Data)	Business validation test results	State of Maine	State of Maine	Infosys	
Mock & Dry run	Mock/DR run results and report	Infosys	State of Maine		
Cutover Strategy Planning	Cutover strategy document	Infosys	State of Maine		
Production Data migration	Data migration report	Infosys	State of Maine		
Data Validation (Prod)	Business validation report	State of Maine	State of Maine	Infosys	
Post migration issues	Issue tracker with resolution	Infosys	State of Maine		

1.2.3.9 *Interface and Integration*

Proposed Solutions must provide both interface and real-time integration capabilities. Proposals must provide complete technical details on these capabilities including, at a minimum, standards supported, restrictions, and identify all Finance systems/ERPs where the Solution has existing interface/integration capabilities available.

Response requirement:

- RTM: Tab 4, TECH-35 through TECH-59
- Inline Narrative: Bidders must provide a detailed narrative response that describes meeting the Interface and Integration objectives and requirements.

Infosys has proposed the Oracle Integration Cloud (OIC) as the middleware to provide real-time and batch integration capabilities for the State of Maine.

Following guiding principles were considered while proposing OIC for the State of Maine's integration requirements.

Table 16. Oracle Integration Cloud Guiding Principles

SL No	Guiding Principles	Comments
1	Secured On Premise Connectivity	OIC has an lightweight agent which connects to on-premise Systems. State of Maine's current people soft system is on-premise.
2	Rich Adapter Capabilities	OIC has inbuilt Ariba & PeopleSoft adapters for making quick & reliable connections with the State of Maine's applications
3	System Availability	Auto scale up, provisioning, back-up, upgrades, and patch updates
4	Loosely Coupled	To handle State of Maine's future integration needs

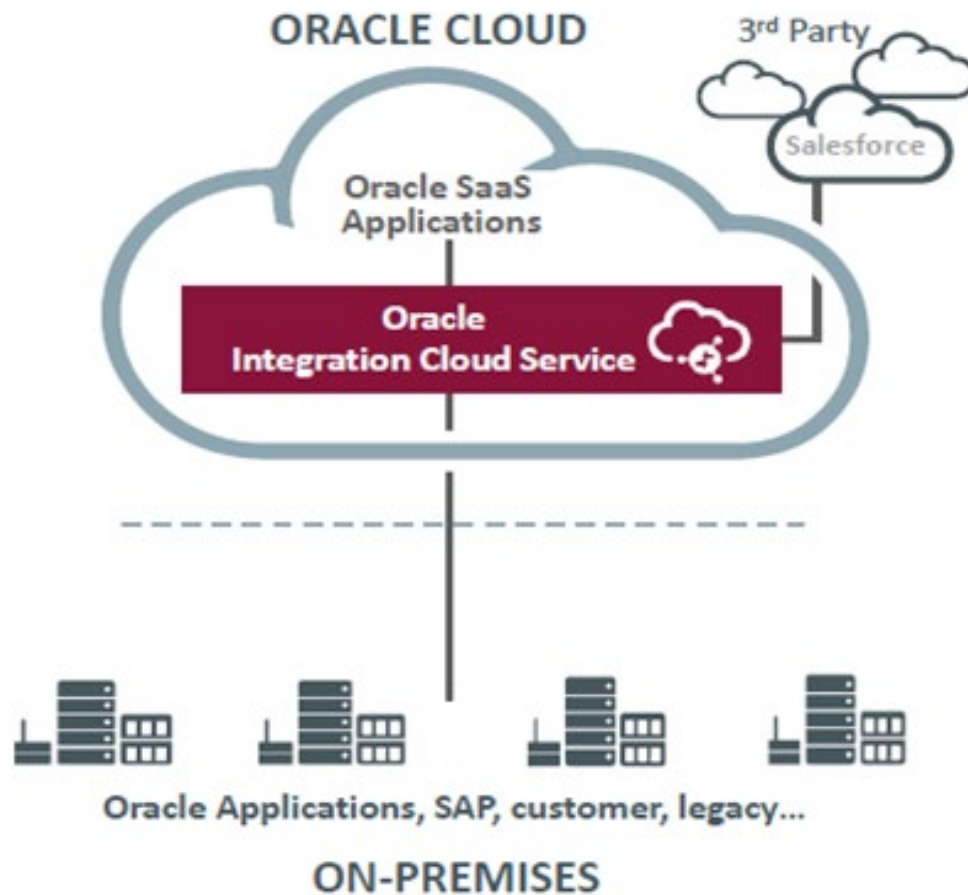


Figure 30. Oracle Integration Cloud Model

Ariba adapter in the OIC has the following features to handle the integration requirements of the State of Maine's eProcurement solution.

Features of Ariba Adapter

Ariba adapter offers Procure to Pay solutions such as:

- Creating requisitions
- Create, update, cancel and close of purchase orders
- Supplier onboarding
- Supplier/Contract data synchronization with other ERPs
- Master data synchronization
- Payments etc.

In addition to the above, Ariba adapter also supports both buyer and sourcing operations such as:

- Enabled to integrate the near real-time data between SAP Ariba and other external systems.
- Receives events from SAP Ariba in near real time, such as receiving newly created or modified purchase orders from SAP Ariba in near real time.
- Provides support for the SOAP web services and Integration Tool Kit (ITK) feature.
- Enables to create, load, update, or delete records into SAP Ariba as a single record or bulk records.
- Enables to import records in bulk into SAP Ariba. For example, the Import Remittance Data operation that imports the bulk records of remittance information.

- Enables to extract/export records in bulk from SAP Ariba. For example, the Export Remittance Locations Data operation that exports the list of remittance details. You can perform the following transactions:
 - Import Ariba data: Load data into Ariba in .csv file format.
 - Export Ariba data: Extract data from Ariba in .csv file format.

Integration Patterns

Infosys will leverage following OIC Integration patterns for integrating with Ariba in order to meet the State of Maine's requirements.

Table 17. Oracle Integration Cloud Integration Patterns

Import User Data with Ariba ITK
Export Supplier Data with Ariba ITK
Subscribe to Incoming Events with an SAP Ariba Adapter Connection
Use Web Services Outbound Functionality

To meet the real-time and batch integration needs of the State of Maine, Infosys will use these integration options which are safe, secure, and reliable:

- HTTPS using a CSV interface (batch integration, and depending on the data volume this can be scheduled to run frequently to achieve near real-time integration)
- SOAP web services that use an XML payload (real-time integration suitable for transactional data)
- REST APIs (supports both synchronous & asynchronous calls)

Security

All of the proposed integration methods for the State of Maine will support:

- SSL 256-bit encryption
- WS-Security
- Digital certificate authentication

Key Design Considerations

During the data import process from any adapter or system, the SAP Ariba Adapter performs the following tasks:

- Compresses a large data file and transform it into a ZIP file
- Sends only a 10 MB ZIP file to the SAP Ariba
- Updates the status to 200 for large data, the SAP Ariba Adapter divides the total data into chunks of 10 MB (zipped file size) and sends ZIP files of 10 MB in size in each turn.
- The SAP Ariba Adapter retains ZIP files of less than 10 MB in size but updates the status to 200.
- The SAP Ariba Adapter sends a ZIP file less than 10 MB in size in the final submit call.
- The Transactional data operation does not show tasks that are not part of any batch process. For example, the Import Catalog Views operation is not part of any batch process. Therefore, the SAP Ariba Adapter does not show it in the user interface. While loading the transactional data into SAP Ariba, the selected task should be part of a batch process. Otherwise, you cannot see the task in the user interface and cannot load the data.
- Multipurpose Internet Mail Extensions (MIME) attachments in an Ariba outbound SOAP service

scenario are not supported.

High Level Integration Architecture for State of Maine

The Oracle integration cloud uses the built-in Ariba adapter to connect with SAP Ariba and it uses the PeopleSoft adapter to connect with Oracle PeopleSoft.

For connecting with the other external on-premise systems, it uses the lightweight connectivity agent called the OIC agent, along with this, it also supports SOAP,REST,DB,JMS,FTP,File integrations.

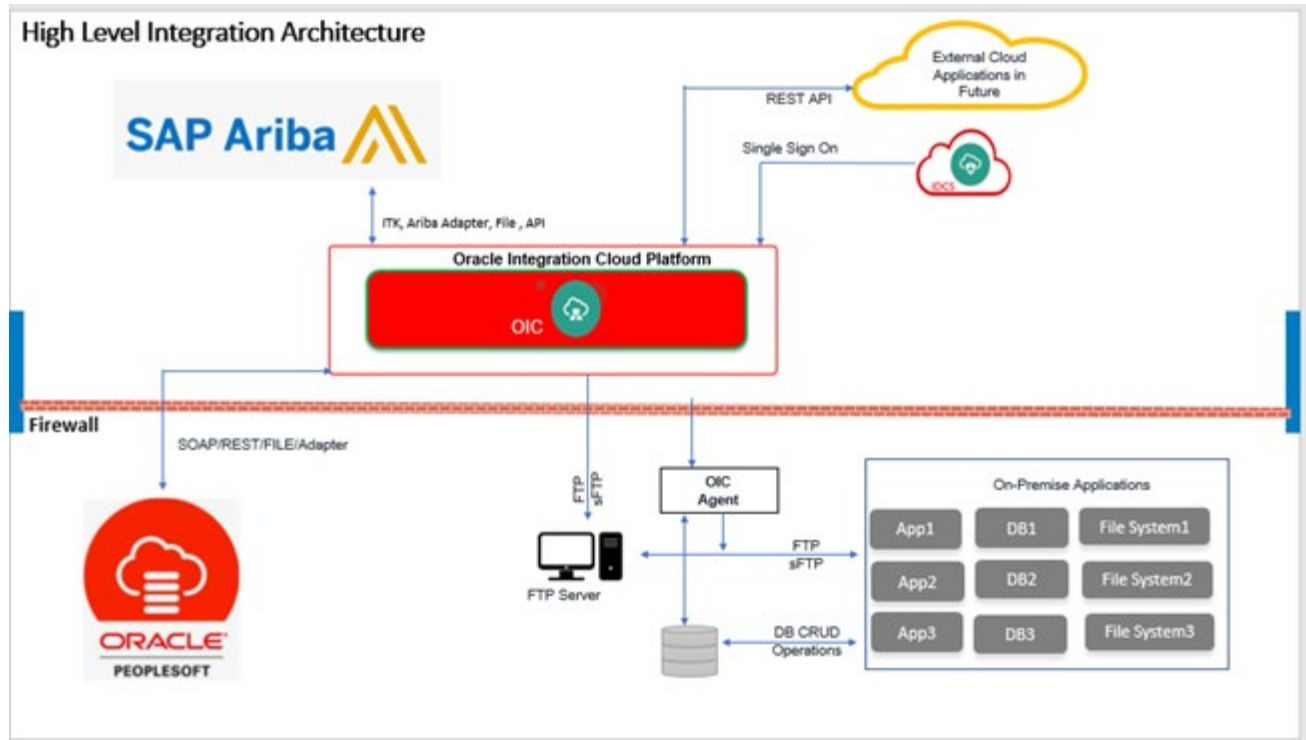


Figure 31. High Level Integration architecture

1.2.3.10 Office Automation Integration

SAP Ariba supports a wide array of document types (including Word, Excel, PowerPoint, PDF files, etc.) and formats as attachments or documents stored within a workspace. Ariba also provides functionality to export reports as excel workbooks.

Ariba has the functionality of Desktop File Sync (DFS), DFS automates the uploading and downloading of files from and to SAP Ariba Strategic Sourcing solutions and allows you to check document version compatibility.

Ariba allows various transactional documents to be Imported/Exported.

- Ariba has the functionality to use Microsoft Excel workbooks to create or update large-sized requisitions particularly if line items on those requisitions consist of a varying mix of accounting combinations.
- SAP Ariba solution provides several sample Microsoft Excel spreadsheets as starting points for creating new contract requests.
- Catalogs can also be uploaded/updated in the excel format in Ariba.
- Questions and requirements can be imported from an Excel document in a fixed format defined by SAP Ariba to a guided sourcing event.
- SAP Ariba can export a summary of the tasks and phases in a project to Microsoft Excel. The export file contains the information for each phase or task- task name, status, task owner, etc.

- Sap Ariba has a feature that allows to export a bid history report to Excel. This report can be useful to buyers to understand how their suppliers' bids have progressed throughout an event.
- SAP Ariba allows to export a Microsoft Excel file for bid comparison containing the pricing conditions for each validity period and item and supplier combination. The bid comparison Excel file includes two sheets:
 - Overview Sheet- This sheet includes information about the event. For example, the event name, publish date, event owner, and event type.
 - Bid Comparison- This sheet displays supplier bid data, including pricing condition and volume information. Initial supplier values appear in shaded gray cells. Supplier values appear in color shaded cells. Each supplier has their own corresponding color.

All of the free-text field in Ariba in various transactional documents allows the data to be copy pasted from other sources.

Using the user Interface, customers with the proper access can import data into Ariba or Export out of Ariba in CSV format.

1.2.3.11 *Mobile Device Support*

The SAP Ariba Procurement mobile app supports Apple iOS and Android devices and the following operating systems:

- -iOS versions 10.x and later
- -Android 8.0 and later

SAP Ariba Supplier supports Apple iOS and Android devices.

SAP Ariba Supplier supports the following operating systems and devices:

- iOS versions 14.x or higher:
 - iPad Air, mini, and mini with Retina display
 - iPhone 8x or higher

For iOS, SAP Ariba Supplier works best when viewed on the iPhone 8, 8 Plus, 9, iPhone X, iPhone XS, iPhone 11, iPhone 12, iPhone 12 Pro, and iPad Air.

- Android versions 9.x or higher.

For Android, SAP Ariba Supplier works best when viewed on Samsung Galaxy S9, S10, and S11 devices.

SAP Ariba Supplier works best with the latest versions of iOS and Android; users with older operating systems may have optimal performance.

The SAP Ariba mobile app is not certified with mobile device management (MDM) platforms.

Security features in the SAP Ariba mobile app help protect your data and the communication between the app and the SAP Ariba.

- App activation code: Users receive a code on their device and enter it in the SAP Ariba solution. The code allows the SAP Ariba mobile app to communicate with the SAP Ariba solution and access solution data.
- App pin: Users create a 6-digit PIN that they use to log in to the SAP Ariba mobile app.
- Touch ID support for iOS devices: allows users with iOS devices to use Apple Touch ID instead of a PIN to access the SAP Ariba mobile app.
- App timeout: By default, the user is logged out of the app after 5 minutes of inactivity. The length of the timeout is configurable by SAP Ariba via a site parameter.
- Data encryption: All data is encrypted, including data transmitted over the network and data

stored on the device (for offline access).

- All communication between the device and the server is over TLS 1.2.
- Data stored on mobile devices is encrypted using AES 256.
- Certificate pinning: The mobile app (a client) is hard-wired with the SAP Ariba servers' certificate digest to ensure that the app is communicating only with the correct servers.
- Jailbreak and rooting detection: You can have SAP Ariba configure a parameter on your site to detect jailbreaking or rooting, forcing the app to close if either state is detected. Jailbreaking and rooting are ways of removing restrictions put in place by device manufacturers.
- Data removal from deactivated devices: SAP Ariba solution data stored on the device is automatically removed from the device when the device is deactivated.

1.2.3.12 *Mobile Applications*

Users can use the Ariba Mobile app to view, track, and approve purchase requisitions, nudge approvers, and access informative articles on the Exchange User Community, all from their mobile devices.

The Ariba Mobile app includes the following features:

- Shopping Cart: Allows you to create requisitions from the Ariba Mobile app on your mobile device. The Shopping Cart includes the following features:
 - Catalog Search. Users can search their organization's catalog and order items from it.
 - Spot Buy Purchases. Users who are enabled to use the Ariba Network Spot Buy feature see search results from eBay and can purchase directly from eBay sellers.
- Requisition Approval: Approvers can quickly approve or deny requisitions. Approvers can view requisition details and history, view attachments, add comments, and receive reminder nudges from the requester.
- Requisition Tracking: Users can track the requisitions they submitted. They can view requisition details and history, view the approval flow, and nudge the current approver. They can also withdraw requisitions.
- Viewing Requisitions as a Watcher: Users who are watchers in an approval flow can monitor requisitions. Watchers can view requisition details and history, view attachments, add comments, and nudge the current approver.
- Viewing Previous Approvals and Denials: Approvers can review the details and attachments of requisitions they recently approved or denied.
- Ariba Exchange User Community Access: Users can read and comment on articles on the Ariba Exchange User Community.
- Touch ID Support for iOS Devices: If your iOS device has Apple Touch ID capability, and you have enabled it on your device, you can use it to access the Ariba Mobile app instead of using a PIN
- Sending the Supplier 360° Report to an iOS Device: If you have an Apple iOS device, you can send the Supplier 360° report to the Ariba Mobile app, allowing you to view a PDF version of the report on your mobile device.
- Pinning Requisitions: While viewing a requisition in the Ariba Mobile app, an approver can "pin" the document for later viewing in their Ariba Procurement Solution. Pinned requisitions are added to the Pinned Items action tile on the dashboard of the Ariba Procurement Solution

1.2.3.13 *Data Ownership and Access*

- The State completely owns the data in the SAP Ariba Solution and all of its components. The State can extract the data from the solution at any point of time throughout the subscription

with no additional cost. All documents are available in the system for searching, reporting, or legal, tax and audit purposes.

- Document Configurable alerts: Choose specific document types and statuses for which you want to view notifications and receive push alerts on your mobile device.
- Pin orders and invoices: Mark important documents from your mobile device to access them more quickly from a desktop workstation.
- Orders and invoices: View order and invoice details, status changes, and histories. Create invoices, credit memos, and debit memos. Share orders and invoices with your colleagues using any app on your device that can share documents, such as email, text messages, or Google Docs.
- Order confirmation: Confirm standard purchase orders at the header level.
- Receive and respond to leads: Monitor, respond to, and bid on SAP Ariba Discovery postings.
- Company profile management: Track your company profile completeness. Complete your company profile to increase your chances of being discovered by new buyers.
- Mobile Gateway: The mobile gateway is a set of features that allow you to access the full functionality of Ariba Network from within the SAP Ariba Supplier mobile app. Mobile gateway features allow to:
 - update your company profile
 - view the web version of orders and invoices
 - create non-PO invoices
 - create standard PO-based invoices
 - create credit memos, line-item credit memos, and line-item debit memos

Search: Search for specific orders and invoices or filter by status, customer, or pinned documents. SAP Ariba Supplier uses the powerful HANA infrastructure to allow users to search for orders and invoices from the last 12 months. Alternatively, users can browse recent orders and invoices from the last 31 days. The solution provides various tools to download the data. For example: User Interface (Import CSV), API's.

1.2.3.14 *Data Retention, Archive, and Purge Considerations*

SAP Ariba solution along with other solution components confirm archive and purge capabilities as per the requirements given in the RTM.

SAP Ariba is a SaaS solution which is highly scalable with virtually unlimited storage. Transactional data can stay in SAP Ariba without the need of archiving or purging. On the other hand, a customer is in complete control of data deletion and purging which can be manual or automated via integration.

SAP retains customer data for the life of the subscription and in accordance with the Ariba Data Policy and privacy statement found at the following URL: <http://www.sap.com/corporate-en/about/our-company/policies/ariba/data-policy.html>

Data retention is governed by the active contract. SAP retains your data on the service for the duration of the subscription term and any subsequent renewal term, subject to legal requirements imposed on auction site operators. During this time, you may download your data using the functionality within the application, in order to meet your specific retention requirements.

1.2.3.15 *Disaster Recovery Plan*

We plan to run disaster recovery (DR) simulations and exercises once a year. The exercise will be run with the support team and State of Maine's key stakeholders, including the IT support team, leadership team, and some State of Maine users. Since all of our solution components are cloud-based, Cloud

services will not be shut down for the DR simulation. The DR exercise will be conducted during a weekend and will be using a combination of the test environment and production environment, to make sure that business operations are not interrupted.

A formal DR Exercise plan will be created with relevant communication protocols established and documented. The DR exercise schedule, as appropriate, will be posted and communicated via the Portal to ensure that user communities are aware of the exercise. All support personnel including service desk will be informed of the exercise so that they can properly handle normal incidents ticket as well as DR related “incidents”.

In addition, our team will work closely with cloud service providers portal, SAP, Oracle and ServiceNow to ensure State of Maine’s Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) are coordinated with respective service plans and activities performed by these cloud vendors. Below are some technologies, processes and procedures that have already been established by these vendors.

Tier 1 – SAP Ariba and OIC

SAP Solution

SAP Ariba solutions are deployed in regional data center pairs so, in the event of a failover, the data will remain within the region. Failover from one site to another has a design goal for its recovery time objective (RTO) to not exceed four hours. The design goal for the recovery point objective (RPO) is five minutes.

SAP Business Continuity (BC)

SAP Ariba runs redundant copies of all critical software subsystems including application services, enabling automatic fail-over in the event of an error so that there is no disruption of service. SAP Ariba hardware infrastructure is also implemented with automatic fail-over mechanisms. For further redundancy, SAP Ariba is connected to the internet with two different ISPs running through physically separate conduits to the upstream provider.

In the event of any hardware failure, SAP Ariba Operations will be automatically notified so that the failed equipment can be analyzed and repaired, and the problem prevented in the future. Even if, for some reason, automatic hardware fail-over does not work, the data integrity will still be intact.

SAP Ariba performs periodic preventive maintenance. This preventive maintenance is scheduled for low-use times, such as weekends. All data in the system is maintained and will wait while maintenance is being performed and resume processing when maintenance is finished.

SAP Disaster Recovery (DR)

Disaster recovery options are included for all cloud services for SAP Ariba solutions. In the event of a failover to the secondary data center, no customer changes are required, as all URLs that customers use to reach the applications will continue to work. SAP will notify customers through e-mail in the event of unplanned downtime.

Internally, SAP Ariba solutions use a documented system recovery plan that outlines the approach and steps for recovering the applications. This document defines roles and responsibilities in the event of disaster:

- Cloud engineering services personnel maintain the hardware remotely.
- SAP Ariba solutions maintains the application software.
- Processes are in place to keep database and storage subsystems synchronized between primary and secondary data centers.
- The failover processes for all infrastructure elements are automated.
- If the primary data center incurs a catastrophic event, SAP will declare the primary data center

“down” and the Cloud Engineering Services team will initiate the process to switch to the secondary data center and restart the applications at the secondary data center.

Once the switch is complete, the secondary data center becomes the primary data center and vice versa SAP tests power outage backup scenarios and the disaster recovery plan on a periodic basis to ensure it is up-to-date, successful, and effective.

SAP Backup and Recovery

SAP Ariba performs regular backups of the stored data. These backups do not interrupt the normal operation of the Ariba system. Backup data includes user information, projects and the library. Backups are performed using disk backups. These are changed regularly at each facility and are rotated to off-site storage for additional security.

Oracle Cloud Business Continuity (BC)

Oracle deploys the Oracle Cloud Services on resilient computing infrastructure designed to maintain service availability and continuity in the case of an incident affecting the services. Data centers retained by Oracle to host Oracle Cloud Services have component and power redundancy with backup generators in place, and Oracle may incorporate redundancy in one or more layers, including network infrastructure, program servers, database servers, and/or storage.

Oracle Cloud Disaster Recovery (DR)

Disaster Recovery (DR) services for Oracle Cloud Services are intended to provide service restoration capability in the event of a major disaster, as declared by Oracle.

Oracle will determine whether an event constitutes a disaster requiring the execution of the DR plan for the affected Oracle Cloud Service. Oracle will work to perform DR services for Oracle Services as described below.

Recovery Time Objective: Recovery time objective (RTO) is Oracle's objective for the maximum period of time between Oracle's decision to activate the DR recovery processes described in this document and the point at which You can resume production operations in an alternative site. If the decision to activate DR recovery processes is made during the period in which an upgrade is in process, the RTO extends to include the time required to complete the upgrade.

Recovery Point Objective: Recovery point objective (RPO) is Oracle's objective for the maximum period of data loss measured as the time from which the first transaction is lost until Oracle's declaration of the disaster. The RPO does not apply to any data loads that are underway when the disaster occurs.

The RTO and RPO do not apply to customizations that depend on external components or third-party software. During active failover events or recovery operations, non-critical fixes and enhancement requests are not supported. Oracle is not responsible for issues arising from third party software and customizations to Oracle programs and services.

Oracle Cloud Backup and Recovery

Oracle periodically makes backups of your production data in the Oracle Cloud Services for Oracle's sole use to minimize data loss in the event of an incident. Backups are stored at the primary site used to provide the Oracle Cloud Services and may also be stored at an alternate location for retention purposes.

A backup is typically retained online or offline for a period of at least 60 days after the date that the backup is made. Oracle typically does not update, insert, delete or restore user data on the user's behalf. However, on an exception basis and subject to written approval.

For Oracle Cloud Services which enable a user to configure backups in accordance with Your own policies, Users are responsible for performing backups and restores of data, non-Oracle software, and any Oracle software that is not provided by Oracle as part of these services. Additionally, Users are encouraged to develop a business continuity plan to ensure continuity of your own operations in the event of a disaster.

ServiceNow Solution

ServiceNow is divided into two distinct environments for Business Continuity (BC) and Disaster Recovery (DR). ServiceNow's corporate environment and its data center environments are separated from each other. A disaster in ServiceNow's corporate environment could occur with little or no impact on the private cloud.

ServiceNow Business Continuity (BC)

ServiceNow's BC process covers its functional offices and is a separate standard operating procedure from its customer environments. The BC Plan (BCP) has been developed in concert with the entire business including Business Impact Assessments (BIA) to understand the impact of the loss of any given systems or locations.

ServiceNow Disaster Recovery (DR)

ServiceNow's customer DR is documented in its Information System Contingency Plan (ISCP), which covers its data center environments, and includes all customer environments as well as the instances that ServiceNow uses to run its business.

ServiceNow Backup and Recovery

While advanced high availability is the primary means to recover data and restore service in the case of a service disruption, in certain cases it is desirable to use ServiceNow's more traditional data backup and recovery mechanism. This data backup and recovery system works in concert with AHA and acts as a secondary recovery mechanism.

The backup cycle consists of four weekly full backups and the past 6 days of daily differential backups that provide 28 days of backups. All backups are written to disk, no tapes are used and no backups are sent off site. All the controls that apply to live customer data also apply to backups. If data is encrypted in the live database then it will also be encrypted in the backups. Regular, automated tests are run to ensure the quality of backups. Any failures are reported for remediation within ServiceNow.

ICAM Solution

With Azure AD B2B, users would be able to conveniently access all their apps with SSO from any location, on any device, from a centralized portal for a simplified user experience and better productivity. With Azure AD B2B, the partner uses their own identity management solution, so there is no external administrative overhead for the State of Maine. Guest users would sign in to State of Maine applications and services with their own work or social identities.

Saviynt would be deployed on a modular and integrated platform for identity governance. The key modules are Access Request, Access Certification, Role Engineering and Management, SOD Management, Policy and Rule Management, Provisioning, and Analytics. It provides the flexibility to deploy these modules individually or together, depending on the nature of business and system requirements/constraints. Infosys will work with the State of Maine to determine the best architecture and deployment model.

ICAM Business Continuity (BC)

Saviynt provides an availability guarantee of 99.5% availability. This level can be further enhanced based on business continuity measures.

Each service in the Saviynt environment is monitored for operational effectiveness and to track availability. These metrics include but not limited to network connectivity, CPU utilization, memory utilization, storage utilization, service status etc. Any failure will generate alert that are pushed to the operations team through email and SMS.

The key to Azure AD's high-availability is that the services can quickly shift traffic across multiple geographically distributed datacenters. Each datacenter is independent, which enables de-correlated failure modes. Through this high availability design, Azure AD requires no downtime for maintenance activities.

ICAM Disaster Recovery (DR)

Saviynt is designed for maximum performance, scalability, and availability. Using the Saviynt cloud delivery model (based on Azure), Saviynt supports a RPO of 15 minutes, based on Multi-AZ failover. If multi-region (DR) capability is required, Saviynt supports a RTO of Approx. 105 minutes.

Azure AD maintains a zero Recovery Time Objective (RTO) to not lose data on failovers. This includes:

- Token issuance and directory reads
- Allowing only about 5 minutes RTO for directory writes

ICAM Backup and Recovery

Production Backup (Azure Tenants) – In case AD is hosted in Azure VMs:

- VM Disk Snapshot automated backup is taken every 24 hours with the retention period of 30 days using Azure Runbook.

Non-Production Backup (Azure Tenants)

- VM Disk Snapshot automated backup is taken every 24 hours with a retention period of 7 days using Azure Runbook.

Recovery

- VM restoration from a snapshot backup

Custom Portal Solution (optional)

The portal solution is a public access mechanism for the awards information. Even though this component of the overall solution does not qualify as a highly critical system from a business continuity perspective, in the event of a disaster. But given it will be hosted on Acquia Cloud, we will always have backups to restore the system and create portal instance into the active datacenter of Acquia cloud, with an RTO of 48 hours and RPO of 5 minutes (RPO will be same as source data system (Ariba)).

There will be no data loss. Only the availability will be affected during the time of disaster.

Overall Continuity Plan

Based on our analysis of the requirements and details, one of the key focus areas is to deliver seamless IT services. To ensure seamless delivery, we will make extensive use of our proven Integrated IT Service Delivery Model for the day-to-day operations. The Application operations and support team will work with development teams, hosting vendors/partners and other support partners, as necessary, to drive enhancements or fixes/resolutions to any issues to provide IT-Service Continuity. The Integrated Service Delivery Model is based on ITIL's Service Management Framework

and has been built on the best practices derived from our experience of running application and infrastructure operations for global corporations. The Integrated Service Delivery Model will not only help integrate various service operations across people, process and technology, but also eliminate redundant handoffs and streamline and simplify the Issue-to-Resolution cycle for all of our solution components.

1.2.3.16 *Solution Environments*

Our proposed solution will have the following environments (Development, Testing and Production) provisioned using SaaS (SAP, ServiceNow) and PaaS (ICAM, OIC, Portal) to meet the State of Maine's requirements. However, logical environments can be created to meet any additional needs of the State of Maine.

SAP Ariba by default provides the production and testing environments. Development, testing and training of procurement processes are carried out in SAP Ariba Test environments. SAP Ariba Production environment is for live business transactions. SAP Team Infosys will leverage the test environments to carry out the development, testing and training needs. For PaaS (ICAM, OIC, Portal) additional environments can be created on need basis.

Below section provides Infosys approach to use different environments for State needs.

Table 18. Solution Environments

Environments	SaaS (SAP Ariba)	PaaS (ICAM, OIC, Portal)	Remarks
Development	Shared	Dedicated	Development, Testing and Training is carried out in SAP Ariba Test Environment
Test	Shared	Dedicated	
Training	Shared	Dedicated	
Production	Dedicated	Dedicated	

1.2.3.17 *Solution Technical Architecture*

The core of our Solution offered is our partner SAP's Ariba Cloud applications. In addition, we will utilize the capabilities of our Portal Cloud, ServiceNow Cloud together with SAP Ariba to cater to the needs of the State. Solution components selected for the State of Maine are all top of the line industry SaaS products in their respective solution areas. Even though there are multiple components, they have a "tight fit" and appear seamless to the end user. The components are straightforward to operate and help fulfill our commitment to long term operations and support. Below is the representation of our technical solution.

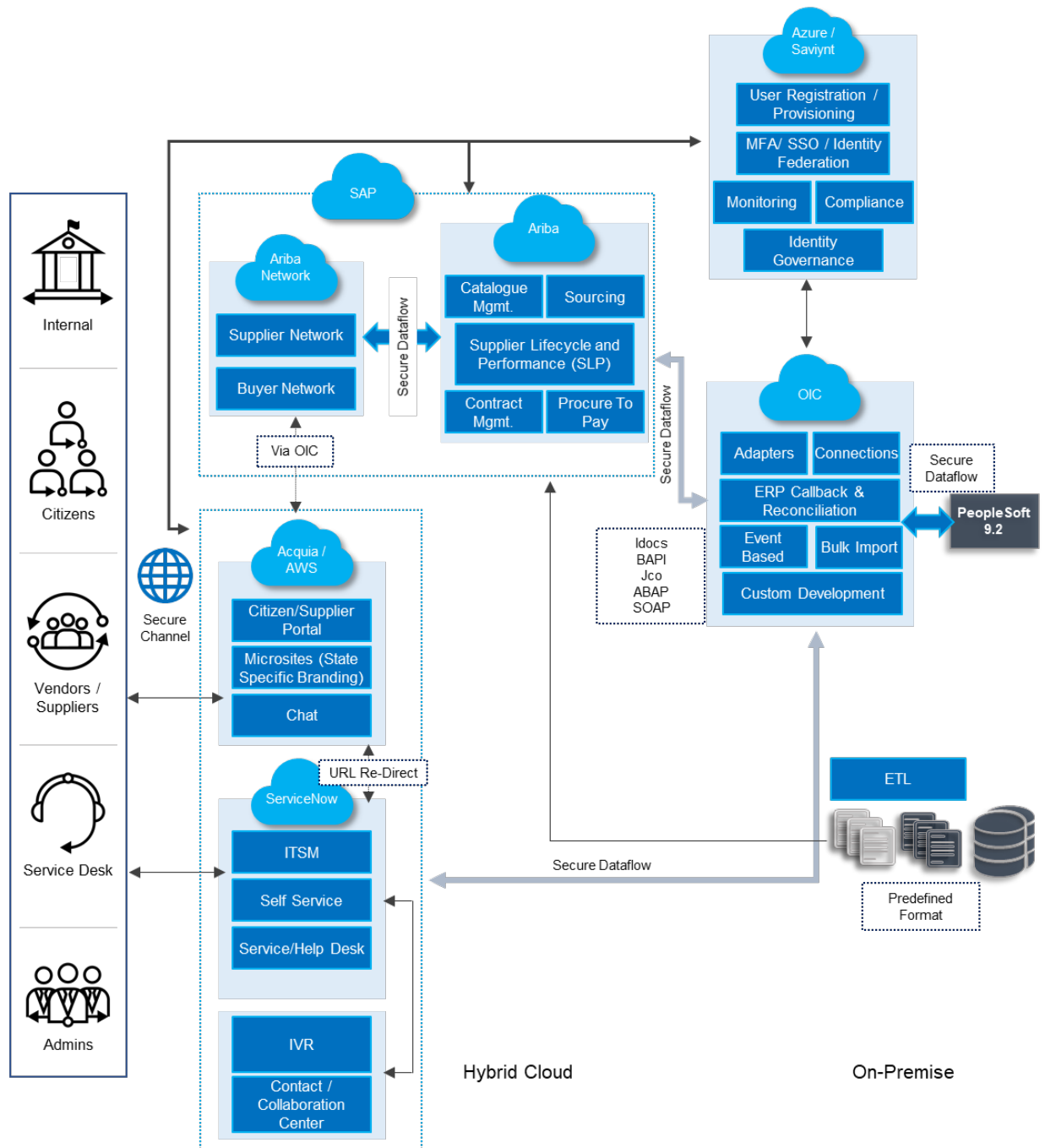


Figure 32. High Level Solution Architecture

The solution we are proposing for the State of Maine includes the following components:

- Core Solution includes:
 - SAP's Ariba cloud-based SaaS eProcurement solution covering Sourcing to Contracts and Procure to Pay
 - Oracle Integration Cloud (OIC) is the middleware used to integrate our solution with the State of Maine's main ERP system
 - Cloud-based Portal Solution integrating access, collaboration, community, personalization, resources and information for both buying and supplier users
- Service Desk Solution includes:
 - ServiceNow Cloud-based SaaS Incident Management system for handling Service

- Desk
 - Service Desk Telephony and IVR Automated Attendant system
- Security
 - Out of the box single sign on feature to support Kerberos, LDAP, and other SAML-based identity and authentication capability
 - Built-in security features and OWSM supported by SOA for transport level security and message level security to support X.509, SAML and OAuth
- Project Implementation and Support Tools include:
 - Microsoft SharePoint for EPS knowledge management and project collaborations, hosted in MS Azure cloud
 - Other productivity and support tools, including system performance testing, and security testing, hosted in Amazon Web Services (AWS) cloud

Key Application/Functional modules of our Solution

Table 19. Key applications and platform

Logical Components	Technology Point	Platform
eProcurement	SAP Ariba (SAAS)	SAP Cloud
Middleware	Oracle Integration Cloud (PAAS)	Oracle Cloud
Helpdesk	AWS Connect (PAAS) Service Now	ServiceNow Cloud
Portal	Acquia (PAAS)	Leverages AWS Cloud
Identity and Access Management	Azure AD(PAAS) & Saviynt (SAAS)-Optional	MS Azure Saviynt Cloud

Key Features of our Proposed Solution

Our proposed solution offers the following benefits:

- An end-to-end SAP Source-to-Pay SaaS system that provides a fully integrated solution, including single vendor accountability, simplified architecture, and accelerated implementation
- A technology infrastructure that builds upon cloud architecture
- A solution that ensures seamless integration with the various State of Maine's enterprise management systems
- Service Desk and Self-Service portal functionality built on the market leading ServiceNow SaaS platform

Data Exchanges between Legacy and Proposed Solution

We propose the Oracle Integration Cloud Suite and infrastructure for the integration between our solution and the State's ERP instances. The proposed solution delivers the following values for the eProcurement implementation:

- Reduce time for new project integration
- Reduce integration cost and complexity
- Efficiently manage business and technology changes
- Provide end-to-end solution monitoring with root cause analysis
- Gain increased visibility to quickly react to business events
- Ensure high availability and scalability for your business infrastructure

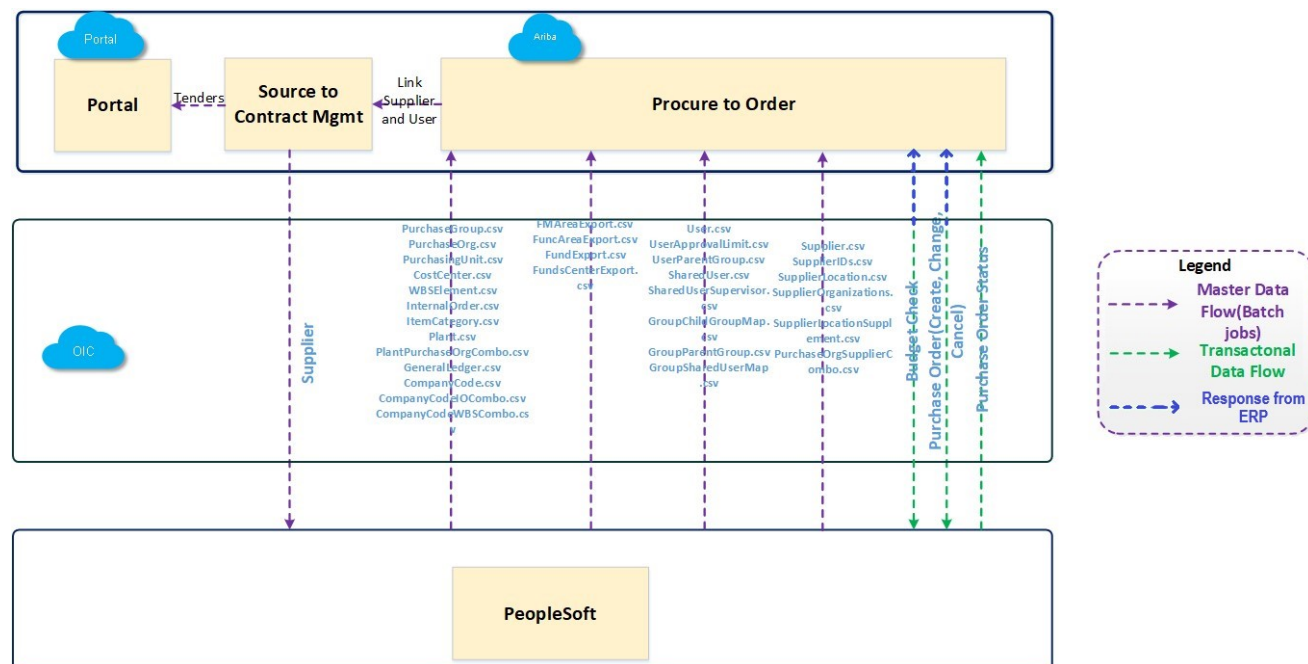


Figure 33. Data Exchanges between Cloud and On-Premise ERP system

The table below lists the other data exchanges within the solution and with the ERP system.

Table 20. Core Data Exchanges

Data Type	Data Source	Data Target	Data format & Type	Integration Tool
Ariba Solution				
Supplier Information	PeopleSoft	SAP Ariba Supplier Management	CSV files /REST	OIC
Sourcing Information (Indirect Spending)	PeopleSoft	SAP Ariba Strategic Sourcing	CSV files /REST	OIC
Procurement	PeopleSoft	SAP Ariba Procurement	CSV files /REST	OIC
Invoicing	PeopleSoft	SAP Ariba Financial Supply Chain	CSV files /REST	OIC
Supply Chain	SAP Ariba Solutions for Direct Spend	NA	NA	NA
Contract Management	SAP Ariba Contracts	NA	NA	NA
Portal Solution				
Static Web content	Drupal	Drupal	PHP	
Award Details	Drupal	SAP Ariba	REST API	OIC
Help Desk Solution				
Customer Contacts	Web, IVR and email	ServiceNow	Adaptors, API	

Development tools and languages:

Our proposed solution leverages a SAAS platform which comes with pre-configured modules for implementing the procurement solution. However, there are certain configuration and integrations which are required. The proposed solution provides out-of-box templates and configuration checklists for carrying out the necessary configuration needed for the State of Maine's application. Infosys has also developed many accelerators for the procurement solution requiring minimal development. However, in the event some development is required, Infosys will leverage the development tools shown below and the IDE's for meeting the State of Maine's needs:

Table 21. Logical Components and Tools

Logical Components	Development tools and Language
eProcurement	Out of box Project configuration Templates.
Middleware (OIC)	REST/SOAP, Files, DB or Out of box Adapter
ServiceNow	Out of box Templates & JavaScript
Portal	Drupal Modules, Acquia Dev Desktop, Acquia BLT and Acquia Git, PHP, JavaScript, HTML, CSS
Identity and Access Management	Out of Box connectors & Azure Automation Scripts(Powershell)
Misc.,	Visio, DevOps Scripts

Development Technique and Approach

Since the proposed solution leverages a vertical procurement solution, Team Infosys will carry out a fit-gap analysis to identify any need of configuration or integration required for each capability listed in the RFP. The proposed solution leverages a hybrid agile approach leveraging Infosys IDEA-Activate™ methodology, which is an extension of SAP's Activate methodology. The IDEA-Activate™ methodology is our proven approach for procurement and Ariba based transformations and aligned to the IMPACT framework. A major advantage of using this approach is to validate a minimum viable product at the earliest point in time.

From the Ariba side, all solution development uses FIPS compliant modules.

Network Architecture and Solution Components sharing

Our proposed solution leverages a SAAS platform which segregates each customer using a strict access control mechanism by having necessary rules and access restrictions in place. Any data, log files or user information associated with one customer account is not visible to another account. For a new State customer onboarding in this solution, virtual segregation will be leveraged and a new account for each customer will be created. Data accessed by the customers associated with a particular account and will not be shared with anyone else.

Detailed description of proposed solution components:

eProcurement Solution:

Ariba cloud services were architected from inception for multi-tenancy and are structured as a SaaS Model IV, where customer unique metadata allows each customer to use the same application but the configuration metadata allows each customer to have their own look and feel to the application as well as configurable aspects, which appear as customizations.

Each customer has unique IDs within the environment and system processes running within the application validate and enforce user permissions and privileges as well as customer logical instantiation by the unique customer id each time the database is accessed for read or write. This is

enforced for all customers and various monitoring processes run in background within the solution to status the validation process as well as other KPI's related to the customer's configuration within the environment.

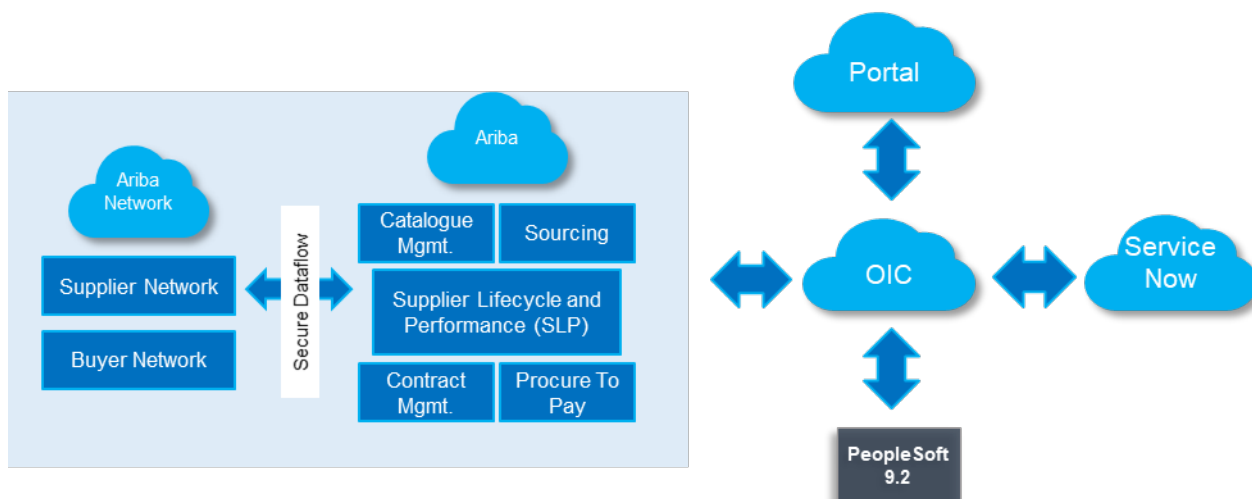


Figure 34. Ariba High Level Architecture

The software's data model keeps the different customers' data strictly separate. Customer data is isolated by realms. A distinct realm is used to identify each individual customer and store their data. Realms are sealed off from other realms such that it is not possible for a given realm to see or access data from another realm.

No direct access to the database is allowed in order to enforce the customer ID validation and user permissions and privileges and the only systems that interact with the data in the database are the business application servers where customer users access the applications.

Table 22. eProcurement Layers

Server	Description
Web Layer	Ariba uses multi-processor servers to run multiple Apache web servers that are configured to be redundant and fault-tolerant. Ariba Cloud Services packages are run on Redhat server platforms. The web servers serve as smart proxies such as module which decides which app node to send the request.
Application Layer	Ariba applications run on multi-processor servers and are run on AMD Redhat Linux server platforms. A single server is capable of running multiple application nodes as determined by load testing and performance optimization. Ariba application servers are configured to be redundant to handle increased system loads if one or more of the servers go offline. Ariba uses Tomcat as its underlying application server software. All major Ariba-developed application services hosted by Ariba consist of three basic software layers: - HTML Rendering Layer: This layer renders application objects and data in HTML/XML templates for display in client browsers. - Application Logic Layer: The application logic layer is coded primarily in Java. This layer handles client requests using the core business application logic and interacts with the persistence layer to persist data and retrieve data from the underlying database.

Server	Description
	Persistence Layer: The persistence layer interacts with the underlying relational database to manage the object-to-relational mapping. The persistence layer stores and retrieves application data. Ariba uses Oracle and HANA database software and management utilities. Application Software Release Strategy All Ariba Cloud Service components and other applications, such as web server software, monitoring tools, and release and deployment tools, can be released and distributed together or independently. Ariba has a wide portfolio of services each with its own 9-to-12 month release cadence. To facilitate high quality, rapid customer adoption, and minimum change impact, Ariba delivers a subset of its portfolio each quarter. Customers are notified of a new release three to six weeks before it is deployed. The releases are scheduled during off-peak hours and weekends to minimize the impact of downtime. All configuration logic settings, branding resource files, library data, and project data are upgraded for customers at this time. All configuration files and data are upgraded and tested by Ariba so that customers' environments remain consistent before and after major releases.
Data Layer	Ariba uses Oracle 11g and HANA databases running on Linux for the Basic/Professional packages. For failover, the Ariba databases run in highly available clusters. Ariba has deployed 3rd party vendors for enterprise-grade storage technology from HP (3PAR Inserv) and EMC (Symmetrix), to ensure the database servers have fault-tolerant disk storage. The 3rd party vendor provides performance, connectivity, and functionality for consolidation and application storage management. Information stored in the database is behind three layers of firewall protection and an Intrusion Detection System monitoring traffic for anomalous behavior. The Database Servers are hardened and accessible only to a handful of operations personnel.
File Servers	Ariba uses Network Appliance clusters (NetApps) unstructured data storage. Examples include order attachments, backup index files, catalogs, and other data. NetApps are dedicated multi-protocol file servers with more storage capacity that Ariba uses in a clustered configuration. The NetApps' speed, short backup window, and reduced management overhead facilitate efficient management of the Ariba application.

Portal Solution:

Our portal solution acts as a landing site where end users will initiate interaction with the core system and with Service Desk. Our solution will be enabled to accomplish the portal WCM (web content management) requirements. The OOB (out of box) search module will be configured to accomplish the portal content search requirement within the portal, such as communications and knowledge bases. The system localization application will be used to achieve the bilingual requirements for the State of Maine, to support English and other languages as needed. Interactions with the Ariba application will be through SOA based web services (SOAP/REST) accomplished via our middleware solution.

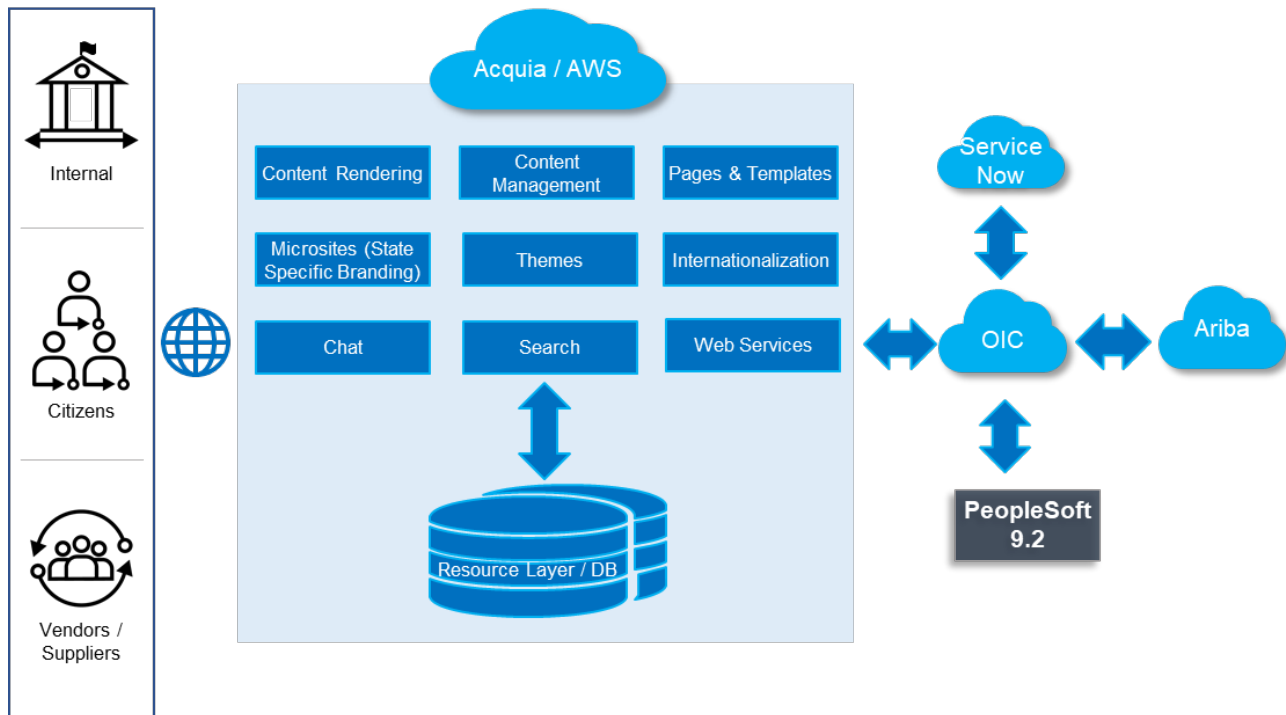


Figure 35. Portal High Level Architecture

The portal's business processes will be accomplished by workflows for complete content lifecycle comprising content stages from create, review, and approve to publish. Reusable authoring and presentation templates/components will be designed which will be leveraged by business teams to build the portal pages and content. Portal site taxonomies and metadata models will be designed to meet the optimal website navigation and content exploring needs.

Middleware Solution:

The Oracle integration cloud uses the built-in Ariba adapter to connect with SAP Ariba and it uses the PeopleSoft adapter to connect with Oracle PeopleSoft. For connecting with the other external on-premise systems, it uses the lightweight connectivity agent called the OIC agent, along with this it also supports SOAP, REST, DB, JMS, FTP, File integrations.

The SAP Ariba Adapter in OIC enables integrations with SAP Ariba. We configure the SAP Ariba Adapter as an invoke connection and a trigger connection in an integration in Oracle Integration. The SAP Ariba Adapter offers procure-to-pay solutions. It helps to create requisitions, purchase orders, and payment methods in the SAP Ariba application. The SAP Ariba Adapter also supports supplier onboarding, master data synchronization with other ERP systems.

The ServiceNow Adapter is one of many predefined adapters included with Oracle Integration. We configure the ServiceNow Adapter as an invoke connection in an integration in Oracle Integration.

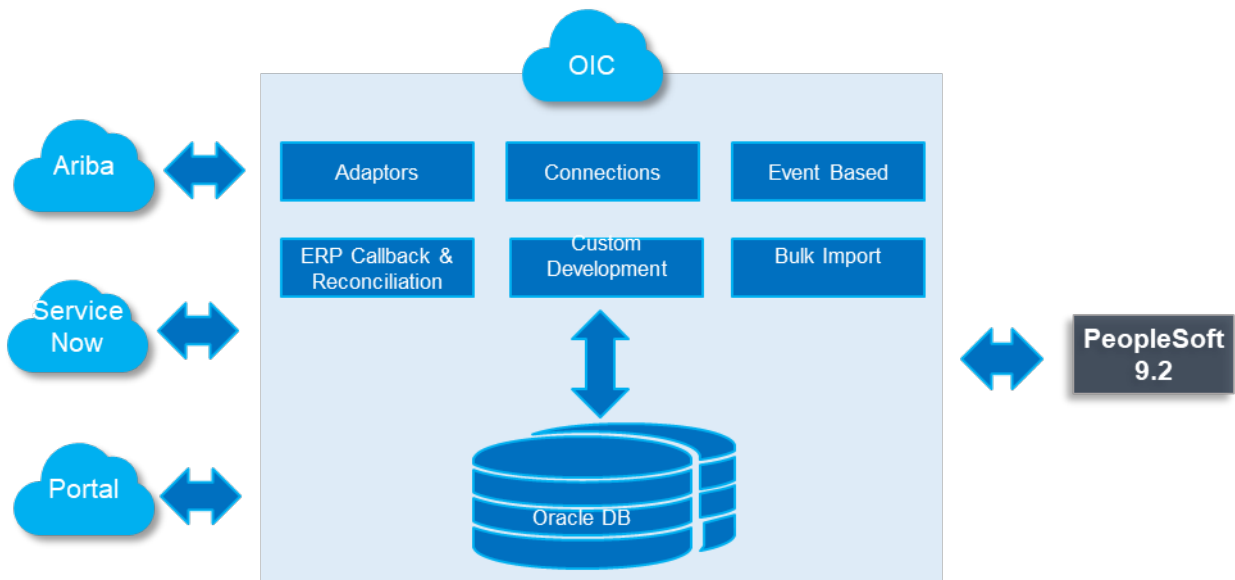


Figure 36. OIC High Level Architecture

The REST Adapter exposes integrations as REST APIs by configuring a REST Adapter connection as a trigger. The REST Adapter also consumes any external REST API by configuring a REST Adapter connection as an invoke. This section identifies the capabilities of the REST Adapter when used as a trigger or invoke connection.

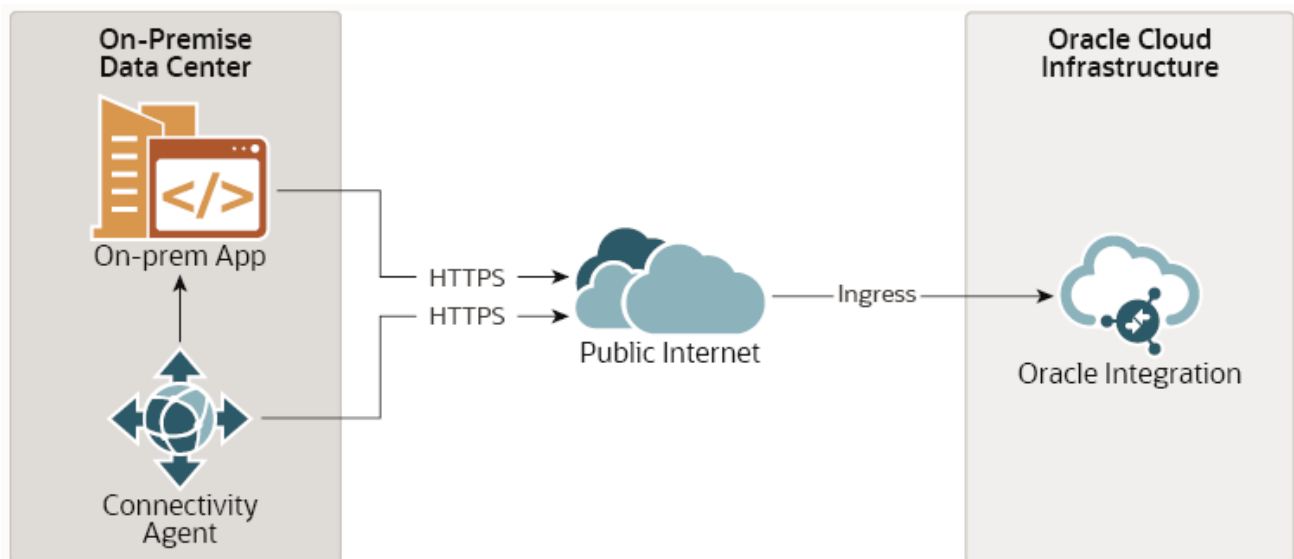


Figure 37. OIC and On-Premise Integration

The inbound and outbound traffic to Oracle Integration goes over the public internet. For the outbound traffic from Oracle Integration, the connectivity agent initiates a secure connection to Oracle Integration, retrieves the request, and then invokes the required API in the on-premises application.

Helpdesk Solution:

ServiceNow's architecture is built on a ServiceNow fully owned and operated private cloud. This private cloud hosts the ServiceNow platform and applications that are offered to its customers under a subscription service model. The private cloud operates out of co-location data centers that provide robust physical and environmental controls.

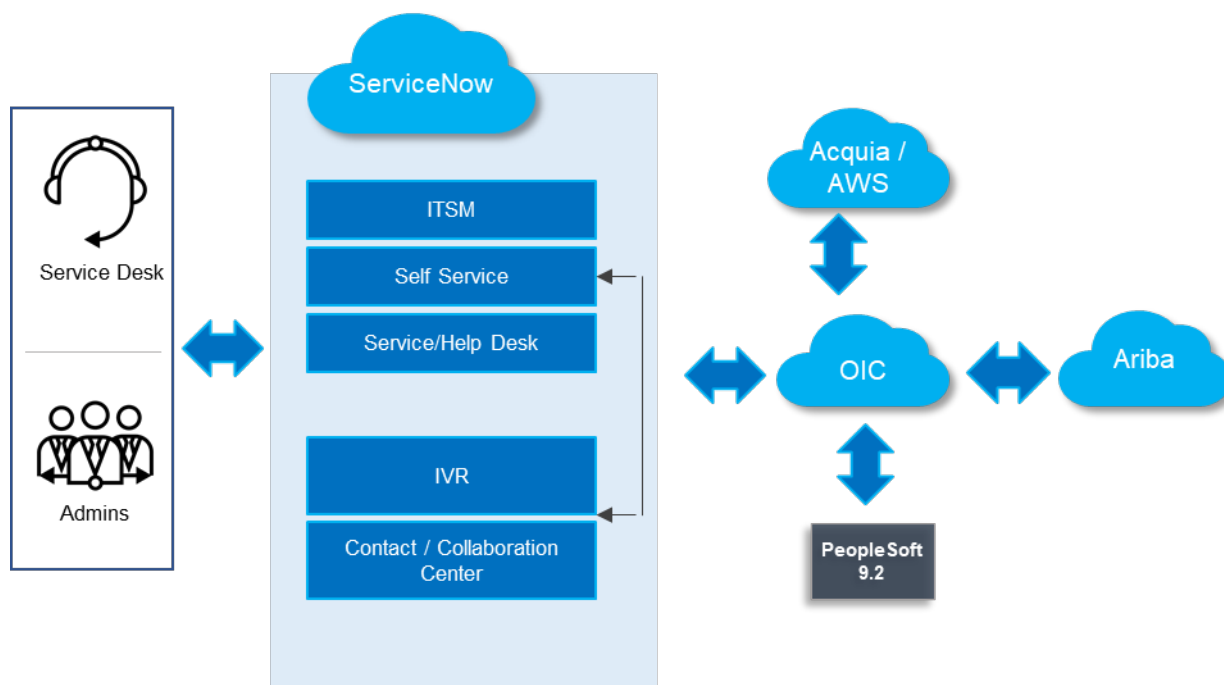


Figure 38. Helpdesk High Level Architecture

Table 23. ServiceNow Application Layers

Server	Description
Web Layer	The proxy layer consists of ServiceNow's network and security equipment typical of a DMZ environment that provides a front end to the application layer and obfuscates ServiceNow's internal network
Application Layer	Each instance consists of multiple application nodes to provide redundancy with each application node having an isolated virtual environment on a shared physical server
Data Layer	Each instance has its own dedicated database, running in this defined network zone

The Infosys ESM Café solution is Infosys' gold image of the ServiceNow solution, it is designed by Infosys on top of ServiceNow and has ready-to-deploy work packages for base ITSM applications. The end-to-end accountability for all aspects including ServiceNow platform, implementation, maintenance and support lies with Infosys. ESM Café has preconfigured processes incident, problem, change, knowledge, self service and service request management. These predefined processes can be deployed for the State of Maine with minimum configuration.

1.2.3.18 *Solution Network Architecture*

Infosys' proposed solution leverages a Hybrid Cloud based architecture with the core solution platform as SAP Ariba. SAP Ariba SAAS Solution is designed based on industry best practices to achieve resilience, high availability and scalability as well as to ensure security across the solution components. All interactions with our proposed procurement solution will be routed over the public internet. Communication between SAP Ariba with other supporting solution components will be leveraging industry standards network and communication protocols to ensure than solution is compliant and flexible to integrate over public internet line both for on premises and SAAS based solutions.

Ariba's Network Architecture, Access Points and Components

Infosys' proposed solution leveraging the SAP Ariba SAAS platform will have access points enabled through the public internet using an HTTP channel. Our proposed solution provides a separate access point for production and non-production environments. Access restrictions from a particular network or IP address can be configured using the SAP Ariba administration console leveraging Ariba access management policies.

SAP Ariba solutions' Web tier utilizes Web servers in conjunction with F5 load-balancers to provide perimeter security for all SAP Ariba solutions in the cloud. F5 provides TLS termination (SSL) and enables support for modern strong encryption, including elliptic curve ciphers and 256-bit encryption. Connectivity between F5 and the Web servers are also protected with a TLS connection behind F5's Internet perimeter.

Our proposed solution implements an n-tier network architecture that physically segments Web, application, and data tiers. The communication protocols used between the systems are TCP/IP-based. The Cloud Engineering Services team constantly monitors and maintains all systems. Redundant load balancing and security firewall devices are inserted between each tier of SAP Ariba solutions.

The following description provides a detailed overview of the path of a request from an SAP Ariba solutions customer to an SAP Ariba solutions service:

- The customer connects through a browser to the appropriate Internet URL address.
- The user request passes through perimeter routers and the first level of firewalls, and the connection is terminated by a redundant set of load balancers.
- The load balancers use a round-robin and source-IP/cookie-based SSL persistence to determine which Web server should be connected, and then reissues another connection to it.
- The Web server accepts the request and identifies which application node to send the request based on the URL and a round-robin protocol. The Web server initiates another connection to the application node, which traverses through a second layer of firewalls.
- The application servers accept the request, process application-level security and authorization checks, interpret the request, and determine if data interaction is required.
- If data interaction is required, the application servers issue requests through a third layer of firewalls to the database servers or the file servers.
- The database servers and file servers return the requested data back to the application server layer, which generates the required response.
- Application servers send the response back to the web server layer, which returns the response to the original requester.

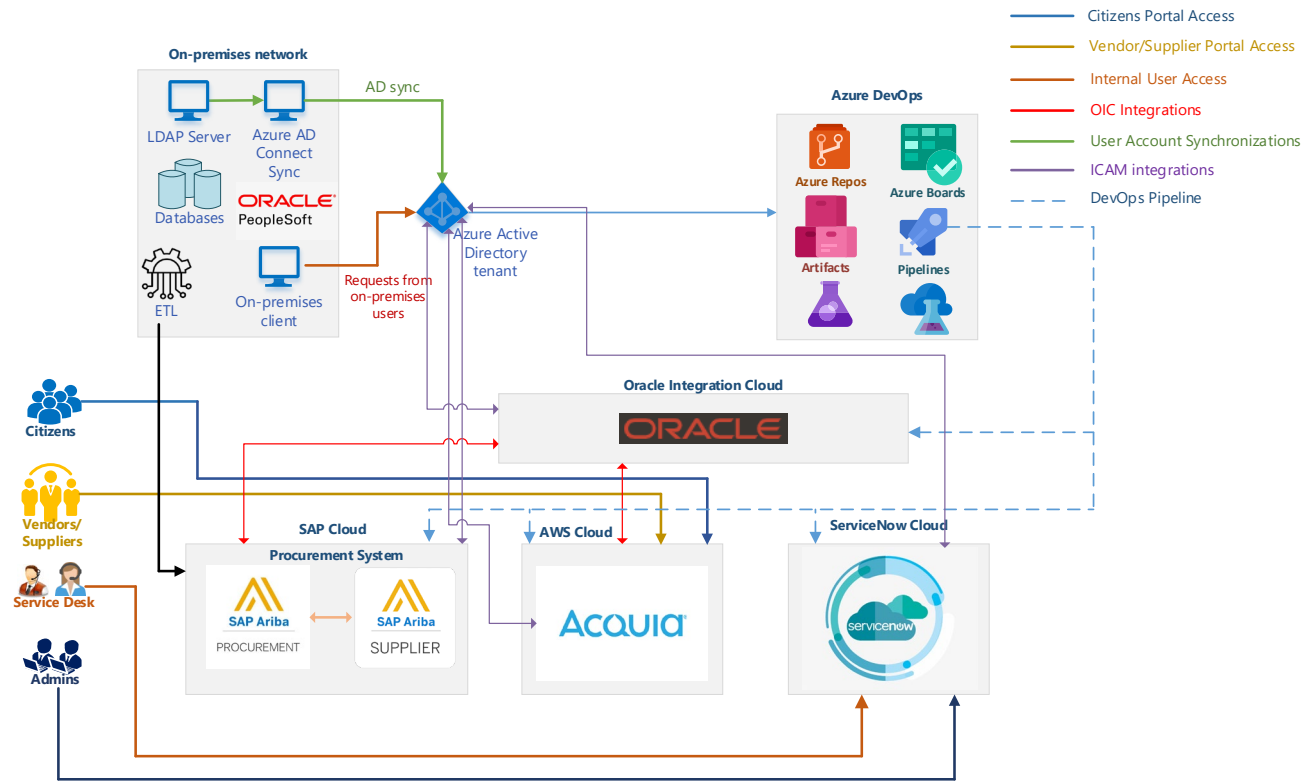


Figure 39. Logical Network Architecture

Internet Connections: SAP Ariba solutions maintain diverse redundant connections to the Internet through top-tier carriers. These are configured using BGP (Border Gateway Protocol) for redundancy. BGP is used to achieve 100% network uptime, providing redundancy for IP networks.

Switches and Routers: SAP Ariba solutions use cutting-edge technology and industry-standard equipment for ensuring optimum network connection performance. They deliver enterprise-class versatility, integration, and power to SAP Ariba solutions. Together, these routers provide the required support for Internet and intranet access with firewall security. Routers are the primary networking components in SAP Ariba solutions. They coordinate the delivery of data packets between the various system components while providing several essential security controls and features. Routers provide packet filtering by creating access control lists (ACLs) that define the types data packets (protocol, source, and destination) allowed to pass through the router interfaces. Data packets that do not meet the criteria specified in the ACLs are rejected.

Load Balancers SAP Ariba solutions' load balancers control traffic and guarantee optimal utilization of the Web servers. Although it is not considered a security component, the load balancers provide access control functionality to ensure authorized traffic flow. Access control entries (ACEs) deny all traffic through the load balancers except traffic between the internal interface of the firewall and the external interface of the web servers. ACEs also deny traffic that is not using one of the required protocols for firewall-to-Web server communications. The load balancers are used as SSL-termination end points for TLS 1.2 initiated sessions.

Firewalls SAP Ariba solutions employ next-generation firewall appliances that deliver strong security and performance and create almost no network performance impact. The solutions enforce secure access between an internal network and Internet, extranet, or intranet links. SAP Ariba solutions use cutting-edge technology and industry-standard equipment to control the traffic to and from the Internet, between the corporate intranet of SAP Ariba solutions and the cloud solutions, and between the cloud solutions' servers.

The firewall servers are configured for high-availability configuration setup. Specifically, firewall servers are used in each level of data communication within SAP Ariba solutions:

- Between the internet and web servers
- Between the web servers and the application servers
- Between the application servers and the database servers

These firewall appliances allow the Cloud Engineering Services team to rigorously protect SAP Ariba solutions from unauthorized access, providing full firewall security protection.

For integration with the State of Maine's on-premises data center, Infosys will work with State of Maine to expose an API or use inbuilt PeopleSoft adapter in Oracle Integration Cloud.

The network diagram below shows the placement and connectivity of the various hardware infrastructure components i.e., compute (servers), storage, firewalls, load balancers and switches. It also details the "No Single Point of Failure (NSPOF)" architecture design principle. The security zones depicted in the diagram are for representation purposes and the actual deployment can be defined based on the security policies as defined.

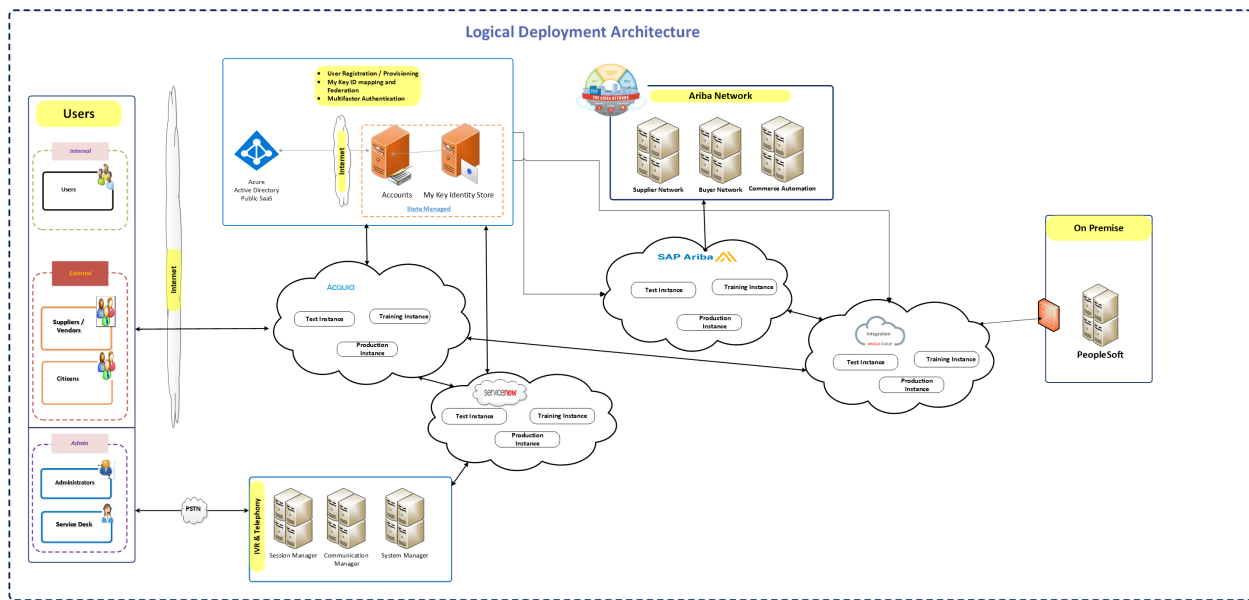


Figure 40. Logical Deployment Architecture

The eProcurement Solution can be hosted in any location. However, considering the State of Maine and other State security requirements, Infosys will provision SAP instances in the US region which has a data center in the eastern US (VA). Data will always be in the U.S region. SAP Ariba deploys secondary data centers (not listed in above link) in the region of the primary data center for backup and disaster recovery purposes. A high-level view of SAP data center design and how it manages power supply, cooling, controlled access, hardware failure, fire protection, building management, data privacy and data access is available at above mentioned links.

Below provides details of our core solution (SAP) data center locations on a map. Additional details are available in website SAP Ariba Trust Center



Figure 41. SAP Data Centers

The figure below provides information on the measures available based on industry and technology standards for the data center operations.

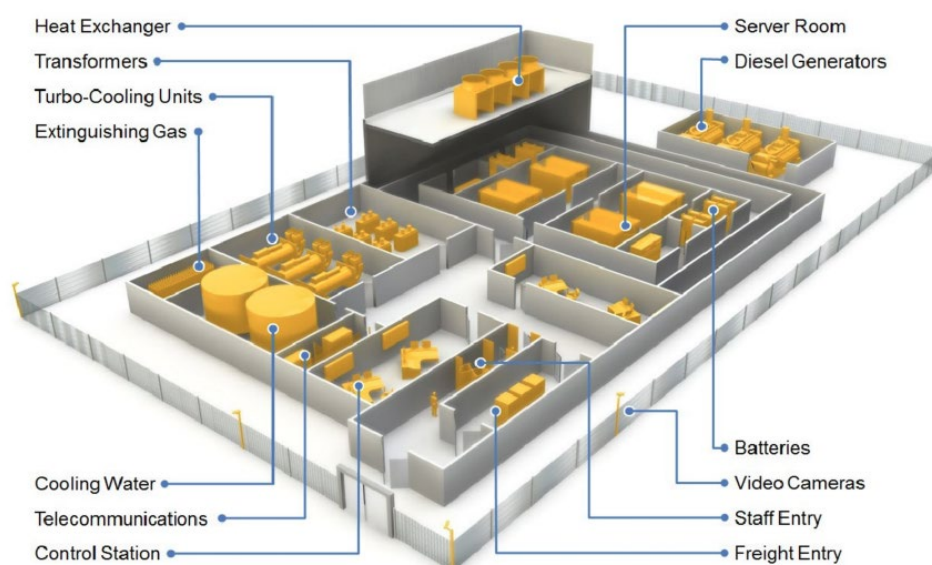


Figure 42. Data Center Components

Table 24. eProcurement Network Features

Features	SAP Ariba eProcurement Component
Bandwidth & Redundancy	SAP uses Border Gateway Protocol to peer with redundant Internet Service Provider's and manage the bandwidth accordingly SAP Ariba maintains diverse redundant connections to the Internet through top tier carriers. These are configured using BGP (Border Gateway Protocol) for redundancy. BGP is used to achieve 100 percent network uptime, providing redundancy for IP networks. Redundant load balancing and security firewall devices are inserted between each tier.
Power Supply	The data center is connected to two separate grid sectors operated by the local utility company. If one sector were to fail, then the second one will ensure that power is still supplied. The uninterruptible power supply (UPS) ensures that the quality of the power remains constant. It compensates for voltage and frequency fluctuations, effectively protecting sensitive electronic

Features	SAP Ariba eProcurement Component
	components and systems.
Cooling	Servers are installed in racks, which resemble standardized shelving units. They are laid out so that two rows of racks face each other, thereby creating an aisle from which the front side of the server is accessible. The aisles are covered above and closed off at the ends by doors. Cool air set to a temperature of 24°C to 26°C is blown in through holes in the floor, flowing through the racks and dissipating the heat emitted by the servers.
Controlled Access	Access to the data center is allowed only for a limited number of authorized individuals. Entry is possible only through single-person access and mantrap systems. Freight can be brought into the data center using a special freight lock. An intrusion detection system monitors incoming data and identifies suspicious activities, while firewalls made by different manufacturers protect the data in the data center. Data and backup files are exchanged with customers in an encrypted format or trans-mitted over secure fiber-optic cables.
Physical Security	The data center is monitored around the clock. Single-person access and mantrap systems provide access only to authorized individuals. Technicians can enter special rooms using custom-configured ID cards. High-sensitivity areas require authentication by means of biometric scans.
Hardware	All virtual and physical servers, storage units, networks, and databases in use access a pool of physical hardware. If an individual component should fail, the load can be immediately reallocated to other components without impairing system stability. If hardware fails due to a fire, data can be recovered from the backup system.
Data privacy	SAP helps ensure compliance with data protection provisions. Data from cloud customers falls under the jurisdiction selected by the customer and is not forwarded to third parties. SAP support services help ensure that data protection is maintained during required maintenance operations.
Back-up	Backups are carried out in the form of a disk-to-disk copy, which enables rapid data creation and recovery. In addition to full back-ups done on a daily basis, interim backup versions are created several times per day and are then archived, like all backups, at a second location for security purposes.
Floor Space	The exterior walls are 30 centimeters thick and made of reinforced concrete. The server rooms are surrounded by 3 concrete walls. This design provides effective protection against storms or a small-airplane crash.

Along with the SAP Solution, our proposed solution leverages other SAAS and PAAS components. Since our solution is fully SAAS based solution leveraging multiple cloud component services as PAAS and SAAS services. Cloud providers (SAP, Azure, AWS and Oracle Cloud) provides a layer of abstraction on infrastructure components like (hardware, operating system, high availability configurations, power failures, disaster recovery) and will be handled by cloud providers. Details of each cloud vendor approach to manage these tasks related to data center management, security and associate activities are provided in data center details column in the table below.

Table 25. Data Residency & Data Center Locations

Solution Components	Cloud Provider	Data Residency and Data Center location	Data center Details
eProcurement	SAP Ariba (SAAS)	U.S EAST Virginia	Additional details are given in SAP Ariba Trust Center website
Middleware	Oracle Integration Cloud (PAAS)	U.S EAST Virginia	https://www.oracle.com/cloud/data-regions/
Helpdesk	AWS (PAAS)	U.S EAST Virginia	https://aws.amazon.com/about-aws/global-infrastructure/
Portal	Acquia (PAAS)	U.S (EAST) Virginia	Leverages AWS Data centers (https://docs.acquia.com/cloud-platform/arch/#aws)
Identity and Access Management	Azure AD (PAAS) & Saviynt (SAAS)	U.S EAST Virginia	https://azure.microsoft.com/en-us/global-infrastructure/

The solution will leverage the “security in depth” design principle by means of controls such as firewalls, intrusion prevention system, anti-virus solution etc. along with the core network services in the data center to ensure security and connectivity of the solution serving systems.

The below three components—authentication, encryption, and integrity—are key to securing the overlay network infrastructure.

- Authentication - The solution ensures that only authentic devices can send traffic to one another
- Encryption - All communication between each pair of devices is automatically secure, eliminating the overhead involved in securing the links
- Integrity - No group keys or key server issues are involved in securing the infrastructure

1.2.3.19 *System Development Methodology*

Development Methodology:

Security and privacy are an integral part of our development process to achieve security and privacy by design. Ariba leverages a secure software development cycle (Secure SDC) that is aligned with ISO 27034 principles. It ensures the quality, long-term flexibility and reusability.

ISO principles includes:

- Secure code (OWASP Top Ten) training to engineers
- To ensure quality, code is reviewed by peers before build cycles.
- Static and dynamic code analysis, with load testing for resiliency
- Reviews and approvals at multiple phases for meeting security criteria prior to release to production.

Solution Testing Process:

We leverage an extensive automation test suite, built on Selenium, which provides consistent, repeatable testing, decreased test time, and more complete testing than relying purely on manual testing. Automation, which is run for every build, also allows us to manage and maintain quality

throughout the development lifecycle. In addition to automated testing, we also execute a comprehensive suite of manual test cases and perform regular ad hoc “group” testing each week.

The test scenarios, test cases and test scripts are designed as per the requirements mentioned in the functional specifications document approved by the business/State of Maine. Prepared test scenarios and test scripts are thoroughly reviewed by the Test lead and then to be approved by the State of Maine. It ensures that the testing process covers all the business requirements and also it ensures the system reliability.

We would perform the Unit testing, Functional Testing, System Integration Testing and User acceptance testing to ensure the quality of the solution.

Quality Assurance Program:

Our quality assurance program is an integral part of the common Product Lifecycle Methodology (PLM), under which all of our software products are developed. The PLM has predefined development phases each with specific activities, deliverables, and success factors. Each phase has non-negotiable entry and exit criteria, for release quality over schedule. Milestone exit is not allowed without meeting the exit criteria cleanly. Exit criteria include defect trends, test case execution/pass rates (both manual and automated), and code review statistics. Each phase has a formal exit review. For all releases, GA sign-off is required by product development executive leadership.

Our development process is based on the Agile Scrum development methodology, which is centered on small, empowered, cross-functional teams called “feature teams” or “scrum teams”. Scrum team members include Development, QA, Solution Management, User Centered Design (UCD), Documentation, and Globalization.

Performance Testing:

We use the following quality control processes within the common Product Lifecycle Management (PLM): Technical Reviews, Automated & Manual Testing, Performance, and Stress Testing. We leverage an extensive automation test suite, built on Selenium, which provides consistent, repeatable testing, decreased test time, and more complete testing than relying purely on manual testing. This ensures response time and reliability guarantees are met. The Automation, which is run for every build, also allows us to manage and maintain quality throughout the development lifecycle. In addition to automated testing, we also execute a comprehensive suite of manual test cases and perform regular ad hoc “group” testing each week.

Configuration /Change Management Methodologies:

After a product deploys, defects found by customers are fixed, and an analysis is made of these problems to improve the next release. Production quality metrics are tracked continuously to determine areas for improvement. All releases are fully documented, covering requirements, design, and test approach for all features.

The documented systems development methodology describes the change initiation, software development, change documentation, and approval processes.

Changes to applications, which include emergency changes, are subject to change management procedures and require testing and management approval prior to deployment.

Changes to the implementation of hardware, operating system, patches and packages, are subject to change management procedures.

All changes are categorized per impact and risk level assessment according to the guidelines of a routine, standard and emergency change.

Furthermore, standard and emergency changes go through the daily Change Advisory Board (CAB) consisting of domain owners for final confirmation and approvals.

1.2.3.20 *Service Level Agreement*

Infosys has reviewed and indicated compliance to the attached Service Level Agreement standard provided with the RFP document. The attachment provided by Infosys is “**Exhibit 2. RFP 202102021 Model SLA_Infosys Response.docx**”. The standard Service Level Agreement for Ariba Cloud Services is also included in the response. Please refer to section “**Attachment 1 - Service Level Agreement for SAP Cloud Services**”.

1.2.4 Security Requirements

1.2.4.1 *Cloud Security Alliance (CSA) Compliance*

Infosys proposed procurement solution is comprised of best in breed in cloud solutions to simplify the procurement management process, integrations and operations. The proposed cloud solutions are compliant with the security requirements detailed in the RFP, primarily the CSA CCM requirements and NIST 800-53 requirements. The table below provides a summary of the CSA compliance requirements for the proposed cloud solutions:

Table 26. CSA Compliance

SI No	Cloud Solution	Solution Area	Part of the core solution?	Cloud Service Provider	CSA compliance Artefact
1	SAP Ariba	Procurement Solution	Yes	SAP	Completed CAIQ questionnaire can be found in -> Security Attachments.zip - > 8969 CSA - CAIQ v.3.0.1.xlsx
2	Oracle Integration	Integration	Yes	Oracle	Third party Independent assessment report for compliance with CCM 3.01 can be found in -> Security Attachments.zip -> Oracle OCI CSA STAR L2 - May 2021.pdf
3	ServiceNow	Helpdesk ITSM process management	Yes	ServiceNow	Completed CAIQ questionnaire can be found in -> Security Attachments.zip - > ServiceNow-CAIQ_v3.1-2021.xlsx
4	Azure Active Directory/ Azure Services	User authentication	No – optional component	Microsoft	Completed CAIQ document can be found in -> Security Attachments.zip -> Azure - Cloud Security Alliance - Consensus Assessments Initiative

SI No	Cloud Solution	Solution Area	Part of the core solution?	Cloud Service Provider	CSA compliance Artefact
					Questionnaire (CAIQ).pdf
5	Saviynt	User Accounts Administration and Provisioning, Access Certification	No – optional component	Saviynt, hosted on Azure cloud	Saviynt is currently part of our optional offering for Identity Credential and Access Management (ICAM) component. Saviynt will be deployed on Maine specific Microsoft Azure tenant and will inherit the Azure CAIQ compliance. An updated CAIQ worksheet will be provided post the solution configuration, provided the State decides to choose ICAM offering from Infosys
6	Acquia Cloud	Portal Solution	No – Optional Component	Acquia, hosted on AWS cloud	Completed CAIQ questionnaire can be found in -> Security Attachments.zip - > Acquia_CDP_CAIQ_v3.1.xlsx

Infosys will inherit the security controls implemented by our cloud vendors/partners and apply any additional customer specific controls to meet the overall security objectives of the proposed solution. Our cloud security solution is designed with the “Defense in Depth” approach with focus of protecting State of Maine information assets using multiple layers of defense. Our Cloud Security Approach for maintaining and supporting cloud security includes review and configuration of security controls in the below areas based on the cloud service model (IaaS, PaaS, SaaS):

Table 27. Security Control

Network and Infrastructure Security	Incidence Detection, Response and Monitoring	Data Protection	Identity Access Management & Governance	Application Workload Security	Cloud Governance & Compliance
- Firewall Policy Review, Host Configuration and Management - NGFW Integration & Automation, Endpoint Protection - Vulnerability Management and Scanning - VNets/Subnets, Security Groups, ACLs etc.	- SIEM/SOAR Integration with Log Resources - Incident Detection, Investigation and Monitoring - Malware & Forensic Analysis - Use Cases Libraries	- Data Classification & Tagging - Data Loss Prevention - Key Management - Encryption, and Masking	- Enterprise-wide SSO, Multifactor Authentication - Privilege Identity Management - Role Based Access Control (RBAC) - Users, Applications, Cloud Resources Provisioning	- Source Code Analysis and Configurations - Security Control Integration with CI/CD Pipeline Code Deployment - Application Workload Security - DevSecOps	- Continuous Compliance Monitoring - Organizational and Standard Applicable Governance Policy Frameworks and Compliance Standards - Risk Metrics and Dashboards

During transition and operational phase, Infosys will execute the below activities to support ongoing maintenance and compliance of the overall solution subject to the cloud service delivery model:

Table 28. Support Activity Model

Transition	Steady State Support
Identify the security, privacy & compliance	Support compliance monitoring solution with cloud subscription

Transition	Steady State Support
requirements of the business process. • Discuss & finalize regulatory and compliance standards, policies, and frameworks • Decide RACI matrix for security, privacy & compliance standards • Discuss & finalize the audit frequency • Finalize & review compliance & assessment solutions, policies and frameworks • Gather the NDA, firewall etc. requirements for cloud integration with compliance monitoring solution • Create Operations Support Documents (SoPs), Run Book	• Support Inbound/Outbound integration with external SIEM/SOAR and VM solutions • Identify and configure custom organization policies for compliance monitoring • Run & monitor scan with monitoring solution to examine the compliance status • Monitor non- compliance, policies for violations • Discuss & advise the remediation steps • Container image analysis and vulnerability scanning • Audit the privilege access micro-segmentation policies • Discover onboarded resources on the cloud and audit the historical changes done on cloud resources • Identify and monitor vulnerabilities, insecure configuration issues and other security threats • Visualize risks and prioritize security issues based on severity level • Automatically discover and identify real time resources and profile assets • Generate executive dashboard report with overall compliance risk score • Provide customized compliance report w.r.t organizational policies, specific GRC frameworks etc. • Report compliance violations, governance issues with a feedback for actions • Provide an advisory for the appropriate remediation actions • Identify and provide advisory for implementing automatic remediation action

Any cloud computing solution adoption within Infosys goes through a proper due diligence and risk assessment by the Infosys Information Security Group wherein the group does a thorough security evaluation of the 3rd party cloud provider vis-à-vis the cloud security and privacy framework which is developed internally. The due diligence includes areas such as access control, vulnerability management, data segregation in multi-tenant requirements, data disposal, log monitoring and review, portability and interoperability, network controls such as firewalls, IDS, IPS, DLP solutions etc. Any security risks that come up as part of the assessment of the cloud provider are brought to senior management's attention and appropriately managed (risk reduction, acceptance etc.).

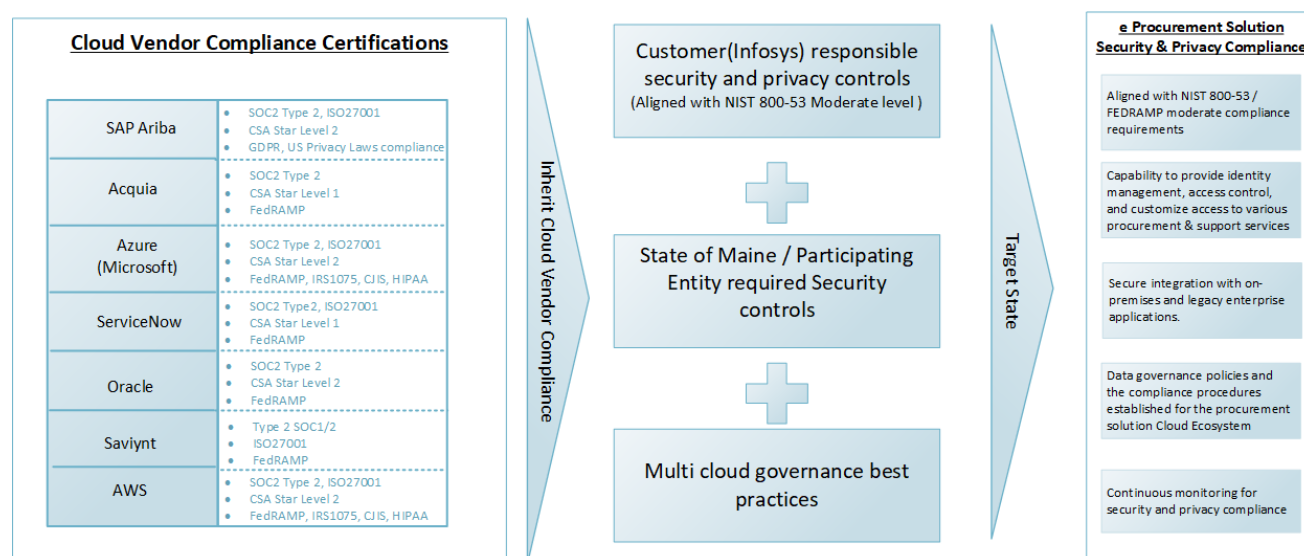
Furthermore, the contractual agreements with cloud providers are analyzed and essential information security clauses are incorporated into the agreements to ensure adherence to information security requirements of Infosys by the cloud provider and any other supplier that the cloud provider further outsources its services to with regards to Infosys. The above-described approach ensures minimal risk to Infosys from the inherent risks in cloud computing.

Infosys will designate cloud security consultants as part of the implementation and support phase, who will serve as the primary interface with the State of Maine IT security team, Cloud vendors and will be responsible to ensure the security compliance of services managed by Infosys in public cloud environment. The Infosys team would carry out periodic assessments to ensure the security posture of the overall integrated solution is maintained as per the CSA or other applicable controls.

1.2.4.2 Security and Privacy Controls

Infosys proposed procurement solution leverages public cloud offerings from the leading cloud service providers and that been recognized as “Trusted Cloud” platforms with their wider adoption by large enterprises and public sector customers. These cloud service offerings have undergone extensive third party assessments and implemented robust security controls to provide the required confidence and controls for customers to adopt the services.

The below diagram provides a high-level framework of how Infosys leverages the cloud vendors existing certifications, configure customer specific controls as applicable based on the cloud service model and manage the overall security and privacy governance across multiple cloud platforms.



As indicated in the above diagram, Infosys will inherit FEDRAMP/NIST compliance from the cloud service providers and configure customer specific controls as applicable for the eProcurement solution.

SAP Security and Privacy Controls:

It must be noted that the core procurement solution component is still in the process of being certified for FEDRAMP/NIST. However, has undergone various other compliance assessments like ISO27001, SOC2 Type 2 which have similar security controls/ requirements as that of NIST 800-53. As part of the certification, SAP Ariba is audited and certified by independent third-party auditor PricewaterhouseCoopers (PwC) for compliance with ISAE 3402 SOC1 Type II, SOC2 every six months and a SOC 3 report is issued annually. Upon completion of the audit, an attestation letter is issued, stating the level of compliance. In addition, SAP's primary hosting facility (Equinix) infrastructure is audited for compliance with SSAE 16 SOC1 Type II, SOC 2 Type II.

The Service Organization Controls report (SOC) is aimed at three different audiences. SOC1 (aimed at financial auditors) is the same type of report as the SAS70 but also includes an attestation letter signed by both our company and the auditor. SOC2 is aimed at IT and security practitioners. The SOC3 is the publicly viewable web seal to show that we have been audited. Further details regarding

SOC compliance can be found in SAP Trust Center website by searching Ariba SOC Compliance.

Upon request respective compliance certifications and associated artefacts can be made available to the State or a participating entity.

Infosys Specific Controls

In addition to the compliance by cloud service providers, Infosys as an organization, is aligned and certified to ISO 27001:2013 standard and is assessed for SSAE 18 SOC 1 Type II by an independent third party. Any other compliance requirements (such as HIPAA, FISMA, CJIS, PCI, etc.) would be subject to applicability for Infosys facilities and location from where support services delivered. Infosys has the required capabilities to be compliant to this regulation at an account level. Infosys will ensure data protection controls required by the regulation including any access restrictions are enforced.

Infosys' Information Security Policy framework is aligned to Information Security Standard. The information security policy is supported by a set of supplementary policies, procedures, and standards to achieve the enterprise level information security objectives.

The standard specifies control objectives and controls in the following areas:

- Information security policies
- Organization of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development, and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance; with internal requirements, such as policies, and with external requirements, such as laws

The table below is a compendium of Security controls and practices followed by Infosys for Technical Security, Operational Security, Management Security, and controls. They provide a high-level description of the security control catalogue which is organized into classes and control families. These control families are the basis of securing access and endpoints used by Infosys service desk / support personnel as part of the implementation and support phases.

Table 29. Technical, Operational and Management Security Controls for Infosys assets and locations

Technical Controls	Control Description	Infosys Public Services (Infosys) Security Practices
Access control	Security controls that support the ability to permit or deny user access to resources within the information system	• All employees are provided unique user IDs through Microsoft Windows Active Directory Service (ADS) upon request by an authorized Human Resources (HR) executive. All users have to authenticate with the ADS before accessing any application on intranet. The administrative access on all Infrastructure

Technical Controls	Control Description	Infosys Public Services (Infosys) Security Practices
		including servers and network devices is provided only to designated system administrators belonging to the Computers and Communication Division (CCD). A password protected screensaver policy has been implemented on all systems which enables within 10 minutes of user inactivity. • Access control is implemented using proximity cards (for data centers and server rooms). Only authorized personnel are allowed to enter the data center. • Access to eProcurement solution applications/cloud services will be based on the identity management solution option chosen by State/participating entity.
Audit and accountability	Security controls that support the ability to collect, analyze, and store audit records associated with user operations performed within the information system	• Infosys endpoints, office utility applications and networks are configured to send all audit events to our centralized Security Information and Event management. • All logs are monitored in real time through a Global Security Operation Centre (SOC) which operates in a 24X7 model •
Identification and authentication	Security controls that support the unique identification of users and the authentication of these users when attempting to access information system resources	• All Infosys employees are provided unique user IDs through Microsoft Windows Active Directory Service (ADS) upon request by an authorized Human Resources (HR) executive. All users have to authenticate with the ADS before accessing any application on intranet. • Smart cards with “Biometrics” activated turnstiles which require two factor authentication including fingerprint scan and electronic access card have been deployed across all India Development centers as illustrated below:
System and communications protection	Security controls that support the protection of the information system itself as well as communications with and within the information system	• To ensure the protection of information in networks and their supporting information processing facilities making use of latest technology combined with the right set of security controls. Following are some of the network security controls for providing security to the information transferred within the organization and with external entities.
Operational Security		
The operational security class consists of the following control families		

Technical Controls	Control Description	Infosys Public Services (Infosys) Security Practices
Operational Controls	Control Description	Infosys Public Services (Infosys) Security Practices
Awareness and training	Security controls that deal with the education of users with respect to the security of the information system	- Business Continuity Management System (BCMS) - BCMS awareness is ensured for all employees and focused training is provided to identify BCMS members. - Infosys - conducts a security awareness session at the time of induction programs for refreshers and lateral joiners. The flash video used for this training covers the overview of Infosys Security Policies and the dos and don'ts from a security perspective. The objective of the training is to make every employee familiar with the information security policy of Infosys. This training is provided on security objectives, and on their roles and responsibilities for security.
Configuration management	Security controls that support the management and control of all components of the information system (e.g., hardware, software, and configuration items)	Configuration Management security controls are involved in all artefacts generated during the lifecycle. - All servers are hardened using secure configuration standards. We have a defined process to monitor all threats including security vulnerabilities. The Information Security Group monitors vulnerability advisory sources for information on new vulnerabilities and patches. When security updates are released by the vendor, we tests them & issues an internal vulnerability advisory to relevant departments. The Computers and Communication Division (CCD) is responsible for deploying the patches to end user systems through Microsoft SMS / SCCM. - All project data is stored on access-controlled file servers which is restricted to authorized personnel working on the project strictly on a need to know and least privilege basis. The list of individuals having access is subjected to regular reviews by the Project Configuration Controller.
Contingency planning	Security controls that support the availability of the information system services in the event of component failure or disaster	The Business Continuity Management System (BCMS) is managed as a program known as the Phoenix program. The Phoenix team is responsible for planning and implementation of controls and ensuring adherence to compliance related to BCMS as per the ISO 22301 standard. The BCMS program provides following :

Technical Controls	Control Description	Infosys Public Services (Infosys) Security Practices
		○ Is responsible for organizational, location and account level BCMS requirements. ○ Composes of key members from identified functions like IT, Facilities, HR, IS, Security, Delivery, and Infrastructure groups. ○ All Development Centre's (DCs) act as backup and recovery sites. ○ Applicable redundancy built into all essential infrastructures including office space, network connectivity, power, computing resources and personnel. ○ All DCs have adequate food, water, power, limited accommodation facilities to last at least 3-4 days in case of any emergency. ○ BCMS exercises are planned and performed at corporate, locational and engagement levels. ○ BCMS awareness is ensured for all employees and focused trainings are provided to identified BCMS members ○ BCMS reviews are covered through self-assessments and audits through internal and external audits ● Assessed and Certified for ISO 22301 standard for process adequacy and coverage. The Business Continuity Management Planning is broadly divided into 4 interdependent components : ○ Corporate Level Plan ○ Functional Level Plan ○ Development Centre/Location Level Plan ○ Account/Engagement Level Plan
Incident response	Security controls that support the detection, response, and reporting of security incidents within the information system	Information Security Incident Management involves: ● Institute systems and practices to receive alerts when incidents occur, and to handle the incidents as soon as they occur. ● Ensures that incidents are handled according to the process. ● Analyze incidents for trends ● Real time monitoring of logs through a Global Security Operation Centre (SOC) which operates in a 24X7 model

Technical Controls	Control Description	Infosys Public Services (Infosys) Security Practices
		- Real time security incident management through: - Detecting the possible attacks targeted to Network(External and Internal) - Identifying the origin of the attack with detailed investigation and remediating/ resolving the impact of the attack - Finding the root cause, taking corrective and preventive measures - Maintaining the learning from incidents as knowledge base - Perform forensic investigations of information and communications technology systems involved in incidents - Conduct Malware Analysis
Maintenance	Security controls that support the maintenance of the information system to ensure its ongoing availability	All IT infrastructure assets are recorded in an asset management system called AMANAT. Inventory is maintained for all physical assets and is reconciled periodically with internal systems. Infosys has deployed stringent controls for all asset movement into or out of the premises. Any material being brought into premises by anyone is subject to inspection by the security guard at entrance. Premises are classified as a customs bonded area and hence material is moved into or out of the building strictly per Government-prescribed procedures. All equipment/materials in the bonded area are subject to audits by the concerned government departments.
Media protection	security controls that support the protection of information system media (e.g., disks and tapes) throughout their life cycle	- Data Security - Data on media is erased using secure disposal methods. Hard copies, Paper documents are shredded, and floppies/CDs/DVDs are physically destroyed, and magnetic tapes are degaussed. - For the purpose of Disk Level encryption, all laptops are installed with FDE (Full disk encryption). - We follow a process of taking daily backup of Information onto backup tapes in case of dedicated, standalone servers. In all other scenarios, data is stored on NAS and the backups are triggered at regular intervals over the network.
Physical and environmental protection	Security controls that support the control of physical access to an information system	The Physical and Environmental Security Controls are implemented by Physical Security and Facilities departments respectively. We have implemented adequate controls for Physical & Environmental

Technical Controls	Control Description	Infosys Public Services (Infosys) Security Practices
	as well as the protection of the environmental ancillary equipment (i.e., power, air conditioning and wiring) used to support the operation of the information system	security. Some of the controls at the Campus, Building & Data Center level are: • Campus Security ○ All the campus entry and exit points are manned 24x7 by the security guards. ○ Baggage & vehicle check is carried out at all entry and exit points. ○ Smart cards with “Biometrics” activated turnstiles which require two factor authentication including finger print scan and electronic access card have been deployed across all India Development centers as illustrated below: ○ If an employee forgets the ID card, a temporary pass is issued to the person and the physical access to the proximity card allocated to the employee is deactivated for that particular day. The temporary pass is returned to the physical security team when the employee leaves the premises. ○ All visitors are assigned photo IDs and are always accompanied by authorized personnel to gain entry to the premises. • Building Security control involving: ○ Security guards are deployed for each building at all times across locations. ○ Turnstiles are present at all building entrance for authorized access. ○ Appropriate security controls like access control doors, CCTVs are deployed across multiple geo locations. ○ Environmental Security Controls (fire alarms, smoke detectors, extinguishers etc.) are installed in all buildings. ○ Project specific security requirements can be established (e.g., CCTV, Physically secured area- Offshore Development Center (ODC) etc.) ○ The Restricted Area Access System (RAAS) is used to manage Physical Security access control for ODCs. ○ The system allows allocation and de allocation of Physical access to an ODC area for individuals on a business need-to-have basis. • Data Center Security Control involving:

Technical Controls	Control Description	Infosys Public Services (Infosys) Security Practices
		○ Access control is implemented using proximity cards (for data centers and server rooms). Only authorized personnel can enter the data center. ○ CCTV Monitoring, Temperature & Humidity controls are implemented in all server rooms. ○ Gas Based Fire Suppression system (FM 200) has been implemented for select Data centers.
Personnel security	security controls that support the procedures required to ensure that all personnel who have access to the information system have the required authorizations as well as the appropriate security screening levels	The Human Resource Department is responsible for handling Personnel security. • All visitors are assigned photo IDs and are always accompanied by authorized personnel to gain entry to the premises. • Access control is implemented using proximity cards (for data centers server rooms). Only authorized personnel can enter data center. • All project data is stored on access-controlled file servers which is restricted to authorized personnel working on the project strictly on a need to know and least privilege basis. The list of individuals having access is subjected to regular reviews by the Project Configuration Controller.
System and information integrity	security controls that support the protection of the integrity of the information system components and the data that it processes	• Information security is a top concern for the organization and so the IT security framework is designed to ensure the selection of adequate and proportionate security controls to protect the whole gamut of information assets. • Communications Security ○ To ensure the protection of information in networks and its supporting information processing facilities we make use of latest technology combined with the right set of security controls. Following are some of the network security controls for providing security to the information transferred within the organization and with external entities. • Network Security ○ All external connections (e.g., customer connection, internet connectivity) are secured using a state of the art inspection firewall.

Technical Controls	Control Description	Infosys Public Services (Infosys) Security Practices
		○ Access to a customer network is restricted and provided only to required resources using approved access methods of customer. ○ DMZs are protected by Network Intrusion Prevention systems (IPS). ○ We have implemented 802.1x network access control (NAC) mechanism wherein only authenticated endpoints (workstations, laptop) having valid certificate can connect to the corporate network, thereby preventing rogue devices from connecting. ○ Access to internet is restricted and internet access Policy is enforced using internet content filtering technology. ○ The perimeter is protected by NIPS (Network Intrusion Prevention System) which is updated by latest signatures. ○ Vulnerability assessments are performed in-house using Industry standard tools and techniques to identify vulnerabilities. These Vulnerability tests are performed on a periodic basis and the identified vulnerabilities are tracked to closure. Continuous monitoring of critical servers for vulnerabilities ensures that has Secure Infrastructure.

Management Security

The management security class consists of the following control families

Management Control	Control Description	Infosys Public Services (Infosys) Security Practices
Security assessment and authorization	Security controls that deal with the security assessment and authorization of the information system;	● Corporate Certification, Assessment and Audit team (C-CAT) conducts organization-wide audits and assessments which ensures continual improvement and adherence to various industry certification standards. ● Data is encrypted using authorized systems and processes only. Only well established and proven encryption algorithms are used ● At Infosys, Information Security Group department is responsible for information security related activities including assessments of internal systems for compliance with security policies & regulatory standards.

Technical Controls	Control Description	Infosys Public Services (Infosys) Security Practices
		• Vulnerability assessments are performed in-house using Industry standard tools and techniques to identify vulnerabilities. These Vulnerability tests are performed on a periodic basis and the identified vulnerabilities are tracked to closure. Continuous monitoring of critical servers for vulnerabilities ensures we have Secure Infrastructure. • BCMS reviews are covered through self-assessments and audits through internal and external audits • Digital Rights Management System (DRMS) has been implemented which helps safeguard information from unauthorized usage – both online & offline. DRMS has helped to prevent sensitive emails, other critical and sensitive documents from being forwarded, printed or copied. • All project data is stored on access-controlled file servers which is restricted to authorized personnel working on the project strictly on a need to know and least privilege basis. The list of individuals having access is subjected to regular reviews by the Project Configuration Controller.
Planning	Security controls that deal with security planning activities including privacy impact assessments	The Business Continuity Management System (BCMS) is managed as a program known as the Phoenix program. The Phoenix team is responsible for planning and implementation of controls and ensuring adherence to compliance related to BCMS as per the ISO 22301 standard. The Infosys Business Continuity Management Planning is broadly divided into 4 interdependent components. • Corporate Level Plan • Functional Level Plan • Development Centre • Location Level Plan The Infosys Legal department looks after compliance with regulations of the different geographies. Infosys assists its customers' compliance with any applicable regulations.
Risk assessment	Security controls that deal with the conduct of risk assessments and	• Infosys Information Security Group, Computers & Communications Division (CCD), Information Systems (IS), Quality & Productivity, Delivery Risk Management, Commercial, Facilities,

Technical Controls	Control Description	Infosys Public Services (Infosys) Security Practices
	vulnerability scanning	Administration and Security, Human Resource, Chief Risk Officer, IP Cell, Privacy & Data Protection. The ISC is headed by the COO who is a Member of the Board. • Information Security Risk Management • Facilitate the implementation of information security controls in all units, departments, accounts, development centers and other facilities, including subsidiaries. • Facilitate the implementation of new security initiatives. • Review internal and external audit findings and facilitate closure of enterprise level security risks • Facilitate preparation for organization level external audits such as ISO 27001, customer audits, SSAE16 & PCI DSS audits etc. • Analysis and closure of risks arising from recurring audit findings • Perform risk assessments for the enterprise. • Implement procedures for collection of information security metrics to demonstrate effectiveness of security controls • Participate in meetings with customers and prospects and address their information security requirements • Define solutions for spreading security awareness and manage their development, implementation and operation. • Provide pre-engagement support in terms of responding to RFI/RFPs or reviewing information security clauses in agreements with customers and vendors • Periodically verify and certify contractual security obligations of engagements
System and services acquisition	Security controls that deal with the contracting of products and services required to support the implementation and operation of the information system	Implementation of Security Controls • IT Security controls at Infosys are implemented by the Computers & Communications Division (CCD). The Computers & Communications Division is responsible for the IT infrastructure management of the entire enterprise. • The Physical and Environmental Security Controls are implemented by Physical Security and Facilities departments respectively. The

Technical Controls	Control Description	Infosys Public Services (Infosys) Security Practices
		Human Resource Department is responsible for handling Personnel security. • The Contractual and Legal compliance aspects related to Information Security are handled by the Legal Department. • Service account monitoring: Through advanced identity correlation and behavior analysis, highly sensitive service and shared accounts are automatically identified and monitored for outlier behavior such as new connection types, addresses, times, frequency, amount – all of which are reliable indicators of a compromise.

Data privacy requirements implemented by Infosys during project execution originate from the client, data privacy regulations or Infosys privacy policy. Infosys, being a data processor, processes personal information only for providing services to the client, as documented in the services agreements. Personal data will not be used for any purpose other than that specified by the client.

In addition to the non-disclosure agreement signed by each Infosys employee regardless of the project they work for, when client or regulations require additional declaration, appropriate mechanism will be implemented by the Infosys project execution team. Records of such declaration including commitment to confidentiality shall be maintained by Infosys. All employees shall undergo mandatory data privacy awareness training and quiz at least once every year.

When Infosys subcontracts personal/sensitive data processing of client to a third party for further processing, it will be done with the prior written approval of the client and only after establishing that the third party has means to protect data as required by regulations and inclusion of all data privacy clauses present in the contract between Infosys and the client into the contract between Infosys and the subcontractor.

Any personal data obtained from the client for during the tenure of the contract shall not be retained and will be destroyed or returned, as required by the client, when the agreed retention period lapses unless legal requirements need longer retention.

For Public cloud services, such controls are validated through the cloud vendor third party certifications, review existing privacy policies/controls and ensure the same is aligned with State requirements. Appropriate organizational and technical security measures shall be implemented for protecting personal/sensitive data, as mentioned above.

Breach notification, as per the process mentioned in Section 1.2.4.10, will be followed by Infosys for notifying the client about any personal data breach.

Infosys' corporate audit and assessment team will conduct periodic audits to verify that project teams are adhering to the security and privacy requirements mandated by the client or law.

1.2.4.3 Security Certifications

The State of Maine eProcurement Solution and services will contain protected data, such as Procurement Contracts, tenders and bid submissions with commercially sensitive information. It is critical that State of Maine eProcurement Solutions and services and its data receive highest level of security protection. When selecting a SaaS solution for State of Maine eProcurement Solutions, Infosys has gone through extensive review and assessment of solution options, not only from

application solution fitness perspectives, but also from application security compliance perspectives. We have selected product and services for that are compliant with key industry IT security standards and are certified by primary Industry IT Security Certification programs.

In addition, as a leading technology company, Infosys itself has rigorous IT security policies, procedures, and training programs in place. This is to ensure our clients' systems and data are well protected, and security audit and monitoring programs are in place to provide expedient resolutions in case of any security breaches or incidents.

This section summarizes our Industry IT Security Certification demonstrating the below:

Industry IT Security Certifications are provided for the following entities:

- State of Maine Bidder: Infosys Public Services
- State of Maine Bidder Service Partner: EY
- State of Maine Bidder SaaS Product Provider: SAP, OCI and ServiceNow

All the above entities have rigorous and disciplined policies in place to obtain and renew these IT Security Certifications. See details below.

State of Maine Bidder: Infosys Industry IT Security Certification

Infosys, as the primary system integrator for the State of Maine eProcurement Solutions and services is a CMMi Level 5 certified organization. The maturity, quality systems and rigor of our processes extend to our stringent security and data controls processes. We have routine and on-going training of all our employees and system security audits, to ensure that our data and systems are protected. Infosys as an organization is aligned and certified to ISO 27001:2013 standard. Moreover, Infosys Limited as an organization is assessed for SSAE 18 SOC 1 Type II by one of the large public accounting organizations.

An engagement specific PCI DSS compliance could be planned in case the Infosys offshore engagement stores, processes and or transmits any card holder information of the Customer. Based on applicability, Customer shall provide advance notice to Infosys when access to cardholder data is made available to Infosys. Both parties shall discuss and mutually agree upon the timeframe by when compliance against this standard would (e.g., PCI DSS, HIPAA, FISMA, NIST, SSAE 16 SOC 1 and SOC 2 etc.) be achieved. The cost for the certification, implementation of controls & procurement of additional tools as required for PCI DSS certification would have to be borne by the Customer. Furthermore, the engagement would have to operate from a physically isolated ODC environment as per the expectations of PCI DSS. Nevertheless, if any State of Maine eProcurement Solutions has protected health information access at offshore, Infosys will ensure that the State of Maine eProcurement Solutions is meeting the compliance requirements of HIPAA by the implementing appropriate Technical, Physical and Administrative safeguards.



KPMG Assurance and Consulting Services LLP
Embassy Golf Links Business Park
Pebble Beach, B Block, 1st and 2nd Floor
Off Intermediate Ring Road
Bengaluru 560 071 India

Telephone: +91 80 6833 5000
Fax: +91 80 6833 6999
Web: www.kpmg.com/in
Email: indiawebsite@kpmg.com

Infosys Limited
44, Electronic City, Hosur Road
Bangalore – 560100, India

24 December 2020

Attention: Nabarun Roy, Senior Vice President, Group Head – Quality

KPMG Assurance and Consulting Services LLP (hereinafter referred to as “KPMG”, “We”, “Our”) have completed SOC 1 Type 2 examination for Infosys Limited (herein after referred to as “Infosys” or “service organization”) as outlined in our engagement letter dated 17 September 2020. This report to you represents our final report for SOC 1 Type 2 examination.

The data included in this report was obtained from you, on or before 30 November 2020. We have no obligation to update our report or to revise the information contained therein to reflect events and transactions occurring subsequent to 30 November 2020. The attached report is the electronic version of our signed deliverable, which has been issued to you in the hard copy format.

This report sets forth our views based on the completeness and accuracy of the facts stated to KPMG and any assumptions that were included. If any of the facts and assumptions is not complete or accurate, it is imperative that we be informed accordingly, as the inaccuracy or incompleteness thereof could have a material effect on our conclusions.

This report is intended solely for the information and use of the management of Infosys, its user entities and the independent auditors of user entities (collectively referred to as authorized parties) and is not intended to be, and should not be, used by anyone other than these authorized parties. If this report is received by anyone other than authorized parties, the recipient is placed on notice that the attached SOC 1 report has been prepared solely for authorized parties for their internal use and this report and its contents shall not be shared with or disclosed to anyone by the recipient without the express written consent of Infosys and KPMG. KPMG shall have no liability and shall pursue all available legal and equitable remedies against recipient, for the unauthorized use or distribution of this report.

Please contact us if you have any questions or comments. We look forward to providing services to your company.

Yours sincerely,

M.N. Gururaja
Partner, KPMG Assurance and Consulting Services LLP

Figure 44. SOC 1 Report



KPMG Assurance and Consulting Services LLP
 Embassy Golf Link Business Park
 Pebble Beach, B Block, 1st and 2nd Floor
 Off Intermediate Ring Road
 Bengaluru 560 071, India

Telephone +91 80 6833 5000
 Fax +91 80 6833 6999
 Internet www.in.kpmg.com

Mr. Nabarun Roy
 Senior Vice President
 Group Head - Quality
 Infosys Limited,
 44, Electronic City, Hosur Road
 Bangalore – 560 100, India

18 January 2021

Dear Nabarun Roy,

We have completed SOC 2 Type 2 examination for controls related to Infosys Limited's General Operating Environment supporting the delivery of Technology Services for Trust Services Criteria Security, Availability and Confidentiality from the delivery centers located in India covering an audit period 01 October 2019 to 30 September 2020 as outlined in our engagement letter.

The report contains the following:

Section 1: This section contains KPMG overall opinion. For the said audit period, KPMG noted that there is reasonable assurance that control objectives included in the report are met and therefore, the report is an unqualified report.

Section 2: This section contains the management assertion provided by Infosys, which has been included in the report.
 Section 3: This section contains the description of the system provided by Infosys, which includes overall control environment, risk assessment, information and communication systems, monitoring and control activities.

Section 4: This section contains the details of trust services category, criteria, control activities, test procedures performed by KPMG and results of testing.

We would like to thank the senior management at Infosys for the executive sponsorship provided to this program, which was key to the success of this program. We would also like to thank the teams involved for the support extended to us during the course of the audit.

We have provided a copy of the report to you separately. The data included in this report was obtained from you, on or before 10 December 2020. We have no obligation to update our report or to revise the information contained therein to reflect events and transactions occurring subsequent to 10 December 2020.

Please contact us if you have any questions or comments. We look forward to providing services to your company.

Yours sincerely,

M N Gururaja
 Partner, KPMG Assurance and Consulting Services LLP

Figure 45. SOC 2 Report

State of Maine Team Member: Ernst & Young

Ernst & Young (EY), Infosys' partner on the State of Maine eProcurement program, has obtained and maintains the ISO/IEC 27001 certificate. EY has stringent security and data controls processes and have routine and on-going training of all its employees and system security audits, to ensure that our data and systems are protected. This certification is renewed every 3 years to allow review of the latest security and controls processes and IT environment in place.

State of Maine eProcurement SaaS Product Provider: SAP Industry IT Security Certification

Third-party certification bodies provide independent confirmation that SAP meets the requirements of international standards. Since 1998 SAP has held an ISO 9001 certificate. We are also certified according to ISO 27001, ISO 22301, and BS 10012. All locations worldwide work according to one common process framework, including data security and privacy regulations. We regularly check compliance through internal reviews and audits



Figure 46. SAP ISO/IEC 27001 Certificate

SAP Ariba solutions demonstrate the information security assurances by complying with industry - recognized standards and regulations. Compliance with the standards is measured through either annual or semiannual audits. Current attestation reports and certificates can be made available upon request.

Further details regarding SOC compliance can be found in SAP Trust Center website by searching Ariba SOC Compliance.

Upon request respective compliance certifications and associated artefacts can be made available to

the State or a participating entity.

SAP Ariba is audited and certified by independent third-party auditor PricewaterhouseCoopers (PwC) for compliance with ISAE 3402 SOC1 Type II, SOC2 every six months. A SOC 3 report is issued annually. Upon completion of the audit, an attestation letter is issued, stating our compliance. In addition, our primary hosting facility (Equinix) infrastructure is audited for compliance with SSAE 16 SOC1 Type II, SOC 2 Type II.

The Service Organization Controls report (SOC) is aimed at three different audiences. SOC1 (aimed at financial auditors) is the same type of report as the SAS70 but also includes an attestation letter signed by both our company and the auditor. SOC2 is aimed at IT and security practitioners. The SOC3 is the publicly viewable web seal to show that we have been audited.

Further details regarding SOC compliance can be found in SAP Trust Center website by searching Ariba SOC Compliance.

Upon request respective compliance certifications and associated artefacts can be made available to the State or a participating entity.

In addition, we have attained PCI (Payment Card Industry) - DSS (Data Security Standard) certification as a Level 1 Service Provider and compliance with the Visa USA Cardholder Information Security Program (CISP) and MasterCard Site Data Protection (SDP) program. These programs were created specifically for merchants and service providers who process, store, or transmit cardholder data.

The PCI DSS is a set of comprehensive requirements for enhancing payment account data security which was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. It was developed to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data. CISP and SDP reflect Visa's and MasterCard's respective longstanding commitment to information security.

Further details regarding compliance can be found in SAP Trust Center website by searching Ariba Compliance.

Upon request respective compliance certifications and associated artefacts can be made available to the State or a participating entity.

NOTE: Many of the certifications are available for download on the SAP Trust Center website.

We are not designed to handle HIPAA data. Our solutions are designed Business to business transaction, and we do not support storing HIPAA/PII/Personal data.

The following figures explain the regulations and standards that SAP Ariba solutions comply with, are in the process of certifying, or are attesting this compliance.

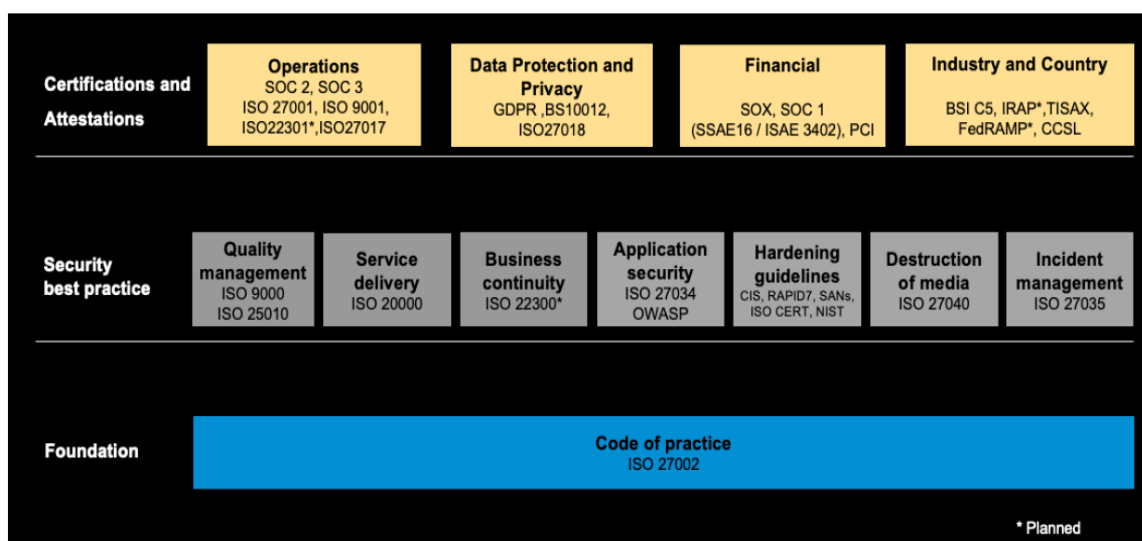


Figure 47. SAP Ariba Regulations and Standards Compliance

The below table shows the details of certifications and regulations SaaS vendors comply with:

Table 30. Vendor Certifications

SaaS Vendor	Certification
SAP Ariba	• ISAE 3402 SOC1 (formerly SAS 70), SOC2 and SOC3 • SAP Ariba PCI-DSS AOC 2020 • ISO 27001/27002, ISO/IEC 27032 and ISO 27018, ISO 9001
ServiceNow	• SSAE16 SOC 1 Type 2 and SOC 2 Type 2 since 2013, • ISO 27001 certified organization since 2012, 27018 • FedRamp Moderate JABP-ATO • US DoD impact Level 2 • EU Privacy Shield • Multi-Tier cloud security standard • Australian signals directorate
Microsoft Azure	• ISO 27001, ISO 9001, SSAE 18 SOC 1, SOC2, SOC 3 • FedRAMP, NIST ITSP 800-171, NIST SP 800-53 Rev. 4 • IRS 1075 September 2016 • HIPAA HITRUST 9.2
Oracle Cloud Infrastructure	• Cloud Security Alliance Security Trust Assurance and Risk • ISO 9001: Quality Management Systems • ISO/IEC 27001: Information Security Management Systems • Payment Card Industry Data Security Standard • System and Organization Controls 2 SOC2 • HITRUST CSF • FedRAMP

SaaS Vendor	Certification
	HIPAA (Health Insurance Portability and Accountability Act)
Acquia	- SOC 1 (SSAE No. 18 and ISAE No. 3402) - SOC 2 - PCI DSS (Payment Card Industry Data Security Standard) - ISO 27001 certification - FedRAMP - FISMA - CSA STAR (Cloud Security Alliance Security, Trust and Assurance Registry) - HIPAA(Health Insurance Portability and Accountability Act)
Saviynt	- ISO 27001:2013 - ISO 27017:2015 - Type 2 SOC 2 Report - FedRAMP

State of Maine eProcurement SaaS Product Provider: Oracle IT Security Certification

Oracle

Oracle provides information about frameworks for which an Oracle line of business has achieved a third-party attestation or certification for one or more of its services in the form of “attestations.” These attestations can assist in determining compliance and reporting, providing independent assessment of the security, privacy and compliance controls of the applicable Oracle cloud services. In reviewing these third-party attestations, it is important that you consider they are generally specific to a certain cloud service and may also be specific to a certain data center or geographic region.

State of Maine eProcurement SaaS Product Provider: ServiceNow IT Security Certification

ServiceNow

Every year ServiceNow is rigorously audited by independent third-party companies and government bodies to prove that they comply with various global and regional standards.

ServiceNow is audited annually by a third party and has maintained its SSAE 18 SOC 1 Type 2 attestation since 2011 (SSAE 18 superseded SSAE 16 in 2017). SSAE 18 is aligned with international standard ISAE3402 and replaced the now-deprecated SAS70. ServiceNow has also undertaken an annual SOC 2 Type 2 attestation since 2013, relevant to security, availability and confidentiality controls listed in the AICPA Trust Services Criteria (TSC).

HITRUST was developed by the healthcare industry to standardize compliance objectives through their CSF Framework of controls, originally built on ISO27001. They have since incorporated and mapped to many common security standards, including NIST 800-53 and the AICPA SOC 2 Trust Services Criteria. The SOC 2 + HITRUST report is a collaboration between the AICPA and the HITRUST Alliance. It provides a mechanism for the service auditor to opine on the design and

effectiveness of the Trust Services Criteria and the HITRUST CSF in the same report.

ServiceNow has the U.S. Federal Risk and Authorization Management Program Joint Authorization Board P-ATO (FedRAMP JAB) at the High level. ServiceNow received its JAB High Provisional Authority to Operate (P-ATO) in 2019. The FedRAMP JAB High P-ATO also meets the requirements for DoD Impact Level 4. In addition, ISO/IEC 27017:2015 standard is concerned with the implementation of the cloud-specific information security controls specified in ISO/IEC 27002. The certification is gained by an annual independent audit and ServiceNow has been an ISO/IEC 27017:2015 certified organization since 2018.

State of Maine eProcurement SaaS Product Provider: Microsoft Azure IT Security Certification

Azure AD

Azure compliance offerings are based on various types of assurances, including formal certifications, attestations, validations, authorizations, and assessments produced by independent third-party auditing firms, as well as contractual amendments, self-assessments, and customer guidance documents produced by Microsoft. Azure compliance offerings are grouped into four segments: globally applicable, US government, industry specific, and region/country specific.

Azure adheres to security controls for ISO 27001, ISO 27018, SOC 1, SOC 2, SOC3, FedRAMP, HITRUST, MTCS, IRAP, and ENS. Microsoft Azure maintains a PCI DSS validation using an approved Qualified Security Assessor (QSA) and is certified as compliant under PCI DSS version 3.2.1 at Service Provider Level 1.

State of Maine eProcurement SaaS Product Provider: Saviynt IT Security Certification

Saviynt

Saviynt has completed information security compliance initiatives like; ISO/IEC 27001 and ISO/IEC 27017 for Saviynt Identity Governance and Cloud Security Solution on both AWS and Azure. Saviynt is certified at the FedRAMP Moderate level which indicates that there are significant controls in place to prevent the loss of confidentiality, integrity or availability of an agency's assets, or finances.

In addition to FedRAMP authorization, ISO/IEC 27001 and ISO/IEC 27017, Saviynt also completed the examination for SOC 1 Type 2 and SOC 2 Type 2.

1.2.4.4 Annual Security Plan

Infosys will develop a detailed security plan (SSP) which will provide an overview the proposed solution, describe the controls in place or planned, responsibilities and expected behavior of all individuals who access the system.

It must be noted that currently application specific controls, deployment and operations related controls can be implemented independently and will inherit existing controls applicable at agency level such as data center controls, network security, media protection, etc. Infosys will work with State authorized security and privacy officer to develop a detailed Security Plan, conduct privacy impact analysis and risk assessments to ensure compliance requirements are addressed through the lifecycle of the project. The diagram below provides Infosys approach to developing the Information Security Plan and supporting deliverables produced at various stages of the implementation phase :

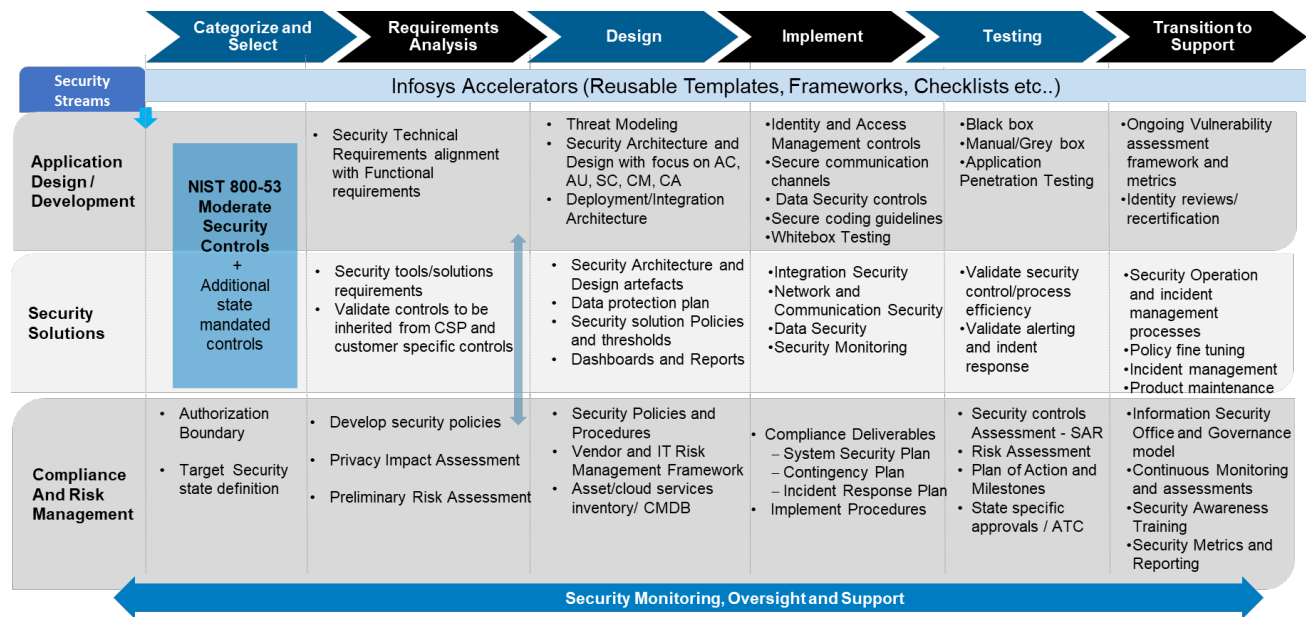


Figure 48. Stages of Security Control Implementation

- **Security Policies;** Infosys will develop EPS solution specific policies per NIST 800-53 requirements and align with Maine/ Participating entity security policies which may need to be inherited for scenarios like user administration, integration with state's on-premise/legacy systems. All cloud vendors have established security policies and validated through SOC2 or FEDRAMP certification.
- **Logical security controls** (privacy, user access and authentication, user permissions) : the proposed solution has necessary modules and capabilities to meet user access and authentication requirements and if necessary integrate with State's existing identity management solution. Also, an optional Identity Management solution has been provided as part of the proposal if the State would like Infosys to implement and manage the solution. All application support role-based access control and each user can be mapped to specific roles which are required at minimum for performing their official duties. The proposed cloud service solutions are compliant with US and GDPR privacy requirements, in addition where necessary additional privacy controls such as user consent, reporting, incident management can be implemented in collaboration with State. All such logical controls will be designed and documented as part of the security strategy document and implemented
- **Technical security controls and security architecture:** the proposed solution comprises of best in breed cloud services trusted cloud vendors in the industry who have proven capabilities and established standards for technical security controls and architecture frameworks such as Zero trust architecture, defense in depth, etc. All cloud services inherit such robust security controls and used by large clients across Public and commercial sectors. For areas where additional technical security controls are required based on the cloud service model or integration between other EPS cloud services or external systems, Infosys will implement and document the same.
- **Security processes** – Infosys has developed standard security operational procedures and processes to be followed for operating and managing procurement solution for other customers with similar requirements. Infosys will leverage best practices and learnings from other clients to establish the security processes, adapt to the State's requirements where necessary and periodically monitor for efficiency and maturity.
- **Security Strategy** – As indicated in the solution description, procurement solution comprises

of leading cloud service providers who have implemented and proven technical security specifics to ensure the solutions allow secure adoption in a multi-tenancy model and assure confidentiality of information as a custodian.

Infosys in collaboration with State to facilitate privacy impact assessments to identify PII elements, associated information flows, assess sensitivity of information and systems and ensure necessary information handling protocols, processes are established.

Each cloud service provider is required to conduct continuous security assessments to comply and maintain the certifications. Security assessments include third party security assessment of security controls to comply with ISO, SOC2 or FedRamp, application vulnerability and penetration testing. Such reports can be made available to State on request. Infosys will conduct additional security tests during the implementation phase such to ensure secure configuration of the cloud services, secure integration mechanisms and vulnerability assessment for any custom developed solution modules.

All the above controls will be validated and ensure the current status is accurately reflected in the Security plan, supporting artefacts are produced, any gaps identified during the process will be documented and tracked for closure.

- **Detailed diagrams** – Infosys will provide the detailed diagrams depicting the capability offered by each cloud service within the procurement solution, integrations and data flows between different cloud services/external systems, protocols, Authentication and Access controls in place, etc. the diagrams will be included as part of the information security plan.

In addition to the cloud service provider policies, Infosys will inherit organizational security controls for managing its employees and their access to endpoint devices, network security etc.

Below are the Overall Security Controls at Infosys



Figure 49. Infosys Overall Security Controls

As an organization, Infosys is ISO27001:2013 certified, and therefore, all of our policies, processes, and standards are in line with internationally accepted standard. However, Infosys caters to clients belonging to a wide variety of industry domains and geographies. We also take cognizance of the cyber security requirements of our clients and the regulations which are applicable to their geography, e.g. Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA) for healthcare domain, Payment Card Industry Security Standard (PCI-

DSS) for cardholder data protection, etc. Internal audits, risk assessments, periodic reviews of contractual obligations, vulnerability assessments, and penetration tests are some of the other services that are provided at the engagement level.

Infosys has extensive experience in implementing Information Security Management Framework for our customers or for a managed services platform operated on behalf of client. As requested in the RFP, Security Plan will include the below:

- High-level description of the program and projects.
- **Security risks and concerns:** Infosys will implement cloud service management process to help classify all information and services/assets based on their business impact and criticality and to thereby guide the stakeholders implement relevant Security controls, accordingly, Identify and manage Security Risks to the procurement solution platform, analyze recurring risk patterns and implement preventive measures to mitigate or avoid recurrence of risks.
- **Security roles and responsibilities** – For the State of Maine, Infosys will assign a dedicated Security Lead/Officer with expertise in managing implementation and maintaining information security plan. He will work closely with State of Maine's security organization, SaaS vendors, and State of Maine Project team to ensure that proposed solution once fully integrated and operational is compliant with NIST 800-53. Security Lead will be responsible in establishing and executing IT security plan for State of Maine and develop a RACI (Responsible, Accountable, Consulted, Informed) Model was discussed with all Information Security stakeholders and agreed for seamless Cyber Security Management.
- **Program and project security policies and guidelines:** Infosys will inherit existing cloud service provider policies, its organizational policies for its staff implementing and managing the procurement solution and develop State specific security and policy for the procurement solution platform management.
- **Security-specific project deliverables and processes:** Infosys will develop additional project specific deliverables such as security strategy/design document, policies and procedures, operations manual, security test plan and test results,
- **Security team review and approval process:** a dedicated security team led by information security officer will be responsible to review and ensure the overall security controls required to secure the procurement solution are implemented, all ongoing changes and enhancements are reviewed, and security impact assessment (SIA) is conducted before approving change. Security review and approval will be integrated with the IT Service Management processes and documented.
- **Security-Identity management and Access Control for Bidder and Participating Entity joiners, movers, and leavers:** Infosys in collaboration with the state will define user Lifecycle management with respect to identity and access management are defined. As part of the response, Infosys has provided an option for state to request Infosys to implement Identity management solution or integrate the solution with state's identity management solution. Based on the solution option chosen by the state, Infosys will align the use lifecycle management policy and process accordingly.

Summary

The Infosys Information Security Program is an essential element of all engagements. As part of safeguarding the information customers entrust to Infosys, this program has helped build customer confidence and assurance, thus demonstrating the commitment and credibility of Infosys to all its stakeholders. The information security practices at Infosys have evolved to look beyond compliance. The Information Security metrics program has been contributing to the continuous improvement of the existing security practices and in integrating the Information security within the business processes. Information management being an essential part of a good IT governance is a cornerstone in Infosys

and has helped provide the organization a robust foundation. Information security is a top concern for the organization and so the IT security framework is designed to ensure the selection of adequate and proportionate security controls to protect the whole gamut of information assets. There is a concerted effort from top management down to the end-users as part of the development and implementation process and care is taken to ensure that standardized policies or guidelines are applicable to and practical for the organization's culture, business, and operational practices.

Information Security requires participation from all spheres of the organization. Senior management, information security practitioners, IT professionals and users all have a pivotal role to play in securing the assets of an organization. The success of information security can only be achieved by full cooperation at all levels of an organization, both inside and outside and this is what defines the level of commitment here at Infosys.

The Infosys Team will secure information assets using an integrated data privacy and information security strategy:

- We align our information security governance with our data privacy governance to provide a consistent, cohesive vision around the protection of our information assets, personal data and client information.
- We subject our global applications and systems to both data privacy impact assessments and security certification reviews, which support a robust, consistent approach in deployment and operation.
- We protect personal data within our network using appropriate physical, technical, and organizational security measures.
- We provide assurance that our policy contract will contain provisions that will be commensurate with policies, practices, and controls to confirm your data is managed properly and securely, in accordance with the State of Maine's stated requirements.

1.2.4.5 *Secure Application and Network Environment*

The State of Maine solution leverages various cloud models and the deployment model varies from one service model to the other. However, for each CSP, it has been validated that deployment aspects have been implemented and demonstrate compliance to State's Security requirements. CSP's provide a secure foundation across the physical network infrastructure, application infrastructure and operational security.

The core of the Maine Solution offered is with our partner SAP and other Cloud applications. Which constitutes of various modules within SAP's SaaS offering namely Discovery and Ariba network. In addition, we will utilize the capabilities of the ServiceNow Cloud together with Saviynt IAM feature, Azure Active Directory to cater our needs for the State of Maine Portal deployed on Drupal's Acquia. The sections below demonstrate the security posture of each component in the solution:

1. SAP Ariba

Boundary Protection: SAP Ariba provides 24/7 monitoring from a SOC as part of the service.

All devices are under continuous monitoring, comparing their running configuration to an approved stored configuration.

The management software provides logging at the system, network, and application levels where both informational and exception data is tracked. The systems maintain a system log of related information and the firewall generates logs via syslog as well. The application generates an extensive number of informational logs when a client authenticates, sends a notification, changes a configuration, etc.

The application also generates logs and alerts when exceptions occur.

Audit logs are maintained on the hosting network monitoring system. There are audit logs generated from the web server; monitoring is automated, and alerts are sent to operations personnel. While monitoring of audit logs is automated, alerts are sent to operations staff when an issue is detected, operations staff regularly review audit logs.

A firewall separates the SAP Ariba corporate network from SAP Ariba cloud solution infrastructure. Therefore, unauthorized SAP Ariba employees cannot access SAP Ariba cloud solutions data from the SAP Ariba corporate network infrastructure. Access is limited to specific roles or functions within the SAP Ariba Cloud Engineering Services team. Additionally, access is managed on an “exception” basis whereby personnel need clearance to be authorized. Access is time-limited, after which time re-authentication is required.

Authentication: SAP users are required to log on via jump hosts to the cloud customer systems using 2-factor authentication (username, password, and a token) compliant to SAP security policies.

Only certified representatives of SAP Ariba have access to SAP Ariba computers within the data centers. These data centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, biometrics access control, and other measures to prevent equipment and data center facilities from being compromised. Access history is recorded for audit purposes.

Security Plans and Policies: SAP Ariba has an internal security policy and various processes and procedures that are outlined in documents that are managed, updated and adhered to by the SAP Ariba Cloud Engineering Services team. These documents include descriptions of processes to follow for database recovery, database extracts, and other systems maintenance tasks.

Unauthorized Access: All devices are under continuous monitoring, comparing their running configuration to an approved stored configuration.

The management software provides logging at the system, network, and application levels where both informational and exception data is tracked. The systems maintain a system log of related information and the firewall generates logs via syslog as well. The application generates an extensive number of informational logs when a client authenticates, sends a notification, changes a configuration, etc.

The application also generates logs and alerts when exceptions occur.

Audit logs are maintained on the hosting network monitoring system. There are audit logs generated from the web server; monitoring is automated, and alerts are sent to operations personnel. While monitoring of audit logs is automated, alerts are sent to operations staff when an issue is detected, operations staff regularly review audit logs.

We are committed to the security and integrity of customer information. We utilize security measures to protect against the loss, misuse, or alteration of the information under our control. To prevent unauthorized access, maintain data accuracy, and facilitate the correct use of information, we have put in place appropriate physical, electronic, and managerial procedures to safeguard and secure the information we collect within the solution.

From time to time, security-related white papers are also available to customers and prospects offering further detail regarding our approach to secure architecture. Customers can review the SAP Ariba SOC II report issued by our independent third-party auditor, which offers detail as to the security controls in place for the SAP Ariba cloud applications.

SAP Ariba uses internally developed file integrity monitoring within the production network.

Maintenance Tools:

Equipment removal is required to be managed using both an internal ticketing system as well as a data center ticketing system for process control, audit and tracking purposes.

(a) Verifying that there is no organizational information contained on the equipment.

All items of equipment containing storage media are verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

SAP deletes the logical volumes, which will cause the storage device to re-use the storage space and overwrite the customer data. By deleting the logical volumes, customer data may not be accessed or extracted.

If hardware is removed from data centers a physical decommissioning process is applied. When an IaaS provider is used, processes for secure disposal of storage devices are managed by the infrastructure service provider.

(b) Sanitizing or destroying the equipment.

We have documented policies and procedures for the secure destruction of confidential or sensitive data. Our data disposal practices are aligned with the NIST 800-88 standards for clearing, sanitizing and data destruction to prevent data remanence prior to retiring or allowing storage media outside of our security envelope.

(c) Retaining the equipment within the facility; or

Equipment is located to minimize unnecessary access into work areas. Information processing facilities handling sensitive data are positioned carefully to reduce the risk of information being viewed by unauthorized persons during their use. Storage facilities are secured to avoid unauthorized access. Items requiring special protection are safeguarded to reduce the general level of protection required.

Controls are adopted to minimize the risk of potential physical and environmental threats, e.g., theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, and vandalism.

Business Continuity Plan: SAP Ariba's disaster recovery plan is updated at least annually. The company uses a variety of techniques to provide assurance that the plan will operate in real life. These include table-top testing of various scenarios (discussing the business recovery arrangements using example interruptions), simulations (particularly for training people in their post-incident/crisis management roles), technical recovery testing (so information systems can be restored effectively), testing recovery at an alternate site (running business processes in parallel with recovery operations away from the main site), tests of supplier facilities and services (so that externally provided services and products will meet the contracted commitment) and complete rehearsals (testing that our personnel, equipment, facilities, and processes can cope with interruptions).

Portable device: Portable media storage is not permitted in the production environment. Logical access to systems within the production environment is only allowed through role based and attributes-based tools and established bastion hosts under Operations control. Physical access to the servers and devices within the production environment where customer solution data is received processed and stored is under audited controls and all logical access to the environment by high privilege users is key shell logged for forensics and monitoring.

SAP maintains a strict BYOD (Bring Your Own Device) policy where all devices must be activated and brought under the control of the corporate security and MDM (Master Data

Management) system before being allowed to be connected to the corporate network or a corporate device.

All corporate laptops are whole disk encrypted. All approved portable devices are encrypted and have a phone home capability which allows them to be wiped remotely.

Portable media storage is not permitted in the production environment. Logical access to systems within the production environment is only allowed through role based and attributes based tools and established bastion hosts under Operations control. Physical access to the servers and devices within the production environment where customer solution data is received, processed, and stored is under audited controls and all logical access to the environment by high privilege users is key shell logged for forensics and monitoring.

SAP Ariba Network environments and virtual instances are designed and configured to restrict and monitor traffic between trusted and untrusted connections, these configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, and ports, and compensating controls. SAP Ariba Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks. SAP Ariba

The SAP Ariba environment is classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical Environment is located at all sites and/or geographical locations and their usage over are maintained and updated regularly. SAP Ariba supports physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) to safeguard sensitive data and information systems. SAP Ariba supports protection, retention, and Lifecycle management of audit logs, adhering to applicable legal, statutory, or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach. File integrity (host) and network intrusion detection (IDS) tools are implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents. SAP Ariba synchronizes time-service protocol (e.g., NTP) to ensure all systems have a common time reference

SAP Ariba is hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.

The SAP Ariba production and non-production environments are separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties. Secured and encrypted communication channels is used between servers, applications, or data to virtual servers. Access to administrative consoles are restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles). Network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures implemented such as defense-in-depth techniques (e.g., deep packet analysis,

traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.

2. Saviynt

Saviynt offers a complete Cloud-based Identity as a Service (IDaaS) platform to deliver the next generation IGA solution with no requirement for any on-premises footprint. Saviynt has developed partnerships with both Amazon Web Services (AWS) and Microsoft (Azure) to host the Saviynt platform.

The Saviynt Connect server software is deployed on site and communicates with Saviynt Cloud leveraging outbound https communication channels. Saviynt Connect fetches data and provides an outbound connection ONLY to the Saviynt Cloud.

Saviynt offers a modular and integrated platform for Identity Governance. The key modules are Access Request, Access Certification, Role Engineering & Management, SOD Management, Policy & Rule Management, Provisioning, and Analytics. There are several other platform-level components that are shared by these modules. Saviynt provides flexibility to deploy these modules individually or together, depending on the nature of business and system requirements/constraints. There is no client-server architecture involved in the solution.

Saviynt deploys the service into the cloud using Amazon Web Services or Azure Cloud Services as a hosting provider and has the ability to select country and region where the solution is deployed. The solution can be hosted in US data centers on AWS or Azure based on Customer's choice of a cloud service provider at no additional cost. Resilience across multiple AWS/Azure data centers is an available option.

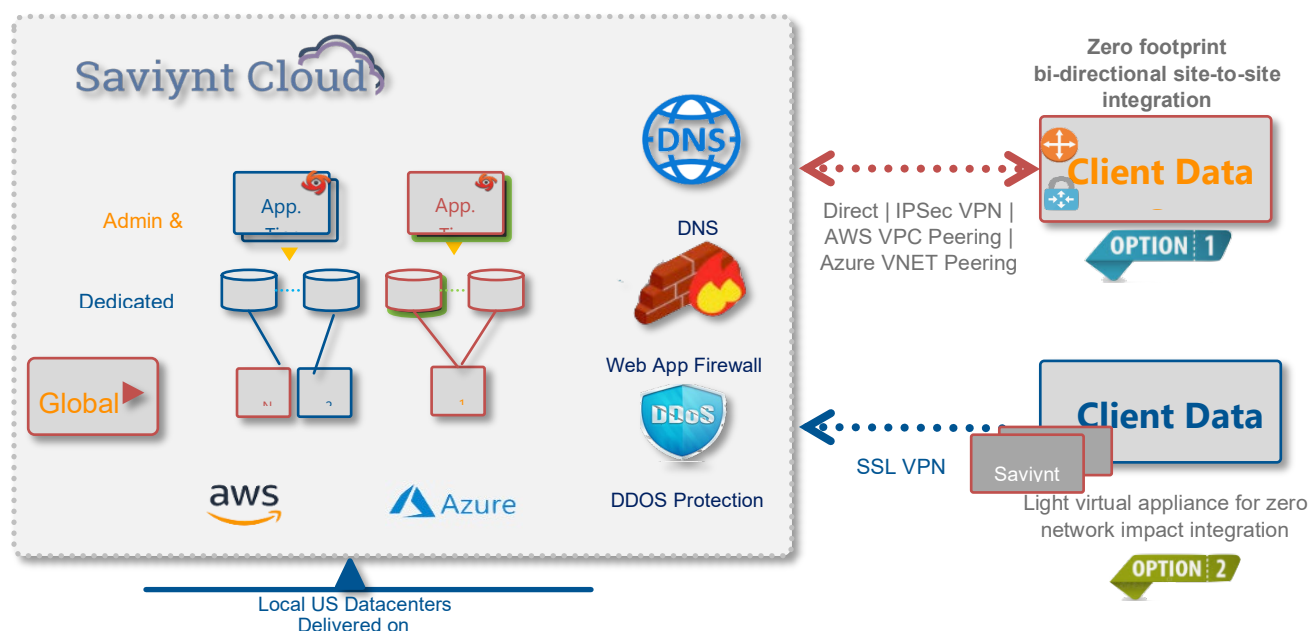


Figure 50. Saviynt Cloud Deployment Model

Backup Processes: The Saviynt solution leverages Azure Backup and AWS capabilities to back up the Saviynt identity warehouse. With the AWS / Azure backup service, we get key enterprise features like backup, restore, policy-based management, backup alerts, job monitoring, instant data recovery without deploying any infrastructure in our tenant environment. We get the ability to back up Managed Disk VMs directly from VM management

blade and the user experience is consistent with a backup of VMs attached to standard or premium unmanaged disks.

3. ServiceNow

ServiceNow's architecture is built on a ServiceNow fully owned and operated private cloud. This private cloud hosts the ServiceNow platform and applications that are offered to its customers under a subscription service model. The private cloud operates out of colocation data centers that provide robust physical and environmental controls. Access to customer data and to the production network is only granted to ServiceNow staff based on their roles and job requirements. To ensure access entitlements are appropriate, reviews are conducted on a regular basis. ServiceNow does not outsource any function that would give a third party access to customer data.

ServiceNow's private cloud is a highly standardized environment from identically configured cages in the data centers to the consistent logical infrastructure. This exclusive, highly defined and limited environment allows for a number of key benefits:

- Automation: Most activities in the ServiceNow infrastructure are conducted using automation tools that require zero-touch such as provisioning new instances. This creates consistent configurations, reducing the potential for impact from human error as well as increasing the efficacy of configuration management within the private cloud.
- Support and Scalability: ServiceNow is highly focused on supporting one service. The ServiceNow environment consists of one homogeneous environment, one interface path. This environment supports thousands of instances, which allows for economies of scale, not attainable in diverse, multi-function environments needed when supporting many applications.
- Control: ServiceNow fully manages the underlying software and hardware platform as well as the ServiceNow software development, allowing ServiceNow complete control over all components in the environment. The control of all aspects of development and deployment of ServiceNow reduces supply chain risks and allows effective setting and management of operational level agreements (OLAs).

Boundary Protection: To manage the ServiceNow private cloud, ServiceNow operations personnel use two-factor authentication and a client-based VPN to access the network.

The private cloud perimeter is protected by firewalls with heavily restricted ingress filtering policies. The logical architecture within the ServiceNow data centers consists of a three tier architecture with network isolation provided by ServiceNow's core infrastructure. The layers that make up the infrastructure consist of:

- Proxy Layer: The proxy layer consists of ServiceNow's network and security equipment typical of a DMZ environment that provides a front end to the application layer and obfuscates ServiceNow's internal network. The proxy layer of the application accepts incoming requests and based on the DNS name being requested does a Port Address Translation before passing the requests through to the next layer.
- Application Layer: Each instance consists of multiple application nodes to provide redundancy with each application node having an isolated virtual environment on a shared physical server. The application layer is a java application that is sand boxed with each instance only listening on a single port and running in its own JVM. This provides code isolation and prevents instances from hearing traffic destined to another instance. This also allows updates to be applied to each instance without affecting other instances.
- Database Layer: Each instance has its own dedicated database, running in this defined network zone. Data coming into the environment must pass through all layers of

infrastructure with all activities/events logged to a central Security and Information Event Management (SIEM) system.

ServiceNow architecture is built on a ServiceNow fully owned and operated private cloud. This private cloud hosts the ServiceNow platform and applications that are offered to its customers under a subscription service model. The private cloud operates out of colocation data centers that provide robust physical and environmental controls.

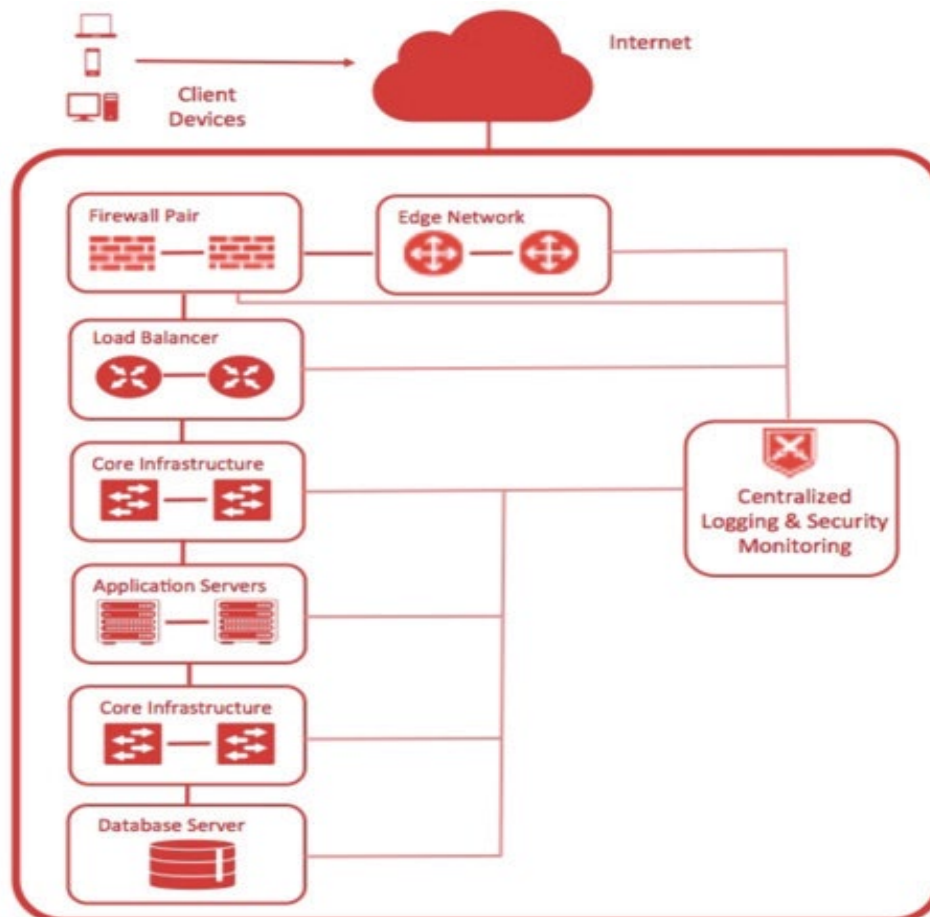


Figure 51. Service Now Deployment Topology

4. Oracle

Boundary Protection: Oracle Cloud Infrastructure has implemented border routers at the border of each region to protect the system. Border routers filter unwanted network traffic and only allow traffic by exception. The border routers also monitor traffic for evidence of a DDoS attack; in the event of a suspected DDoS event against Oracle Cloud Infrastructure and rules are configured to auto-mitigate for high threshold events. If necessary, tickets are created to implement further remediation efforts. Additionally, access control lists (ACLs) logically separate customer and Oracle infrastructure and prevent unauthorized access to systems supporting the services. Border routers do not protect customer systems or infrastructure. Oracle Cloud Infrastructure performs a review of network access control lists including ports semi-annually.

The Oracle Cloud Network architecture consists of a multi-tiered demilitarized zone (DMZ) environment inside a dedicated extranet. It is isolated from Oracle's internal corporate network and inaccessible via VPNs (Virtual Private Network) for non-cloud services. The Oracle Cloud

Network comprises a gateway subnet, tools subnet, and network subnet located in Oracle's DMZ, and it is protected by firewalls.

The first step in the authentication path is the Oracle Cloud Network Access (OCNA) VPN. OCNA functions as a secure access gateway between the user and the target device. OCNA has redundant gateways in various geographies worldwide.

- Authentication: Only approved users with a valid OCNA account can access OCNA, and they must use two-factor authentication.
- Authorization: User attributes describe the specific entitlements the user has to access resources. These attributes are defined at the time of user account creation or modified later (e.g., added by an appropriate entitlement approver, removed upon termination). The user's access is restricted according to these attributes.
- Posture Check: OCNA performs a security posture check to determine whether the user's endpoint is running up-to-date anti-malware software, has a local firewall enabled, and is in line with Oracle policies regarding software updates before permitting the endpoint to authenticate to the VPN.

Bastion Server Authentication

The second step in the authentication path is authenticating to the relevant bastion server. Operator access is permitted from bastion servers only, and the bastion servers are permitted to accept connections from OCNA subnets. Access to bastion servers is controlled in two ways, and users must meet both prerequisites to authenticate to a bastion server.

- Entitlement: Only approved engineers with the required entitlement can access the bastion servers. Entitlements are provisioned using the permissions access management system, are approved by the entitlement owner prior to access being granted, and access is reviewed on a quarterly basis.
- SSH Key: Authorized users provide their public/private SSH key in conjunction with their Linux usernames and authenticate via Lightweight Directory Access Protocol (LDAP). The user's private key is stored on a virtual slot on the user's token, which requires two-factor authentication to access. The user's corresponding public key is configured on the appropriate bastion servers during the access provisioning process.

Access to Individual Devices

Once a user has authenticated to the relevant bastion server, they can connect to an individual device if they have the corresponding permissions entitlement for the device. The permissions access management system manages access to all entitlements and groups, including the code integration tool. Access to entitlements and groups must be approved prior to access being granted, and access is reviewed on a quarterly basis. Inappropriate access identified during the review is investigated and revoked. In addition to having the group entitlement for Network devices, operators must also enter a one-time password (OTP) that expires after 24 hours. Access to hosts is provisioned using a SSH public/private key pairing.

In addition, users with access to the infrastructure supporting the System, source code repositories and the code deployment tool are reviewed quarterly. Issues identified during the review are investigated and remediated.

Media Protection: Oracle Cloud Infrastructure tracks and authorizes equipment, information, or software entering existing Oracle Cloud Infrastructure facilities or data halls. Media is prohibited to be taken off-site from a data hall until the destruction process is complete, and then, with prior authorization. The Oracle Media Sanitization and Disposal Policy outlines the procedures relating to the sanitization of data and the destruction of storage media in Oracle

Cloud Infrastructure data halls. All excess, obsolete and non-performing equipment must be disposed of through an approved Oracle asset disposal process.

5. Acquia

Boundary Protection: The Acquia cloud monitors and controls communications at the external boundary of the system and at key internal boundaries within the system. The cloud vendor monitors and controls communications at key internal boundaries using Iptables and Security Event logging and monitoring. The Acquia SIEM is utilized to log and monitor information security events as noted within the AU control family. In addition, the host based IDS system OSSEC is installed on each host within Acquia cloud Environment and configured to send alerting to Security personnel. In addition, elastic load balances are configured by Acquia to have port restrictions, that restrict communications.

The Acquia Cloud environment monitors and controls communications at key external boundaries via monitoring of AWS perimeter firewall security groups. AWS cloud trail logs are sent to the Acquia SIEM for monitoring and alerting. ACE implements subnetworks for publicly accessible system components that are logically separated from internal organizational networks. Acquia hosts all ACE systems within the AWS Platform as a Service which is completely logically and physically separate from the internal Acquia networks. Cryptographic keys not required or included in the boundary based on security categorization of the information processed by ACE. Acquia does not establish or manage a public key infrastructure.

Security Patch Management: Relevant Acquia personnel (for example, security and engineering teams) subscribe to relevant security notification feeds, including Ubuntu security notices, US-Cert and Drupal Security notices. When a patch or update applicable to Cloud Platform has been published, the patch and vulnerability is reviewed to determine its relevance to the Cloud Platform environment as detailed at Security. If relevant, a tracking ticket is created for Security Engineering teams to assess and score the vulnerability based on applicability, likelihood, impact and mitigating factors using industry-standard scoring frameworks (such as CVSS). A fix for the vulnerability is then incorporated into a later release based on the rating and in alignment with Acquia's standard patching cadence. If the patch or update requires a service restart affecting subscribers, a notification is sent to Cloud Platform subscribers to inform them of the impending maintenance.

Acquia uses a standardized Linux distribution and management tooling to deploy security patches across Cloud Platform.

Data Backup and Disaster Recovery: Acquia utilizes an automated backup tool to help ensure that customer website code, static asset/files and databases are backed up. The tool takes a "snapshot" (backup) hourly that is retained for a pre-defined period according to Acquia's products and services guide. The enterprise monitoring tool is configured to send onscreen alert notifications to operations personnel in the event of a snapshot failure for investigation and resolution (if required). Operations personnel perform a data restoration test on at least a quarterly basis to validate the recoverability of customer production data. The requested data restoration and corresponding results are documented within Acquia's internal ticketing system.

Segregation: The Cloud Platform Enterprise provides independent, logically separate environments for each subscriber application. Certain parts (infrastructure and databases) of the subscriber's primary technology stack in Cloud Platform Enterprise are provisioned on unique, logically distinct infrastructure, except for load balancers. Dedicated load balancers are available to Cloud Platform Enterprise subscribers at an added cost. In Cloud Platform,

Acquia manages host-based firewall policies, which provide logical isolation between distinct subscriber environments in the Cloud Platform. Other parts of the technology stack, such as CDEs, remote administration environments and code repository environments are shared.

Antivirus: Acquia installs ClamAV on all Cloud Platform web servers. ClamAV is an open source General Public License(GPL) antivirus engine designed for detecting Trojans, viruses, malware, and other malicious threats.

SSL and HTTPS: Applications hosted by Acquia Cloud Platform are isolated using several security controls, but internal traffic travels over the same network inside Acquia's shared virtual private cloud (VPC).

1.2.4.6 Secure Application and Network Access

Infosys has deployed the SIEM (Security Information and Event Management) platform which is an event and log monitoring & management platform at an enterprise level. With the recommended logging enabled, the SIEM (Security Information and Event Management) platform collects logs from various enterprises devices (servers, network devices, firewalls etc.). The log monitoring is done based on the use-cases which are configured on the platform using certain criteria and logic. The tool has the capability to correlate among logs from different types of devices and trigger alerts on any suspicious activities detected in the logs.

Logs are stored and retained for shared enterprise devices under scope of SIEM for one year which is completely online. Logs are retained in an encrypted manner and cannot be tampered with. They can only be accessed via application and modification of the logs is not possible. A dedicated team of analysts manages the Security Operation Centre (SOC), which monitors real time alerts triggered from the SIEM system on a 24X7 basis based on the rule sets defined. Also, they do the daily, weekly, and monthly review of logs collected from enterprise network for Infosys end point devices. However, for the State's dedicated laptops, desktops - logging and monitoring will not be part of Infosys scope.

For the State of Maine's proposed solution, associated components provide secure data implementation both at REST and in motion using industry standards transmission protocols such secure sockets layer (SSL) protocol and public key authentication, signing and encryption. Below mentioned table provides details of System components and associated transmission components

Table 31. System and Associated Transmission Components

Logical Components	Access Channel
Portal	HTTPS
eProcurement(SAP Ariba)	HTTPS
Middleware(Oracle Integration Cloud (PAAS)	HTTPS , Secure REST API
Helpdesk(Service Now)	HTTPS
Identity and Access Management	HTTPS

6. Secure Application Access

Core component (SAP Ariba) our Solution leverages both data at rest as well as data in transit are encrypted. We encrypt sensitive data elements stored in the databases using a minimum 256-bit AES (Advanced Encryption Standard) encryption. AES is the federal standard for data encryption. Encryption technology is also applied for the client connection to the Web site (Transport Layer Security (TLS) min v1.2 and preferred v1.2) and to the hosted application passwords in storage. Customer user passwords are one way hashed using SHA256 and

salted with random data. Limited SAP Ariba Operations personnel have data query access and monitoring rights for the SAP Ariba hosting program.

SAP utilizes encryption to protect the confidentiality and integrity of information. SAP and its business must identify requirements for the use of encryption and the protection of encryption keys. Encryption must be used in compliance with applicable contractual agreements, legislation, and regulations. SAP Cloud systems are configured to use secure communication in accordance with the protection requirement of the transmitted information. Suitable measures for securing the exchange of information are used. For strong encryption methods and keys, SAP uses at least a 128-bit symmetric key or a 2,048-bit asymmetric key, as well as strong and internationally recognized cryptographic algorithms.

SAP Cloud storage systems processing sensitive data employ data at rest encryption. Operated storage devices in SAP managed data centers offer data-at-rest encryption or self-encrypting drives, which encrypt data “on the fly” while stored on disks. An encryption key is stored on the service processor or an external key management server. SAP laptops and workstations must have a corporate image and an encrypted hard drive installed.

Portable device: Portable media storage is not permitted in the production environment. Logical access to systems within the production environment is only allowed through role based and attributes-based tools and established bastion hosts under Operations control. Physical access to the servers and devices within the production environment where customer solution data is received processed and stored is under audited controls and all logical access to the environment by high privilege users is key shell logged for forensics and monitoring.

SAP maintains a strict BYOD policy where all devices must be activated and brought under the control of the corporate security and MDM system before being allowed to be connected to the corporate network or a corporate device.

All corporate laptops are whole disk encrypted. All approved portable devices are encrypted and have a phone home capability which allows them to be wiped remotely.

Portable media storage is not permitted in the production environment. Logical access to systems within the production environment is only allowed through role based and attributes based tools and established bastion hosts under Operations control. Physical access to the servers and devices within the production environment where customer solution data is received, processed and stored is under audited controls and all logical access to the environment by high privilege users is key shell logged for forensics and monitoring.

Custom Changes: Security and privacy are an integral part of our development process to achieve security and privacy by design. Ariba leverages a Secure Software Development cycle (Secure SDC) that is aligned with ISO 27034 principles. This includes:

- Secure code (OWASP Top Ten) training to engineers
- Code review by peers before build cycles
- Static and dynamic code analysis, with load testing for resiliency
- Reviews and approvals at multiple phases for meeting security criteria prior to release to production.

Access Control: SAP is committed to the security and integrity of customer information. They utilize security measures to protect against the loss, misuse, or alteration of the information under our control. To prevent unauthorized access, maintain data accuracy, and facilitate the correct use of information, they have put in place appropriate physical, electronic, and managerial procedures to safeguard and secure the information they collect within the solution.

From time to time, security-related white papers are also available to customers and prospects offering further detail regarding our approach to secure architecture. Customers are able to review the SAP Ariba SOC II report issued by their independent third party auditor, which offers detail as to the security controls in place for the SAP Ariba cloud applications. Visitors are screened upon entry to verify identity and escorted to appropriate locations.

Physical Access Control: Only certified representatives of SAP Ariba have access to SAP Ariba computers within the data centers. These data centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, biometrics access control, and other measures to prevent equipment and data center facilities from being compromised. Access history is recorded for audit purposes.

The Equinix Data Center utilizes an array of security equipment, techniques, and procedures to control, monitor, and record access to the facility, including customer cage areas. All areas of the center are monitored and recorded using CCTV, and all access points are controlled. The Data Center is staffed with 24-hour security officers.

Security audit logging

Security Incident and Event Logging: SAP Ariba solutions implements a dedicated appliance to provide security analytics and to meet compliance requirements with SIEM in production environments. A SIEM is classified as a “security information and event management” utility. This is a collection of hardware and software processes that ingest information from logs, net flow, and additional security services as needed. The sensors are deployed throughout the network to collect logs and monitor network traffic. This provides the five essential security capabilities – behavioral monitoring, SIEM, intrusion detection, asset discovery, and vulnerability assessment – for complete visibility.

The SIEM server aggregates and correlates information that the sensors gather and provides single-pane-of-glass management, reporting, and administration.

SAP Ariba supports data security to include confidentiality, integrity, and availability(CIA) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alternation, or destruction. Data and objects containing data are assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization. Policies and procedures are established to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's applications and infrastructure network and systems. Data that traverses public networks are classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data. SAP Ariba supports encryption methodologies (AES 256, etc.) to tenants in order to protect data if it is required to move through public networks. SAP Ariba Policies and procedures are established for labeling, handling, and the security of data and objects which contain data. Mechanisms for label inheritance are implemented for objects that act as aggregate containers for data. Production data are not replicated or used in non-production environments. SAP Ariba supports secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant.

SAP Ariba supports management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the

service, and/or the customer (tenant) has some shared responsibility over implementation of the control. SAP Ariba supports the use of encryption protocols for the protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.

SAP Ariba Keys are stored in the cloud (i.e., at the cloud provider in question) but maintained by the cloud consumer or trusted key management provider.

The SAP Ariba applications utilize secure session cookies to maintain users sessions after they're logged in. Once a browser initiates a secure connection to a server via HTTPS, a secure session cookie is used; this makes sure that the cookie is encrypted when transmitting from the web browser to the web server. A session cookie (or temporary cookie) exists only for the duration of the visit to the website. Session cookies are used to maintain session context, making sure that page changes and/or data selections are retained as the user navigates from page to page. When a user initiates a session in any SAP Ariba cloud solution, the SAP Ariba solution sends a session ID in the form of a session cookie. The session ID is transmitted back and forth between the browser and the server. HTTPS cookies are based on industry standards and provide a more secure method of session management rather than URL-based and form-based session management which are prone to session hacking.

SAP Ariba does not use cookies for marketing purposes; SAP Ariba utilizes cookies only to maintain session for its applications. Almost each cookie is session-based with the lone exception being the persistent cookie used for supporting Desktop File Sync (DFS). DFS stores an encryption key that is used to synchronize workspace file changes from a user's desktop to the SAP Ariba Contract Management Solution.

Security incidents should be logged in SIEM (Security Information and Event Management) platform which is an event and log monitoring & management platform at enterprise level. As per the recommended logging enabled, the SIEM (Security Information and Event Management) platform collects logs from various enterprises devices (servers, network devices, firewalls etc.). The log monitoring is done based on the use-cases which are configured on the platform on certain criteria and logic. SIEM Tool should correlate among logs from different types of devices and trigger alerts on any suspicious activities detected in the logs. Logs should be stored and retained for shared enterprise devices under scope of SIEM for one year which is completely online. Logs are retained in an encrypted manner and cannot be tampered with. They can only be accessed via application and modification of the logs is not possible.

Security Procedures for Employees handling Sensitive Data

Infosys proposed solution leverages SAP Datacenters which will have government grade security inbuilt. Along with Data Center Security Infosys follows a comprehensive Security framework for screening and hiring candidates. The following table describes high level procedures leveraged in our proposed solution to ensure a robust security posture.

Table 32. High Level Security Procedures

Security Procedures	Infosys Public Services (Infosys) Security Practices
Security Awareness and training	All Employees hired by Infosys are required to complete mandatory Security Awareness Training before they will be deployed to a project. Infosys conducts a security awareness session at the time of induction programs as a periodic refresher. The flash video used for this training covers the overview of Infosys Security Policies and the dos and don'ts from a security perspective. The objective

Security Procedures	Infosys Public Services (Infosys) Security Practices
	of the training is to make every employee familiar and competent in the knowledge and with the information security policy of Infosys. This training is provided on security objectives, and on their roles and responsibilities for security.
Background Check	Our hiring procedures include a comprehensive screening of the candidates for key positions and consideration of whether the verified credentials are commensurate with the proposed position. New personnel are selected according to the criteria specified in dedicated job descriptions and offered employment subject to background checks and reference validation, according to the legislation applicable in the employee's country of residence. The background checks are performed by an external party.
Privileged access	All employees who have access to sensitive Data will be multi-factor authenticated and transactions are audited to ensure complete accountability. As part of implementing access to Sensitive data, Infosys will follow the steps below: 1. Analyze applications for identifying access/entitlements that need to be marked as sensitive. 2. Build the risk matrix 3. Define risk scores for the entitlements 4. Configure IDM for the risk model and import metadata for privileged entitlements into IDM 5. Implement controls like additional approvals or standalone access reviews for privileged entitlements
Configuration management	Configuration Management security controls are involved in all artifacts generated during the lifecycle. • All servers are hardened using secure configuration standards. We have a defined process to monitor all threats including security vulnerabilities. The Information Security Group monitors vulnerability advisory sources for information on new vulnerabilities and patches. When security updates are released by the vendor, we test them and issue an internal vulnerability advisory to the relevant departments. The Computers and Communication Division (CCD) is responsible for deploying the patches to end user systems through Microsoft SMS / SCCM. • All project data is stored on access-controlled file servers which is restricted to authorized personnel working on the project strictly on a need to know and least privilege basis. The list of individuals having access is subjected to regular reviews by the Project Configuration Controller.
Maintenance	• All IT infrastructure assets are recorded in an asset management system called AMANAT. Inventory is maintained for all physical assets and is reconciled periodically with internal systems. Infosys has deployed stringent controls for all asset movement into or out of premises. Any material being brought into premises by anyone is subject to inspection by the security guard at entrance. Premises are classified as a customs bonded area and therefore, material is moved into or out of the facilities strictly per Government-prescribed procedures. All equipment/materials in the bonded area is subject to audits.
Personnel	The Human Resource Department at Infosys is responsible for handling Personnel

Security Procedures	Infosys Public Services (Infosys) Security Practices
security	security. • All visitors are assigned photo IDs and are always accompanied by authorized personnel to gain entry to the premises. • Access control is implemented using proximity cards (for data centers server rooms). Only authorized personnel are allowed to enter data center. • All project data is stored on access-controlled file servers which is restricted to authorized personnel working on the project strictly on a need to know and least privilege basis. The list of individuals having access is subjected to regular reviews by the Project Configuration Controller.
System and information integrity	Our proposed solution leverages Infosys' IT security framework and is designed to ensure the selection of adequate and proportionate security controls to protect the whole gamut of information assets. • Communications Security ○ To ensure the protection of information in our networks and our supporting information processing facilities we make use of latest technology combined with the right set of security controls. Listed below are some of the network security controls for providing security to the information transferred within the organization and with external entities. • Network Security ○ All external connections (e.g., customer connection, internet connectivity) are secured using a state-of-the-art inspection firewall. ○ Access to a customer network is restricted and provided only to required resources using approved access methods of customer. ○ DMZs are protected by Network Intrusion Prevention systems (IPS). ○ We have implemented an 802.1x network access control (NAC) mechanism wherein only authenticated endpoints (workstations, laptop) having a valid certificate can connect to the corporate network, thereby preventing unauthorized devices from connecting. ○ Access to the internet is restricted and an internet access policy is enforced using internet content filtering technology. ○ The perimeter is protected by NIPS (Network Intrusion Prevention System) which is updated by latest signatures. ○ Vulnerability assessments are performed in-house using Industry standard tools and techniques to identify vulnerabilities. These vulnerability tests are performed on a periodic basis and the identified vulnerabilities are tracked to closure. Continuous monitoring of critical servers for vulnerabilities ensures a secure Infrastructure.

7. ServiceNow

Unauthorized Access: Customer traffic to the Now Platform comes via the internet utilizing Hypertext Transfer Protocol Secure (HTTPS) TLS encryption. Network connections are managed using a high availability module that provides perimeter filtering. Customer traffic passes through an application delivery controller. Customer traffic interacts with the application nodes which host the application logic, and calls to the database are made. ServiceNow

internal operational connections are made through a secure VPN tunnel which provides access to maintain the applications and infrastructure.

A firewall system is installed and utilized to protect the ServiceNow APaaS. The firewall analyzes data and packets routed to the ServiceNow environment. Any external Internet traffic is required to pass through the firewall to communicate with the production servers. Any type of connection that is not explicitly authorized by the firewall will be denied. Cloud and TIGIR personnel utilize Splunk to monitor and log activity within the firewall system that includes, but is not limited to the following:

- Failed connections
- Permitted connections to specific destinations
- Denied connections to specific destinations TIGIR personnel review firewall logs on a business daily basis, and evidence their review by completing a business daily log review checklist.

Any anomalies are investigated and resolved per the documented Security Incident Management process. Firewall administrators are required to authenticate via a VPN client to the production network and then connect utilizing secure shell (SSH) encryption to gain access to the firewall systems. The firewall system requires administrators to authenticate via a valid user account, PIN, and token to access the firewall rule-set. Administrative access to the firewall system is restricted to authorized cloud operations personnel. Additionally, changes to the firewall cannot be executed without prior authorization by the SRE team.

8. AzureAD

Access to Customer Virtual Machines: External traffic to customer VMs is protected via ACLs but can be configured by the customer to allow external traffic only to customer designated ports and protocols. There is no port that is open by default unless explicitly configured by the customer in the service definition file. Once configured, the Azure Fabric Controller automatically updates the network traffic rule sets to allow external traffic only to the customer designated ports.

Customers can connect to their VMs via the ports and protocols defined by them, create credentials (i.e., username and password) and choose a certificate to encrypt the credentials during initial set-up that expires within 14 days through a secured mechanism. Authentication after set-up is performed using the self-created credentials. The connection is secured via TLS using a self-signed certificate generated by the VM instance. Customers can also upload custom certificates via the Azure Portal and configure their instances to use them securely.

9. OCI

Oracle Cloud Infrastructure maintains a catalog of its assets, and each catalog entry consists of a unique part number and description. Each record contains comprehensive details of the asset including name, type, location (e.g., data hall, rack, and rack unit [U] number). Maintaining this catalog is a continuous process in which newly introduced, moved, and removed hardware is recorded in the catalog.

Oracle Cloud Infrastructure Asset Management Requirements outline the procedures for handling assets and the security requirements to undertake when transferring assets.

Oracle Cloud Infrastructure manages virtual assets using a software package that collects, aggregates and reports information on assets. Tracked assets include, for example, bastions, hypervisors, virtual machines, ILOMs, SmartNIC, network devices, and flamingo devices. Oracle Cloud Identifiers (OCID) is the primary mechanism for uniquely identifying virtual

assets. Each virtual asset tracked includes information such as region information, tenancy OCID, compartment OCID, instance OCID, hostname, and IP address.

Monitoring: Monitoring allows customers to actively and passively monitor their cloud resource using the Metrics and Alarms features. Monitoring uses metrics to monitor resources and alarms to notify customers when those metrics meet alarm-specified triggers. Metrics are relayed to the monitoring service by resources as raw data points, or timestamp-value pairs, along with dimensions and metadata. Alarms publishes alarm messages to configured destinations managed by the notifications service.

System Logs: Authentication logs for servers supporting services, Control Plane Server (CPS) proxy hosts, Smart Network cards and Integrated Lights Out Managers (ILOMs), network devices, and bastion hosts are forwarded to a Security Information and Event Monitoring (SIEM) tool where logs are retained for at least 90 days. Access to the log repository is restricted to approved personnel.

In addition to authentication logs, Oracle deploys a host intrusion detection system (HIDS), a network intrusion detection system (NIDS), anti-virus (AV), and file integrity monitoring (FIM) on servers supporting the system. Logs from this suite of security controls are sent to the log aggregation tool.

The Security Information and Event Monitoring (SIEM) tool creates a ticket if suspicious activity is detected. The ticket is updated throughout the investigation and escalated for additional investigation as required.

Logging provides access to logs from Oracle Cloud Infrastructure resources. These logs include critical diagnostic information that describes how resources are performing and being accessed.

API: Oracle Cloud Infrastructure APIs are typical REST-based and use HTTPS requests and responses. Oracle Cloud Infrastructure API requests require support for HTTPS and TLS V1.1 or V1.2.

Anti-Virus and File Integrity Monitoring: The Oracle Cloud Infrastructure programmatically deploys and manages AV and FIM solutions on hosts supporting services running within the production environment. Log events from AV and FIM feed into the SIEM solution.

Intrusion Detection: The Oracle Cloud Infrastructure has deployed a Network Intrusion Detection System (NIDS) that provides real-time data into the SIEM solution. In addition, Oracle Cloud Infrastructure programmatically configures hosts to provide access monitoring and accounting logs to the SIEM solution. Together with data from FIM, these additional logs provide information for host-based intrusion detection.

10. Acquia

Logging: The Acquia Cloud Platform ensures the appropriate level of logging is implemented at the application and platform layers for Acquia-managed assets to enable necessary analysis and investigation into an incident or issue. Acquia uses a SIEM system to retain the logs for up to 365 days. As noted in the shared responsibility model of cloud platform section, subscribers are responsible for implementing security for their Drupal applications, which includes appropriate logging and monitoring practices and protocols. Acquia offers capabilities such as log forwarding to assist subscribers

System access controls: Acquia limits privileged access both to the information on the subscriber infrastructure under its management and to the infrastructure themselves. Access

is limited to authorized personnel. Network layer controls ensure privileged access is always enforced through secure bastion hosts, using encrypted tunnels through nonstandard ports. Authentication requires multi-factor authentication and each user's credentials are encrypted in transit and at rest. Access attempts are logged and monitored using a security information and event management (SIEM) system.

Subscribers can provision non-privileged user accounts to the subscriber's web nodes using the Acquia web-based user interface and APIs. With the Acquia platform, subscribers can create named users and upload those users' SSH public keys, which are deployed to the subscriber's infrastructure, enabling non-privileged access using SSH. The Acquia platform provides application administrators with the ability to add non-privileged users' accounts and SSH keys, which are then deployed to the subscriber's Cloud Platform web nodes.

1.2.4.7 Data Security

Infosys proposed procurement solution leverages individual cloud service providers Data security process to act as a base for an overall data security Program. The below sections describe the details of individual components different data security objectives.

Infosys as an organization emphasizes on Information Security policy which details about encrypting the data at rest and the data in transit to be compliant with the laws in the locations between which encrypted data is transmitted, where it is stored and any other law that is applicable to the vendor of encryption system to ensure confidentiality of data. All customer data received, processed, and stored within the solution is classified as highly confidential and is subject to confidentiality terms based upon our agreements with customers. Access to information will be based on business requirement using the principle of least privilege. Employees and external parties must have access only to the information they require to carry out their work and are responsible for protecting information and assets to prevent unauthorized access, disclosure, modification, removal, destruction, and improper use.

Data at rest such as backups etc. is encrypted using AES 256 algorithm. However, data on file servers are encrypted on demand only. Laptops are installed with FDE (Full disk encryption) to protect customer information in laptops. Data can be encrypted in storage and transmission as per the customer requirement also. Typically, a Virtual Private Network is setup to encrypt data in transit. Data in transit, over public network is always encrypted using strong encryption algorithm such as AES 256/128, with Hashing as SHA2/SHA1. These are used to established Site-to-Site VPN using IPSEC tunnels for securely connecting to client network.

Access granted to Solution information systems from internal and external parties requires the implementation of authorization and authentication access controls that are proportional to the associated risk.

Patch Management

Infosys has a documented patch management process. The Information security group monitors patch advisory sources for information on new vulnerabilities and patches. Whenever new security patches are released by the vendor, ISG notifies the Infosys stakeholders about the applicable patches. The infrastructure owners are recommended to test the patches in a test environment wherein the team checks the effects of the installed patch on the performance of the system and the simulated environment. Post successful testing, the infrastructure management team deploys the patches on all applicable systems.

For large scale patch deployment, we have solutions like SCCM (System Center Configuration Manager), Casper and satellite servers in place. Patch compliance status is monitored regularly, and non-compliances are highlighted to the concerned stakeholders. The SLA (percentage of patch

compliance) for deployment of the patch compliance will be measured on 12 days across all assets from the date of release of patch by the OEM (Original Equipment Manufacturer).

Hardening

Information Security Group (ISG) Standards team publishes hardening guidelines for operating systems, applications & devices. Some sources of industry accepted hardening standards include but are not limited to: Center for Internet Security (CIS), International Organization for Standardization (ISO), Sysadmin, Audit, Network & Security (SANS), National Institute of Standards Technology (NIST) etc.

These guidelines and procedures, comprising of technical controls, would prevent security incidents that occur due to misconfigurations from affecting the Infosys network. These guidelines transform into organization-wide system security standard & secure configuration best practices for all the IT platforms. This leads to reduction in risks and continuous improvement in the Information security practices in the organization. ISG validation team also performs compliance assessments to check whether the system is built as per the hardening guidelines prior to the release into production environment. This is in case of new hosting that is deployed through a change order. For new machines internal to Infosys network, compliant MDT (Microsoft Deployment Toolkit) images are used.

Infosys Approach for protecting data and applications including threats from outside the service center as well as other customers co-located within the same service center

- Limit the number of external network connections to the system which facilitates monitoring of inbound and outbound communications traffic. The Trusted Internet Connection DHS TIC initiative is an example of a federal guideline that requires limits on the number of external network connections. Filter unauthorized control plane traffic from external networks. Protect the confidentiality and integrity of the information being transmitted across each interface. Examples of control plane traffic include Border Gateway Protocol (BGP) routing, Domain Name System (DNS), and management protocols.
- Deny network communications traffic by default and allow network communications traffic by exception. applies to inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those system connections that are essential and approved are allowed. Deny by default, allow by exception also applies to a system that is connected to an external system.
- Prevent split tunneling for remote devices connecting to State of Maine systems unless the split tunnel is securely provisioned. A virtual private network (VPN) can be used to securely provision a split tunnel. A securely provisioned VPN includes locking connectivity to exclusive, managed, and named environments, or to a specific set of pre-approved addresses, without user control.
- Route State of Maine-defined internal communications traffic to State of Maine-defined external networks through authenticated proxy servers at managed interfaces. Web content filtering devices are one of the most common proxy servers that provide access to the Internet. Proxy servers can support the logging of Transmission Control Protocol sessions and the blocking of specific Uniform Resource Locators, Internet Protocol addresses, and domain names. Web proxies can be configured with State of Maine-defined lists of authorized and unauthorized websites.
- Detect and deny outgoing communications traffic posing a threat to external systems and Audit the identity of internal users associated with denied communications. Analyze incoming and outgoing communications traffic while searching for indications of internal threats to the security of external systems. Internal threats to external systems include traffic indicative of denial-of-service attacks, traffic with spoofed source addresses, and traffic that contains malicious code.

- Only allow incoming communications from State of Maine-defined authorized sources to be routed to State of Maine -defined authorized destinations. Source address validation techniques should be applied to restrict the use of illegal and unallocated source addresses as well as source addresses that should only be used within the system.
- Implement State of Maine -defined host-based boundary protection mechanisms at State of Maine-defined system components. Host-based boundary protection mechanisms include host-based firewalls.
- Isolate State of Maine-defined information security tools, mechanisms, and support components from other internal system components by implementing physically separate subnetworks with managed interfaces to other components of the system.
- Enforce adherence to protocol formats. System components that enforce protocol formats include deep packet inspection firewalls and XML gateways. The components verify adherence to protocol formats and specifications at the application layer and identify vulnerabilities that cannot be detected by devices operating at the network or transport layers.
- Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device. Employing mechanisms to ensure that in the event of operational failures of boundary protection devices at managed interfaces, systems do not enter unsecure states where intended security properties no longer hold. Managed interfaces include routers, firewalls, and application gateways that reside on protected subnetworks
- Block inbound and outbound communications traffic between State of Maine-defined communication clients that are independently configured by end users and external service providers.
- Provide the capability to dynamically isolate State of Maine-defined system components from other system components. Component isolation reduces the attack surface of State of Maine systems. Isolating selected system components can also limit the damage from successful attacks when such attacks occur.
- Implement separate network addresses to connect to systems in different security domains. The decomposition of systems into subnetworks (i.e., subnets) helps to provide the appropriate level of protection for network connections to different security domains that contain information with different security categories or classification levels.
- For systems that process personally identifiable information, Apply the processing rules to data elements of personally identifiable information, monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system, Document each processing exception and (d) Review and remove exceptions that are no longer supported.
- Prohibit the direct connection of State of Maine-defined unclassified national security system to an external network without the use of State of Maine-defined boundary protection device
- Prohibit the direct connection of a classified national security system to an external network without the use of State of Maine-defined boundary protection device. Boundary protection devices (e.g., firewalls, gateways, and routers) mediate communications and information flows between classified national security systems and external networks. In addition, approved boundary protection devices (typically managed interface or cross-domain systems) provide information flow enforcement from systems to external networks.
- Implement physically; logically separate subnetworks to isolate the following critical system components and functions. Separating critical system components and functions from other noncritical system components and functions through separate subnetworks may be necessary to reduce susceptibility to a catastrophic or debilitating breach or compromise that results in system failure
- Monitor and scan for vulnerabilities in the system and hosted applications State of Maine-

defined frequency and/or randomly in accordance with State of Maine-defined process and when new vulnerabilities potentially affecting the system are identified and reported.

- Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for Enumerating platforms, software flaws, and improper configurations
- Analyze vulnerability scan reports and results from vulnerability monitoring and Remediate legitimate vulnerabilities
- Share information obtained from the vulnerability monitoring process and control assessments with State of Maine-defined personnel or roles to help eliminate similar vulnerabilities in other systems. The vulnerability monitoring tool update process helps to ensure that potential vulnerabilities in the system are identified and addressed as quickly as possible. Vulnerability monitoring and analyses for custom software may require additional approaches, such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches.
- Implement privileged access authorization to State of Maine -defined system components for State of Maine -defined vulnerability scanning activities. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and protects the sensitive nature of such scanning.
- Review historic audit logs to determine if a vulnerability identified in a State of Maine -defined system has been previously exploited within a State of Maine-defined time. Define the breadth and depth of vulnerability scanning coverage. Correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability and multi-hop attack vectors
- Establish procedures; Implement mechanisms to ensure State of Maine -defined access control decisions are applied to each access request prior to access enforcement. Authorization processes and access control decisions may occur in separate parts of systems or in separate systems. In such instances, authorization information is transmitted securely (e.g., using cryptographic mechanisms) so that timely access control decisions can be enforced at the appropriate locations.
- Enforce access control decisions based on State of Maine-defined security or privacy attributes that do not include the identity of the user or process acting on behalf of the user.
- Control physical access to State of Maine-defined system distribution and transmission lines within State of Maine facilities using State of Maine-defined security controls
- Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies. Enforce dual authorization for State of Maine-defined privileged commands. Dual authorization, also known as two-person control, reduces risk related to insider threats. Dual authorization mechanisms require the approval of two authorized individuals to execute
- Enforce State of Maine -defined mandatory and discretionary access control policy over the set of covered subjects and objects specified in the policy
- Enforce a Role-based access control (RBAC) policy over defined subjects and objects and control access based upon State of Maine-defined roles and users authorized to assume such roles. RBAC can be implemented as a mandatory or discretionary form of access control
- Enforce the revocation of access authorizations resulting from changes to the security attributes of subjects and objects based on State of Maine -defined rules governing the timing of revocations of access authorizations.
- Restrict access to data repositories containing specific information is intended to provide flexibility regarding access control of specific information types within a system. Restrict access to cryptographic keys, authentication information, and selected sensitive system information

- Enforce attribute-based access control policy over defined subjects and objects and control access based upon State of Maine-defined attributes to assume access permissions.

Infosys approach for Security Risk Management

As part of Risk Management, Infosys Security Team will perform below activities for State of Maine eProcurement Solutions

b) Risk Assessment

- Identify threats to and vulnerabilities in the system, determine likelihood, and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information
- Risk assessments will consider risk from external parties, including contractors who operate systems on behalf of the State of Maine, individuals who access State of Maine systems, service providers, and outsourcing entities
- Risk assessments will be conducted at various steps in the Risk Management Framework, including preparation, categorization, control selection, control implementation, control assessment, authorization, and control monitoring. Risk assessment is an ongoing activity carried out throughout the system development life cycle including system design, the intended use of the system, testing result
- Continuously update the risk assessment or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.
- Document and Review risk assessment results

c) Continuous Monitoring | Risk Monitoring

- Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following Effectiveness monitoring, Compliance monitoring and Change monitoring
- Effectiveness monitoring will determine the ongoing effectiveness of the implemented risk response measures. Compliance monitoring verifies that required risk response measures are implemented. It also verifies that security and privacy requirements are satisfied. Change monitoring identifies changes to State of Maine systems and environments of operation that may affect security and privacy risk

d) Risk Management Strategy

- Develop a comprehensive strategy to manage Security risk to State of Maine operations and systems, assets, and individuals
- Privacy risk to individuals resulting from the authorized processing of personally identifiable information
- Implement risk management strategy consistently across the State of Maine and Review and update the risk management strategy or as required, to address State of Maine changes
- Identify and document Assumptions affecting risk assessments, risk responses, and risk monitoring. Constraints affecting risk assessments, risk responses, and risk monitoring. Distribute the results of risk framing activities and Review and update risk framing considerations
- Respond to findings from security and privacy assessments, monitoring, and audits in accordance with State of Maine risk tolerance

Infosys approach Risk Management Process

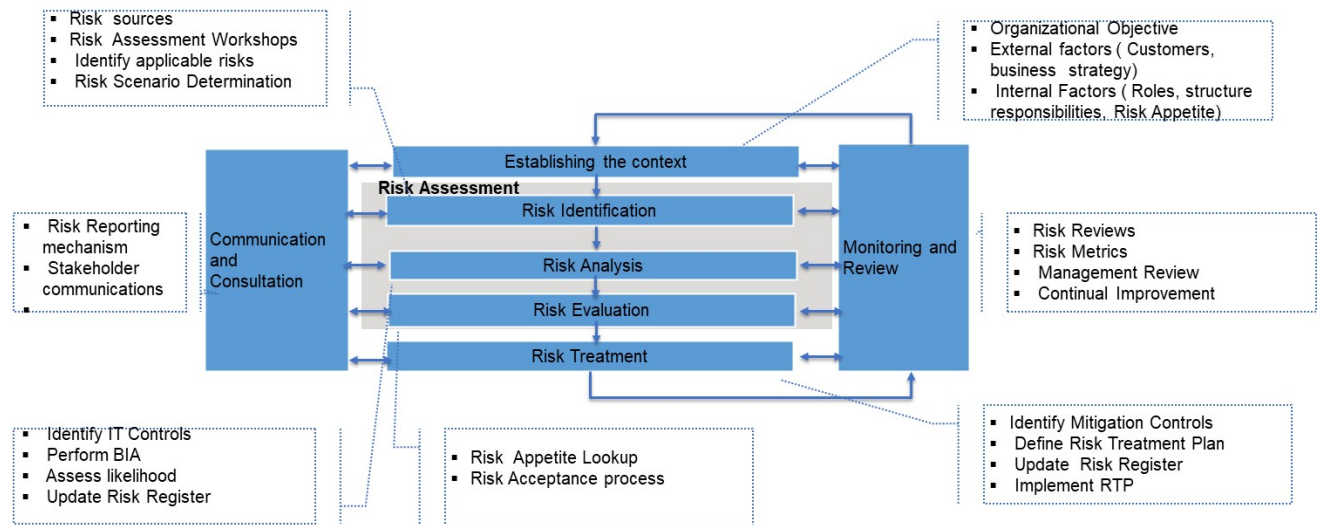


Figure 52. Risk Management Process

Infosys approach to comply with applicable laws and related to data privacy and security standards includes below phases

- a) Privacy Impact Assessments: Conduct privacy impact assessments for systems, programs, or other activities before:
 - Developing or procuring information technology that processes personally identifiable information; and
 - Initiate a new collection of personally identifiable information
- b) System Security and Privacy Plans: Develop security and privacy plans for the system that:
 - Are consistent with the enterprise architecture
 - Explicitly define the constituent system components.
 - Describe the operational context of the system in terms of mission and business processes.
 - Identify the individuals that fulfill system roles and responsibilities.
 - Identify the information types processed, stored, and transmitted by the system
 - Provide the security categorization of the system, including supporting rationale
 - Describe any specific threats to the system that are of concern to the organization
 - Provide the results of a privacy risk assessment for systems processing personally identifiable information
 - Describe the operational environment for the system and any dependencies on or connections to other systems or system components.
 - Provide an overview of the security and privacy requirements for the system
 - Identify any relevant control baselines or overlays, if applicable
 - Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions
 - Include risk determinations for security and privacy architecture and design decisions
 - Include security- and privacy-related activities affecting the system that require planning and coordination with State of Maine-defined individuals or groups and
 - Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.

- Distribute copies of the plans and communicate subsequent changes to the plans to State of Maine-defined personnel or roles
 - Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and
 - Protect the plans from unauthorized disclosure and modification.
- c) Privacy Program Plan: Develop and disseminate an organization-wide privacy program plan that provides an overview of the agency's privacy program, and:
- Includes a description of the structure of the privacy program and the resources dedicated to the privacy program
 - Provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements
 - Includes the role of the senior official for privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities
 - Describes management commitment, compliance, and the strategic goals and objectives of the privacy program.
- d) Security and Privacy Architectures: Develop security and privacy architectures for the system that:
- Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information.
 - Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals
 - Describe how the architectures are integrated into and support the enterprise architecture; and
 - Describe any assumptions about, and dependencies on, external systems and services.
 - Review and update the architectures to reflect changes in the enterprise architecture; and
 - Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.
 - Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards
- e) Privacy Notice: Provide notice to individuals about the processing of personally identifiable information that
- Is available to individuals upon first interacting with State of Maine, and subsequently at State of Maine -defined frequency
 - Identifies the authority that authorizes the processing of personally identifiable information
 - Identifies the purposes for which personally identifiable information is to be processed
 - Present notice of personally identifiable information processing to individuals at a time and location where the individual provides personally identifiable information or in conjunction with a data action
 - Include Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records or provide Privacy Act statements on separate forms that can be retained by individuals.
- f) Privacy Reporting: Develop State of Maine -defined privacy reports and disseminate to
- State of Maine-defined oversight bodies to demonstrate accountability with statutory, regulatory, and policy privacy mandates; and

- State of Maine-defined officials and other personnel with responsibility for monitoring privacy program compliance; and
- Review and update privacy reports as per State of Maine -defined frequency

Infosys Approach for IT Security, Privacy, & Data Protection Service is below

Enterprise Privacy Gap Assessments	Privacy Program Implementation	Privacy Impact Assessments	Data Classification	Privacy Breach & Incident Management Services	Vendor Privacy Risk Assessments and Reporting Services	Privacy by Design and Default(PbDD)
To provide a clear picture on where an organization currently stands with respect to Privacy	Based on a comprehensive privacy assessments, execute the roadmap for the transformation program to prepare the organization for privacy compliance	Develop and implement methods to stay in control of privacy risks for changed and new systems and processes.	Provide Services for Data Classification, Data Inventorization and Data Flow identification	Advisory and Reporting services for handling Data Breach including Breach Reporting and Notification Risk Assessments	Reviewing Organizations Third Party Vendor for - Privacy controls - Processes - Data breach reporting & management capabilities - Agreements for Privacy compliance	Process & Guidelines Advisory Service for Changed and New applications being built
Privacy Training - DP Risk & Compliance Training & Awareness workshops						
Privacy Enhancement Tools- Data Masking,, Anonymization, Pseudonymization etc.						

Figure 53. Infosys Approach for IT Security, Privacy, & Data Protection Service

Privacy and Data Protection Methodology

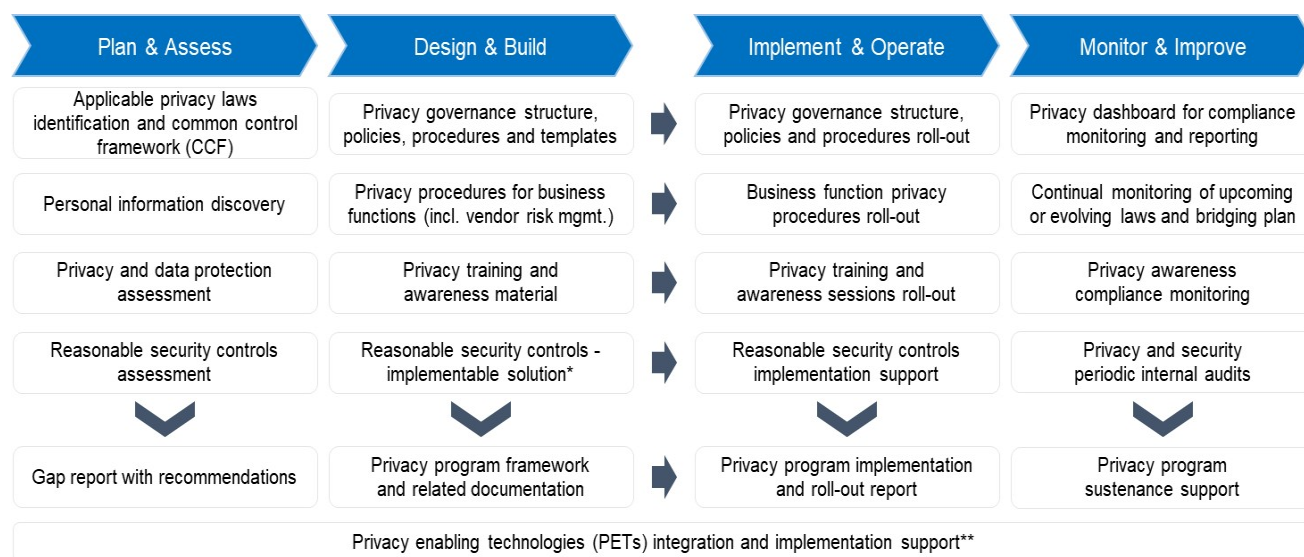


Figure 54. Privacy and Data Protection Methodology

Infosys approach to Data Privacy Gap and Impact Assessment Services

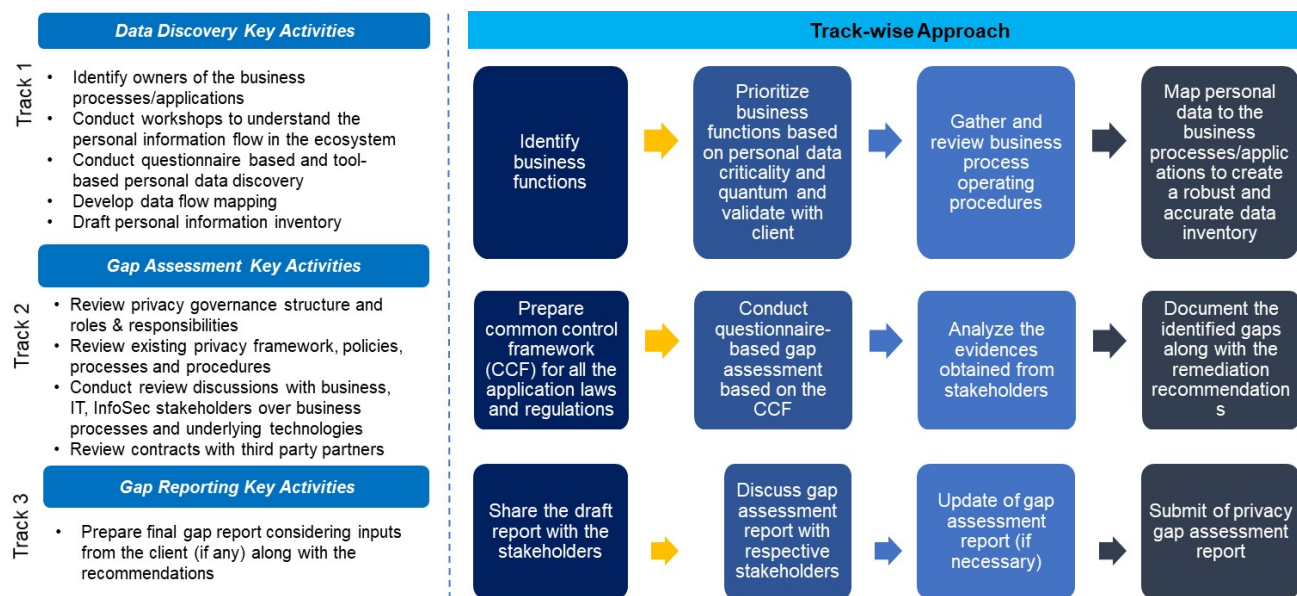


Figure 55. Data Privacy Gap and Impact Assessment Services

Formal processes have been established to:

- Prevent unauthorized access
- Detail user access registration and deregistration
- Detail user access provisioning
- Restrict and control privileged access rights
- Establish the intervals for user access rights reviews
- Ensure removal of access rights upon users' termination of employment, contract, or agreement
- Restrict and control the use of utility programs that can override system and application controls
- Restrict access to program source code
- Control access to systems and applications, where required, by a secure log on procedure
- Hold all users of SAP, systems accountable for safeguarding their authentication information
- Hold all Users of integrated components (Drupal, ServiceNow) accountable for safeguarding their authentication information
- Ensure passwords meet established complexity requirements
- Manage access for external parties

Infosys have a secure way to demonstrate the confidentiality of data at rest and in transit for the proposed solution. The integrated SaaS vendors have an elaborated procedure and mechanisms to safeguard the data in their environment. Below sections will give a broader view on Encryption of data, Data disposal, Data Segregation.

SAP Ariba

Encryption: Both data at rest as well as data in transit are encrypted. SAP Ariba encrypt sensitive data elements stored in the databases using minimum 256-bit AES (Advanced Encryption Standard) encryption. AES is the federal standard for data encryption. Encryption technology is also applied for the client connection to the Web site (Transport Layer Security (TLS) min v1.2 and preferred v1.2) and to the hosted application passwords in storage. Customer user passwords are one way hashed

using SHA256 and salted with random data. Limited SAP Ariba Operations personnel have data query access and monitoring rights for the SAP Ariba hosting program.

Agreement: Ariba solutions are designed to collect process and store Moderate Business Impact information for individuals. They identify Moderate Business Impact Data as personal contact information such as but not limited to business name, business address, business email, business telephone number or IP address. The Ariba Data Policy and Privacy Statement prohibits use of the solutions for processing sensitive personal data. Customers may not use Ariba Cloud Services for storing Sensitive Personal Information or to send documents over the Service containing such information except in limited cases documented by Ariba, where such information is stored in encrypted form, such as storage of credit card numbers in fields designated for such use. Ariba's customers are responsible for complying with laws regarding other basic personal information that might be submitted to Ariba Cloud Services though Ariba takes steps in that regard as well.

Maintenance Tools: Equipment removal is required to be managed using both an internal ticketing system as well as a data center ticketing system for process control, audit and tracking purposes.

(a) Verifying that there is no organizational information contained on the equipment.

All items of equipment containing storage media are verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

SAP deletes the logical volumes, which will cause the storage device to re-use the storage space and overwrite the customer data. By deleting the logical volumes, customer data may not be accessed or extracted.

If hardware is removed from data centers a physical decommissioning process is applied. When an IaaS provider is used, processes for secure disposal of storage devices are managed by the infrastructure service provider.

(b) Sanitizing or destroying the equipment.

We have a documented policy and procedures for the secure destruction of confidential or sensitive data. Our data disposal practices are aligned with the NIST 800-88 standards for clearing, sanitizing and data destruction to prevent data remanence prior to retiring or allowing storage media outside of our security envelope. SAP data disposal practices are aligned with the DOD 5220.22-M/ ISO 27040 and NIST 800-88 Sanitation standards for clearing, sanitizing and data destruction to prevent data remanence prior to retiring or allowing storage media outside of our security envelope.

SAP has a set of procedures that involve disk degaussing on break fix and decommissioning that complies with DOD 5220.22-M and NIST 800-88 Sanitation standards. This process includes Tape degaussing and wiping for backups as well.

(c) Retaining the equipment within the facility; or

Equipment is located to minimize unnecessary access into work areas. Information processing facilities handling sensitive data are positioned carefully to reduce the risk of information being viewed by unauthorized persons during their use. Storage facilities are secured to avoid unauthorized access. Items requiring special protection are safeguarded to reduce the general level of protection required.

Controls are adopted to minimize the risk of potential physical and environmental threats, e.g. theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation and vandalism.

ServiceNow

Encryption: To protect data while in transit, when a customer interacts to their instance of the Now Platform, the data is transmitted utilizing Hypertext Transfer Protocol Secure (HTTPS) TLS encryption.

The TLS encryption allows for 256-bit encryption. ServiceNow utilizes Entrust as the trusted certificate authority to inform users that ServiceNow's hosted web site is authentic.

To protect data at rest, the Now Platform has built in functionality to allow customer administrators to encrypt fields within database tables utilizing 256-bit encryption. This is referred to as column level encryption. Additional encryption options are available upon request.

Sanitizing or destroying the Equipment: Storage devices (HDD/SDD) that are to be replaced due to physical failure or decommissioning are stored within a safe in each co-location space. Their serial numbers are recorded centrally and the incident reference relating to their failure is labeled on the drive. On a periodic basis, quarterly or at a higher cadence if necessary, a ServiceNow Security team member will visit that co-location space and inventory the drives. The Security staff member will escort the drives to the loading dock or similar where a representative from a disk destruction company is awaiting. The ServiceNow Security staff member witnesses the drives being destroyed. A certificate of destruction will be produced for each drive. At no times do the drives leave the data center facility. The destruction follows NIST 800-88 guidelines.

Oracle

Encryption: Oracle has implemented a "ubiquitous encryption" program with the goal of encrypting all data. For customer tenant data, Oracle uses encryption both at-rest and in-transit. The Block Volumes and Object Storage services enable at-rest data encryption by default, by using the Advanced Encryption Standard (AES) algorithm with 256-bit encryption. In-transit control plane data is encrypted by using Transport Layer Security (TLS) 1.2 or later.

Microsoft Azure AD

Data integrity is a key component of the Azure Platform. Internal communication between key Azure components where customer data is transmitted and involved is secured using SSL and TLS. SSL and TLS certificates are self-signed, except for those certificates that are used for connections from outside the Azure network (including the Storage service and the FC). These certificates are issued by a Microsoft Certificate Authority (CA). Customer data is transmitted over a secure channel to the Azure platform services.

Encryption: Microsoft Azure uses encryption to prevent unauthorized disclosure of information and detect changes to information during transmission. Specifically, Azure provides FIPS 140-2 compliant ciphers that include integrity validation for customer connections, interconnected system connections, and remote access connections. For connections to customers, Azure is configured to negotiate FIPS compliant TLS protocols with supported client browsers, though non-FIPS compliant protocols are supported for legacy browser support. Connections within the accreditation boundary occur within Azure facilities. Since Azure owns and controls access to these connections, they do not require FIPS 140-2 encryption.

Customer secrets, including certificates, private keys, RDP passwords and SAKs are communicated through the SMAPI via the REST protocol, or Azure Portal over a secured channel using SSL. Customer secrets are stored in an encrypted form in Azure Storage accounts. Customer secrets are only known to the customer. Further, private root keys belonging to Azure services are protected from unauthorized access.

Customers interact with the Access Control Service namespace over the web and service endpoints. Access Control Service namespace is only accessible through HTTPS and uses SSL to encrypt transmission of customer secrets including cryptographic keys, passwords and certificates over external networks. The customer information transmitted to all the Access Control Service endpoints is encrypted over external networks.

Data Disposal: Microsoft Azure uses data erasure units and processes to cleanse/purge data in a manner consistent with NIST SP 800-88 and which are commensurate with the Microsoft Azure asset

classification of the asset. For assets requiring destruction, Microsoft Azure utilizes onsite asset destruction services.

Data segregation: Microsoft Azure Production network is structured such that publicly accessible system components are segregated from internal resources. Physical and logical boundaries exist between web servers providing access to the public-facing Microsoft Azure Management Portal and the underlying Microsoft Azure virtual infrastructure where customer application instances and customer data reside. All publicly accessible information is managed within the Azure Production network, which is subject to two-factor authentication and boundary protection mechanisms. Multiple levels of network segregation exist. Each Microsoft Azure cluster is logically segregated using a Virtual Local Area Network (VLANs) to separate customer traffic from the rest of the Microsoft network. The Datacenter VLAN contains physical nodes that are used for implementing the Microsoft Azure services. Access to the Microsoft Azure network from outside the cluster is restricted through appropriate NAT based restrictions.

Acquia

Segregation: Cloud Platform Enterprise provides independent, logically separate environments for each subscriber application. Certain parts (infrastructure and databases) of the subscriber's primary technology stack in Cloud Platform Enterprise are provisioned on unique, logically distinct infrastructure, except for load balancers. Dedicated load balancers are available to Cloud Platform Enterprise subscribers at an added cost. In Cloud Platform, Acquia manages host-based firewall policies, which provide logical isolation between distinct subscriber environments in Cloud Platform. Other parts of the technology stack, such as CDEs, Remote Administration environments and code repository environments, are shared.

Data Access: Acquia limits privileged access both to the information on the subscriber infrastructure under its management and to the infrastructure themselves. Access is limited to authorized personnel. Network layer controls ensure privileged access is always enforced through secure bastion hosts, using encrypted tunnels through nonstandard ports. Authentication requires multi-factor authentication and each user's credentials are encrypted in transit and at rest.

Agreement: When a subscriber cancels service with Acquia, the subscriber's infrastructure is terminated, and the application data is deleted. Hard drives and other storage media are never removed from the data centers before the data has been sanitized, so the data can't be recovered. When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process designed to prevent subscriber data exposure to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M (National Industrial Security Program Operating Manual) or NIST 800-88 (Guidelines for Media Sanitization) to destroy data as part of the decommissioning process. If an infrastructure device can't be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry standard practices. Subscriber confidential information is never stored outside of the AWS infrastructure for extended periods of time or on physical media, such as a CD or removable USB media.

Data Disposal: Subscriber data would only be transferred outside of Amazon's EC2 environment if needed to help solve a subscriber's problem, if the problem required local resolution steps, and if the subscriber explicitly authorized the data. After resolving the issue, the files would be purged. In practice, subscriber-sensitive information is never stored on laptops, mobile devices, or physical media outside of the protections AWS provides.

1.2.4.8 *Personally Identifiable Information Protection*

The proposed procurement solution is intended to capture very minimal sensitive personally identifiable information which is not available through other public sources. In our past experience for federal/public sector clients below categories are typically captured:

- For Suppliers at the time of registration it can include generic information such as – business name; contact information including address, email, phone number; lists of owners, directors and partners; socio-economic factors identified or to be identified within the procurement system such as minority groups, Tax identification numbers.
- For Buyers/participating entities – it can include registration details such as username, first name/last name, email address, supervisor details, contact details.
- During a procurement process – it can include supplier sensitive information such as reference details of other customers, resumes of potential supplier resources, work history.
- Other generic categories – can include audit trails for user authentication, timestamps, IP address details.

As indicated above, only personal information, with no contextual sensitivities, collected directly from the individual or authorized suppliers and collected with the user consent. The proposed procurement solution comprises of public cloud solution and is not expected to process extensive sensitive information like healthcare data, FTI, data etc. In the event such data elements need to be stored or processed, Infosys will work with the state or participating entities to identify such data collection and processing requirements and identify any additional privacy/security controls that need to be enforced.

Infosys, being a data processor, processes personal information only for providing services to the client, as documented in the services agreements. Personal data will not be used for any purpose other than that specified by Maine or participating entity

Access to personal data will be provided to Infosys personnel only on a need to know basis. Periodic access reviews are performed by the project team to ensure that access available to personnel is commensurate to their responsibilities in the project.

In addition to the non-disclosure agreement signed by each Infosys employee regardless of the project they work for, when client or regulations require additional declaration, appropriate mechanism will be implemented by the Infosys project execution team. Records of such declaration including commitment to confidentiality shall be maintained by Infosys. All employees shall undergo mandatory data privacy awareness training and quiz at least once every year.

When Infosys subcontracts personal data processing of client to a third party for further processing, it will be done with the prior written approval of the client and only after establishing that the third party has means to protect data as required by regulations and inclusion of all data privacy clauses present in the contract between Infosys and the client into the contract between Infosys and the subcontractor.

Any personal data obtained from or on behalf of the state for project work shall not be retained indefinitely and will be destroyed or returned, as required by the client, when the agreed retention period lapses unless legal requirements need longer retention.

Apart from the above-mentioned organizational security controls measures taken to protect personal data, Infosys will also ensure that the solution components considered for Maine's have appropriate technical security controls and measure for safeguarding personal data which are mentioned as below:

- a) Establish, maintain, and update an inventory of all systems, applications, and projects that process personally identifiable information. An inventory of systems, applications, and projects that process

personally identifiable information supports the mapping of data actions, providing individuals with privacy notices, maintaining accurate personally identifiable information, and limiting the processing of personally identifiable information when such information is not needed for operational purposes. The State of Maine should use this inventory to ensure that systems only process the personally identifiable information for authorized purposes and that this processing is still relevant and necessary for the purpose specified therein

- b) Personally, Identifiable Information Quality Management: Infosys will develop and document organization-wide policies and procedures for
- Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle
 - Check the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle
 - Correct or delete inaccurate or outdated personally identifiable information. Correcting or deleting inaccurate or outdated personally identifiable information
 - Disseminating notice of corrected or deleted personally identifiable information to individuals or other appropriate entities and
 - Appeals of adverse decisions on correction or deletion requests
 - The information life cycle includes the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposition of personally identifiable information
 - Additionally, processes include the provision of responses to individuals of decisions to deny requests for correction or deletion. The responses include the reasons for the decisions, a means to record individual objections to the decisions, and a means of requesting reviews of the initial determinations.
 - Due to the complexity of data flows and storage, other entities may need to be informed of the correction or deletion. Notice supports the consistent correction and deletion of personally identifiable information across the data ecosystem.
- c) Minimization of Personally Identifiable Information Used in Testing, Training, and Research
- Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research.
 - Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes.
 - Authorize the use of personally identifiable information when such information is required for internal testing, training, and research.
 - The use of personally identifiable information in testing, research, and training increases the risk of unauthorized disclosure or misuse of such information.
 - Review and update policies and procedures.
- d) Authority to Process Personally Identifiable Information
- Determine and document the State of Maine authority that permits processing of personally identifiable information; and
 - Restrict the processing of personally identifiable information to only that which is authorized.
 - Processing includes but is not limited to creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal. Processing operations also include logging, generation, and transformation, as well as analysis techniques, such as data mining.
 - The State of Maine may be subject to laws, executive orders, directives, regulations, or policies that establish the organization's authority and thereby limit certain types of processing of

personally identifiable information or establish other requirements related to the processing

- While processing of personally identifiable information may be legally permissible, privacy risks may still arise. Privacy risk assessments can identify the privacy risks associated with the authorized processing of personally identifiable information and support solutions to manage such risks.

e) Authority to Process Personally Identifiable Information | Automation

- Track processing purposes of personally identifiable information using automated mechanisms where possible, else conduct periodic review and audit.

f) Specific Categories of Personally Identifiable Information

- Apply processing conditions for specific categories of personally identifiable information.
- The State of Maine may apply any conditions or protections that may be necessary for specific categories of personally identifiable information. These conditions may be required by laws, executive orders, directives, regulations, policies, standards, or guidelines
- The requirements may also come from the results of privacy risk assessments that factor in contextual changes that may result in an organizational determination that a particular category of personally identifiable information is particularly sensitive or raises privacy risks.

g) Development Process, Standards, and Tools | Minimize Personally Identifiable Information

- Require the developer of the system or system component to minimize the use of personally identifiable information in development and test environments.
- State of Maine can minimize the risk to an individual's privacy by using techniques such as de-identification or synthetic data. Limiting the use of personally identifiable information in development and test environments helps reduce the level of privacy risk created by a system.

h) Boundary Protection | Personally Identifiable Information: For systems that process personally identifiable information:

- Apply the following processing rules to data elements of personally identifiable information: State of Maine -defined processing rules
- Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system
- Document each processing exception; and
- Review and remove exceptions that are no longer supported

i) Information Management and Retention | Limit Personally Identifiable Information Elements

- Limit personally identifiable information being processed in the information life cycle to the elements defined as PII by the State.
- Limiting the use of personally identifiable information throughout the information life cycle when the information is not needed for operational purposes helps to reduce the level of privacy risk created by a system
- The information life cycle includes information creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposition. Risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to determining which elements of personally identifiable information may create risk.

j) Personally, Identifiable Information Quality Operations | Notice of Correction or Deletion

- Notify recipients of personally identifiable information and individuals that the personally identifiable information has been corrected or deleted.
- When personally identifiable information is corrected or deleted, the State of Maine take steps

to ensure that all authorized recipients of such information, and the individual with whom the information is associated or their designated representatives, are informed of the corrected or deleted information.

Within the procurement solution, SAP Ariba is the core solution component which will collect, store, and process such information. Also given that SAP Ariba is a SaaS service offering, Infosys will inherit the privacy controls of SAP Ariba solution and apply any residual controls permissible within the SaaS framework. The security and privacy controls currently enforced by SAP are detailed below:

SAP Ariba has 13 data centers across the world, and it provides the flexibility to run SAP Ariba Procurement portfolio, in several regional data centers.

- Personal data of clients is administered in the selected application data center.
- Supplier profiles are stored in the Ariba Network data center operated in the United States (US).
- Most SAP Ariba applications exchange data with Ariba Network to facilitate communication with suppliers; the exchange can include personal data, such as contact information on a purchase order.
- The data exchange between regional data centers and Ariba Network is provided exclusively over industry-standard encrypted connections.

SAP 1.1 Physical Access Control.

Unauthorized persons shall be prevented from gaining physical access to premises, buildings, or rooms where data processing systems are located which process and/or use Personal Data.

Measures: All Data Centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and Data Center facilities from being compromised. Only authorized representatives have access to systems and infrastructure within the Data Center facilities. To ensure proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) are maintained on a regular basis. In detail, the following physical security measures are implemented at all Data Centers:

- a) SAP protects its assets and facilities using the appropriate means based on a security classification conducted by an internal security department.
- b) In general, buildings are secured through access control systems (smart card access system).
- c) As a minimum requirement, the outermost shell of the building must be fitted with a certified key system including modern, active key management.
- d) Depending on the security classification, buildings, individual areas, and surrounding premises are further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems.
- e) Access rights will be granted to authorized persons on an individual basis according to the System and Data Access Control measures set out below. This also applies to visitor access. Guests and visitors to SAP buildings must register their names at reception and must be accompanied by authorized SAP personnel. SAP and all third-party Data Center providers are logging the names and times of persons entering the private areas of SAP within the Data Centers.
- f) SAP employees and external personnel must wear their ID cards at all SAP locations.

SAP 1.2 System Access Control

Data processing systems used to provide the Cloud Service must be prevented from being used without authorization.

Measures:

(a) Multiple authorization levels are used to grant access to sensitive systems including those storing and processing Personal Data. Processes are in place to ensure that only authorized users have the appropriate authorization to add, delete, or modify users.

(b) All users access SAP's systems with a unique identifier (user ID).

(c) SAP has procedures in place to ensure that requested authorization changes are implemented
Data Processing Agreement for SAP Cloud Services enGLOBAL.v.4-2016 Page 16 of 19 Page 334 of 360

only in accordance with the guidelines (for example, no rights are granted without authorization). If a user changes role or leaves the company, its access rights are revoked.

(d) SAP has established a password policy that prohibits the sharing of passwords, governs what to do if a password is disclosed, requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. In case of domain passwords, the system forces a password change every six months complying with the requirements for complex passwords. Each computer has a password-protected screensaver.

(e) Remote access to the Cloud Service delivery environment requires at least strong authentication mechanisms (for instance a combination of a password and an additional security feature). Passwords with a minimum length of fifteen (15) characters must be used for administrative accounts and service accounts of security-critical IT systems. New passwords must be different from an Authorized User's last five (5) passwords. The company network is protected from the public network by firewalls.

(f) SAP uses up-to-date antivirus software at access points to the company network (for email accounts) and on all file servers and all workstations.

(g) A security patch management is implemented to ensure deployment of relevant security updates.

(h) Full remote access to SAP's corporate network and critical infrastructure is protected by strong authentication.

SAP 1.3 Data Access Control

Persons entitled to use data processing systems shall gain access only to the Personal Data that they have a right to access, and Personal Data must not be read, copied, modified or removed without authorization in the course of processing, use and storage.

Measures:

(a) Access to personal, confidential, or sensitive information is granted on a need-to-know basis. In other words, employees or external third parties have access to the information that they require to complete their work. SAP uses authorization concepts that document how

authorizations are assigned and which authorizations are assigned. All personal, confidential, or otherwise sensitive data is protected in accordance with the SAP security policies and standards.

(b) All production servers of any SAP Cloud Service are operated in the relevant Data Centers/server rooms. Security measures that protect applications processing personal, confidential, or other sensitive information are regularly checked. To this end, SAP conducts internal and external security checks and penetration tests on the IT systems.

(c) SAP does not allow the installation of personal software or other software not approved by SAP to systems being used for any Cloud Service.

(d) SAP security standard governs how data and data carriers are deleted or destroyed.

SAP 1.4 Data Transmission Control

Personal Data must not be read, copied, modified, or removed without authorization during transfer.

Measures:

(a) Where data carriers are physically transported, adequate measures are implemented at SAP to ensure the agreed service levels (for example, encryption, and lead-lined containers).

(b) Personal Data transfer over SAP internal networks are protected as any other confidential data according to SAP Security Policy. Data Processing Agreement for SAP Cloud Services enGLOBAL.v.4-2016 Page 17 of 19 Page 335 of 360

(c) When the data is transferred between SAP and its customers, the protection measures for the transferred Personal Data are mutually agreed in the Agreement. This applies to both physical and network based data transfer. In any case the Customer assumes responsibility for any data transfer from SAP's Point of Demarcation (e.g., outgoing firewall of the SAP Data Center which hosts the Cloud Service).

SAP 1.5 Data Input Control

It shall be possible to retrospectively examine and establish whether and by whom at SAP Personal Data have been entered, modified, or removed from data processing systems used to provide the Cloud Service.

Measures:

SAP only allows authorized persons to access Personal Data as required in the course of their work. SAP implemented a logging system for input, modification, and deletion, or blocking of Personal Data by SAP or its Sub processors to the greatest extent supported by the Cloud Service.

SAP 1.6 Job Control

Personal Data being processed on commission shall be processed solely in accordance with the Agreement and related instructions of the Customer.

Measures:

(a) SAP uses controls and processes to ensure compliance with contracts between SAP and its customers, Sub processors or other service providers.

(b) As part of the SAP Security Policy, Customer Data requires at least the same protection level as "confidential" information according to the SAP Information Classification standard.

(c) All SAP employees and contractual partners are contractually bound to respect the confidentiality of all sensitive information including trade secrets of SAP customers and partners.

SAP 1.7 Availability Control

Personal Data shall be protected against accidental or unauthorized destruction or loss.

Measures:

(a) SAP employs backup processes and other measures that ensure rapid restoration of business-critical systems as and when necessary.

(b) SAP uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to ensure power availability to the Data Centers.

(c) SAP has defined contingency plans as well as business and disaster recovery strategies for Cloud Services.

(d) Emergency processes and systems are regularly tested.

SAP 1.8 Data Separation Control

Personal Data collected for different purposes can be processed separately.

Measures:

(a) SAP uses the technical capabilities of the deployed software (for example: multi-tenancy or separate system landscapes) to achieve data separation between Personal Data from one and any other customer.

(b) SAP maintains dedicated instances (with logical or physical separation) for each Customer.

(c) Customers (including their Affiliates) have access only to own Customer instance(s).

Data Processing Agreement for SAP Cloud Services enGLOBAL.v.4-2016 P

SAP 1.9 Data Integrity Control

Ensures that Personal Data will remain intact, complete, and current during processing activities:

Measures:

SAP has implemented a defense strategy in several layers as a protection against unauthorized modifications. This refers to controls as stated in the control and measure sections as described above.

In particular:

(a) Firewalls

(b) Security Monitoring Center

(c) Antivirus software

(d) Backup and recovery

(e) External and internal penetration testing

(f) Regular external audits to prove security measures

SAP Ariba is GDPR compliant and features/services which SAP Ariba provides to support GDPR compliance includes:

Table 33. GDPR Aspects of SAP Ariba

GDPR Aspect	Product Functionality / Technical Feature
Information/ Transparency	• Display of personal data is available. • Records of processing activities are aligned to GDPR requirements. • Privacy impact assessments (PIAs) are conducted for new products/services (innovations) and product/service changes in the release cycle. • Changes to personal data and privacy settings are logged.
Access to data	Personal data can be accessed only by a user who has been authorized by the SAP Ariba central authentication and authorization mechanisms

GDPR Aspect	Product Functionality / Technical Feature
Rectification of Data	Personal data can be corrected by an authorized user, such as the customer's administrator.
Erasure of data	Data will typically be erased at contract termination; individual personal data deletion is implemented by using anonymization/obfuscation.
Restriction of Processing	Restriction of data processing at the transaction level is not currently implemented; user-level deactivation is available to customer administrator
Data portability	Data portability via export to comma-separated values (CSV) files is available to customer administrators.
Data breach notification	Notification is currently implemented by utilizing the existing security incident process.
Privacy by design and by default	SAP Ariba product development follows the SAP guiding product standard security requirements. Additional privacy principles are applied in the design phase, such as the practice of minimized personally identifiable information (PII) data collection. Default settings are set to the maximum restriction.
Consent	Consent is given by actively accepting the SAP Ariba Privacy Statement (which includes the purpose, the categories of personal data, and other relevant considerations)

Infosys or SAP Ariba does not provide Personal Data to third parties, except as agreed in the contract which include below scenarios:

- State contract authority or its authorized representatives request or authorize it.
- Such disclosure is necessary to process transactions or provide services within the procurement solution (e.g., PCARD processing with credit card companies).
- SAP Ariba is compelled to do so by a governmental authority, regulatory body, or under subpoena or similar governmental request or to establish or defend a legal claim.
- The third party is acting as agent or sub-contractor in performing services or legal compliance activities (e.g., SAP Ariba's use of a third-party e-signature provider); or
- State or Supplier designate Personal Data to be publicly viewable in the Solution.

GDPR (ariba.com)

Additional solution components such as Oracle cloud integration (OCI), ServiceNow, Portal (Acquia) and Identity and Credentials Management do not collect any personal information like Ariba. However, user tracking information (IP address, location), cookies and email address, first name, Last Name (in case of identity credentials management, ServiceNow -is required for creation of user profile) is collected. All the data resides in a US location or North America Region. Each of the Cloud Service Providers have similar security controls enforced such as Role Based Access, Encryption etc. for securing the personal identifiable data. Details of the data collected is mentioned in each of the CSP's privacy statement. As mentioned above, Infosys will provide consent to collect such data in agreement with State of Maine and follow the guidelines for disclosure and storage.

The diagram below represents the lifecycle of Infosys managed PII data:

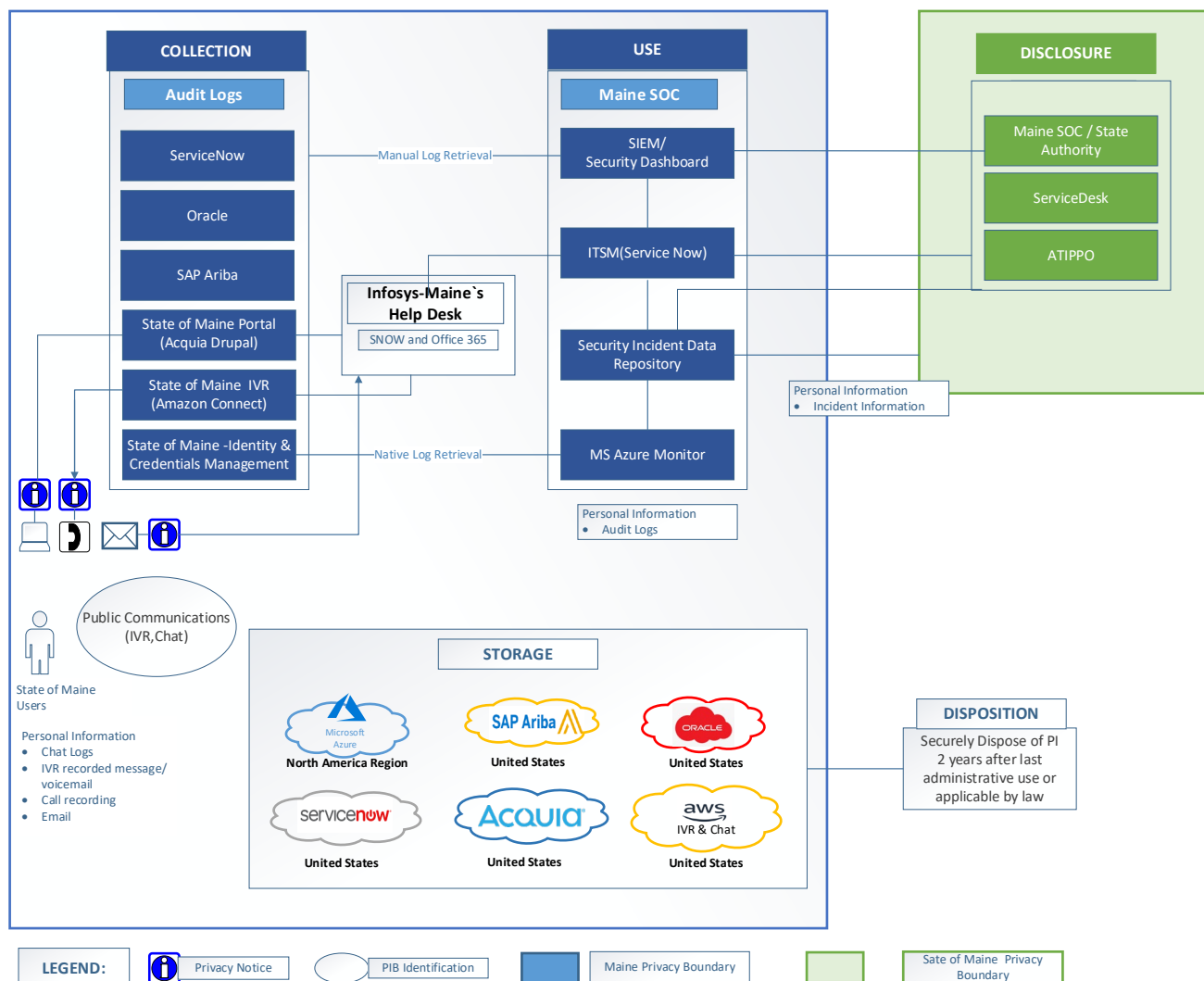


Figure 56. Lifecycle of Infosys managed PII Data

1.2.4.9 Security/Privacy Issue Occurrence

Infosys will report to the State of Maine any security and privacy issue, pertaining to client PII, security breaches etc. promptly upon its discovery. All privacy incidents identified by Infosys are reported to the Infosys' Data Privacy Office, which determines the next steps after an assessment of the incident.

Similarly, all the security incidents upon detection are reported to the client's Chief Information security officer with their incident details and severity. Based on the level of severity relevant participating entities are kept informed.

Infosys work with relevant cloud providers to gather relevant data for the investigations and further co-ordinate with cloud providers to ensure avoidance of reoccurrence of such incidents.

Root cause analysis is performed, and corrective and preventive actions are identified. Infosys will work with the client and CSP's to implement suitable controls to prevent future recurrence of identified issues.

Security & Privacy incidents occurred in any of the CSP's (Cloud Service providers) realm, Infosys will co-ordinate with CSP's. Each of the CSP's components have their internal incident policies and procedures which are based on industry recognized process and certified.

In SAP Ariba, upon notification of a security incident from Infosys SOC personal /designated individual or channel, a documentation trail is begun by the Ariba's InfoSec department and an internal ticket in SAP Ariba is created as the record of reference. The lead security manager of SAP Ariba's calls a meeting including all personnel required to contain and reduce risk and impact appropriate to the nature of the incident.

Within SAP Ariba, tasks are assigned with milestones to be met to validate and determine extent of the incident. Communication is made to the Privacy & Security Board to alert principal membership and foster internal cooperation and awareness. Communication is made to Infosys to include the nature of the incident, actions taken to contain the incident and potential effects of actions if any, in regard to sustained business process and availability of the system. Any workarounds or hot fixes necessary in the solutions are communicated and scheduled reporting to the client is established with an identified single point of contact within SAP Ariba. Based on the nature of the incident, if required, legal counsel present at initial risk & impact meeting, will assist in communicating with law enforcement contacts. Infosys designated SOC personals is kept informed of the milestones met and at scheduled intervals until the incident is fully contained and no further risks or impacts are perceived. All incidents are required to be internally managed by Ariba's InfoSec to include tracking and review on a weekly basis.

SAP Ariba security incidents are audited every six months and evaluated against the Trust Services Principles of ISAE 3402 and the PCI DSS standards as appropriate. All incident reports are presented to and reviewed by the Privacy & Security Board of SAP Ariba and are formally closed with discussion and evaluation to determine what actions can be taken to prevent similar incidents. Depending on the nature of the incident and impact to Infosys and State of Maine, security incidents are not formally closed by the board until appropriate measures to remediate the initial threat are formally communicated.

A similar process is followed for other cloud components such as ServiceNow, Microsoft Azure, Oracle and Acquia cloud. Each of the CSP's have a designed incident response manager and staff to investigate and provide evidence of any security and privacy incident occurred in their environment. All these processes and procedures are documented, and reference is provided in the incident management framework and the SOC2 audit reports.

Upon notification of a security incident, a documentation trail is started by the InfoSec department and an internal ticket is created as the record of reference. The lead security manager initiates a meeting of all personnel required to contain and reduce risk and impact appropriate to the nature of the incident.

Tasks are assigned with milestones to be met to validate and determine extent of the incident. Communication is made to the Privacy & Security Board to alert principal membership and foster internal cooperation and awareness. An appropriate communication channel to the affected customer(s) is determined based on how we were notified of the incident, i.e., from a customer, from an internal report or from a third-party report. Communication is made to the affected customer(s) to include the nature of the incident, actions taken to contain the incident and potential effects of actions if any, in regard to sustained business process and availability of the system.

Any workarounds or hot fixes necessary in the solutions are communicated and scheduled reporting to the customer(s) is established with an identified single point of contact within our company. Based on the nature of the incident, if required, legal counsel present at initial risk & impact meeting, will assist in communicating with law enforcement contacts. The customer is kept informed of the milestones met and at scheduled intervals until the incident is fully contained and no further risk and impact perceived. All incidents are required to be internally managed by InfoSec to include tracking and review on a weekly basis and evaluation of the actions taken in regard to our security concept.

All incident reports are presented to and reviewed by the Privacy & Security Board and are formally closed with discussion and evaluation to determine what actions can be taken to prevent similar incidents. Depending on the nature of the incident and impact to customer(s), security incidents are not formally closed by the board until all affected customers are made aware of the incident and appropriate measures to remediate the initial threat are formally communicated.

1.2.4.10 PII Data Actual/Attempted Access or Disclosure

Once an incident is identified and IPS initiates its privacy incident process, IPS team members will support Maine in its execution of the State Data Breach Protocol by facilitating State's adherence to US privacy laws.

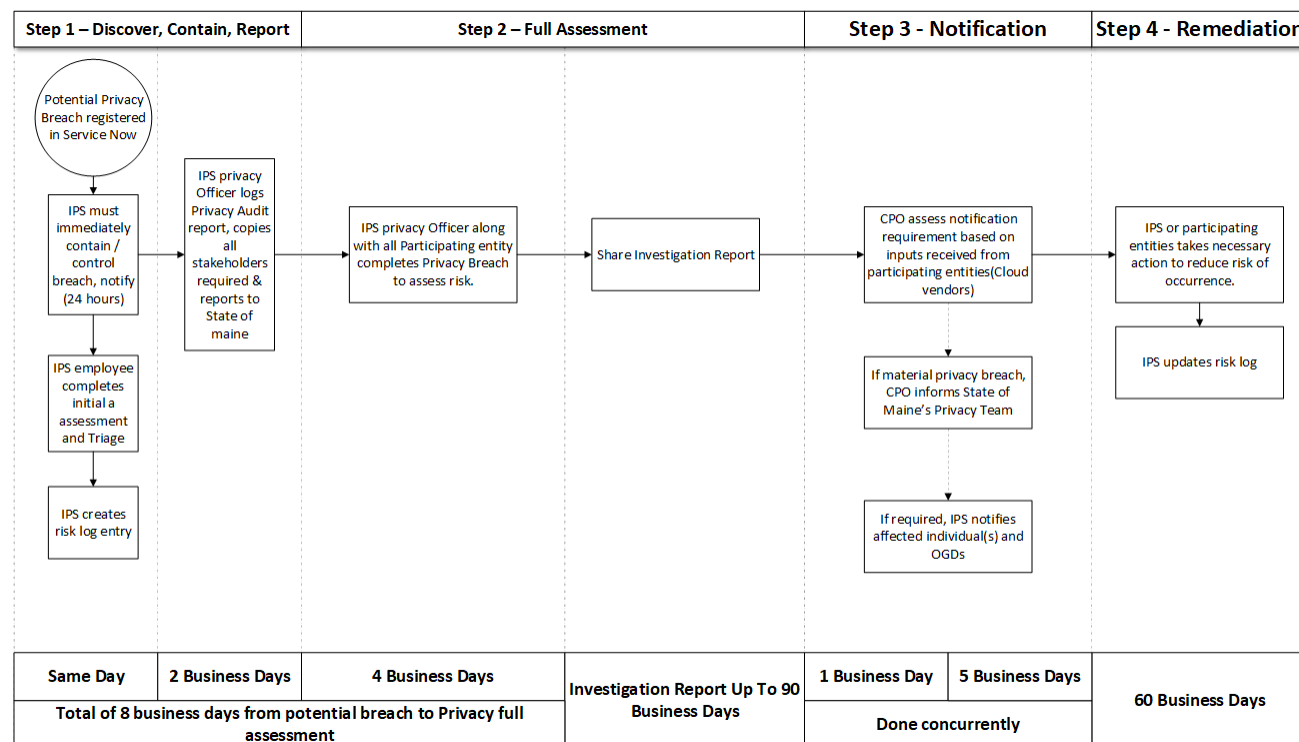


Figure 57. Privacy Breach Notification Process

The participating cloud vendors for Maine solution have their specific Breach and incident notification process. In case of any incident or potential breach the various components will respond as per following:

SAP Ariba

SAP shall promptly inform IPS as soon as it becomes aware of serious disruptions of the processing operations, or any Security Breach in connection with the processing of Personal Information which, in each case, may significantly harm the interest of the Data Subjects concerned.

Furthermore, Infosys has additional terms with SAP which extend to IPS as follows:

Service Provider shall notify Infosys immediately (not exceeding 24 hours) of becoming aware of any actual or potential data breach. In the unlikely event, where data breach or any security related incident involves any Personal Information, Service Provider shall comply with the following terms and conditions without any deviations, unless instructed by Infosys in writing. Service Provider to:

- a. Notify Infosys of the data breach within 12 hours of discovery or becoming aware.

- b. Take prompt measures to contain and control any further exposure of such data involved in the data breach.
- c. Submit a preliminary report to Infosys within 36 hours of discovery of the breach containing the details, including, but not limited to type of data attributes involved, volume, geography, type of individuals affected and potential implications to Infosys under Applicable Privacy Laws.
- d. Monitor the situation closely and use reasonable efforts to remedy the circumstances that permitted to the occurrence of the breach at the first place.
- e. Coordinate with the Infosys, its staff and any third party investigators appointed by Infosys, and to submit a detailed report, which may not exceed seven (7) working days from the date of discovery of the breach, unless Infosys agrees in writing.
- f. Provide full support to cooperate in the investigation, including any reasonable access to Infosys, their authorized staffs, including any third party investigators to the data processing unit or facility where the breach occurred.
- g. Provide full identity and credit restoration services for each individual impacted by the breach and include a cyber-insurance coverage for any identify theft, where PI includes sensitive information of financial nature.
- h. notify Infosys about the corrective actions taken by Service Provider to prevent recurrence of such breaches.
- i. Co-operate with Infosys in determining whether any notification is legally required as per applicable 'governing laws & regulations' or appropriate as a business matter; and
- j. Indemnify, defend, and hold Infosys, its officers, directors, employees, contractors for any claims, disputes or damages arising out of the data breach.
- k. Pay for costs associated with the data breach including without limitation the costs of notification to any government or affected individual(s), third party consultant fees, attorney fees.

Notwithstanding anything to the contrary, Infosys reserves its right to seek injunctive or equitable relief available under the laws of the land, as may be deemed proper by a court of competent jurisdiction.

Oracle

Oracle has implemented controls and policies designed to detect and promptly respond to incidents that create suspicion of or indicate destruction, loss, alteration, unauthorized disclosure or access to Personal Information transmitted, stored or otherwise Processed. Oracle will promptly define escalation paths to investigate such incidents in order to confirm if a Personal Information Breach has occurred, and to take reasonable measures designed to identify the root cause(s) of the Personal Information Breach, mitigate any possible adverse effects and prevent a recurrence.

Oracle will notify IPS of a confirmed Personal Information Breach without undue delay but at the latest within 24 hours. As information regarding the Personal Information Breach is collected or otherwise reasonably becomes available to Oracle, Oracle will also provide with

- a. a description of the nature and reasonably anticipated consequences of the Personal Information Breach.
- b. the measures taken to mitigate any possible adverse effects and prevent a recurrence; and
- c. where possible, information about the types of Personal Information that were the subject of the Personal Information Breach.

Microsoft Azure

Microsoft notifies impacted customers and regulatory authorities of data breaches as required. Microsoft relies on heavy internal compartmentalization in the operation of Azure. Data flow logs are also robust. As a benefit of this design, most incidents can be scoped to specific customers. The goal is to provide impacted customers with an accurate, actionable, and timely notice when their data has been breached.

After the declaration of a CRSPI, the notification process takes place as expeditiously as possible while still considering the security risks of moving quickly. Generally, the process of drafting notifications occurs as the incident investigation is ongoing. Customer notices are delivered in no more than 72 hours from the time we declared a breach except in the following circumstances:

- a. Microsoft believes that the act of performing a notification increases the risk to other customers. For example, the act of notifying may tip off an adversary causing an inability to remediate.
- b. Other unusual or extreme circumstances vetted by Microsoft's legal department and the Executive Incident Manager.
- c. The 72-hour timeline may leave some incident details available. These details are provided to customers and regulatory authorities as the investigation proceeds.

Microsoft provides impacted customers with detailed information enabling them to perform internal investigations and assisting them in meeting end-user commitments, while not unduly delaying the notification process.

ServiceNow

ServiceNow will monitor, analyze and respond to security incidents in a timely manner in accordance with ServiceNow's standard operating procedure. ServiceNow's security group will escalate and engage response teams as may be necessary to address an incident.

Unless notification is delayed by the actions or demands of a law enforcement agency, ServiceNow will report to Customer any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data (a "Breach") without undue delay following determination by ServiceNow that a Breach has occurred.

The initial report will be made to IPS security or privacy contact(s) designated in ServiceNow's customer support portal (or if no such contact(s) are designated, to the primary contact designated by Customer). As information is collected or otherwise becomes available to ServiceNow, and unless prohibited by applicable law, ServiceNow shall provide without undue delay any further information regarding the nature and consequences of the Breach to allow IPS to notify relevant parties, including affected Data Subjects, government agencies and data protection authorities in accordance with Data Protection Laws. The report will include the name and contact information of the ServiceNow contact from whom additional information may be obtained. ServiceNow shall inform IPS of the measures that it will adopt to mitigate the cause of the Breach and to prevent future Breaches.

IPS will cooperate with ServiceNow in maintaining accurate contact information in the customer support portal and by providing any information that is reasonably requested to resolve any security incident, including any Breaches, identify its root cause(s) and prevent a recurrence

Acquia

Acquia maintains a security incident management policy and shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized

disclosure of, or access to Personal Data transmitted, stored or otherwise Processed by Acquia or its Sub-processors of which Acquia becomes aware (a “Personal Data Incident”), as required to assist the Customer in ensuring compliance with its obligations to notify the Supervisory Authority in the event of Personal Data breach.

Acquia shall make reasonable efforts to identify the cause of such Personal Data Incident and take those steps as Acquia deems necessary and reasonable in order to remediate the cause of such a Personal Data Incident to the extent the remediation is within Acquia’s reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer’s users.

The breach is investigated for root cause analysis and preventive action instituted in accordance with the Personal Data Incident Management process of client in the client network and as per Infosys process within Infosys network, as applicable. An incident report containing the details of the incident, data breached, corrective and preventive actions taken is submitted to the client.

The report will consist:

- a. A general description of the incident, including date and time
- b. the circumstances that gave rise to the incident
- c. an inventory of the personal information that was or may have been compromised
- d. the individual, parties, or groups of parties, whose personal information has been wrongfully disclosed or accessed, stolen, or lost
- e. how the affected individual, parties, or groups of parties were identified
- f. the party responsible for the personal information involved
- g. any other relevant information

Since there may be breach reporting obligations and a need to notify data subjects about the breach, appropriate awareness is created within project teams to report any such breach to the Data Privacy Office and relevant stakeholders immediately. In cases where there may be a need to notify data subjects about the breach. Infosys will work with the client’s legal, data privacy and management teams to adhere to local law requirements about notification requirements. Infosys will assist the State of Maine in their breach management process, as required.

Please see above (Security/Privacy Issue Occurrence), any breach or accidental exposure PII data will also consider as a security and privacy incident and same above protocol would follow with CSP’s.

1.2.4.11 Security Breach Reporting

Infosys will follow comprehensive Security Incident/Breach Management Response Framework and work closely with its SaaS /PaaS Service Provider (partner like SAP Ariba, Oracle and Acquia) to provide the beach notification and Analysis Services for Incident Response. Infosys will notify State of Maine within 2 hours of the Security Breach/Incident is notified to Infosys by individuals, cloud Service Providers.

Below diagram depicts the framework which Infosys will adopt for reporting the breach to the State of Maine.

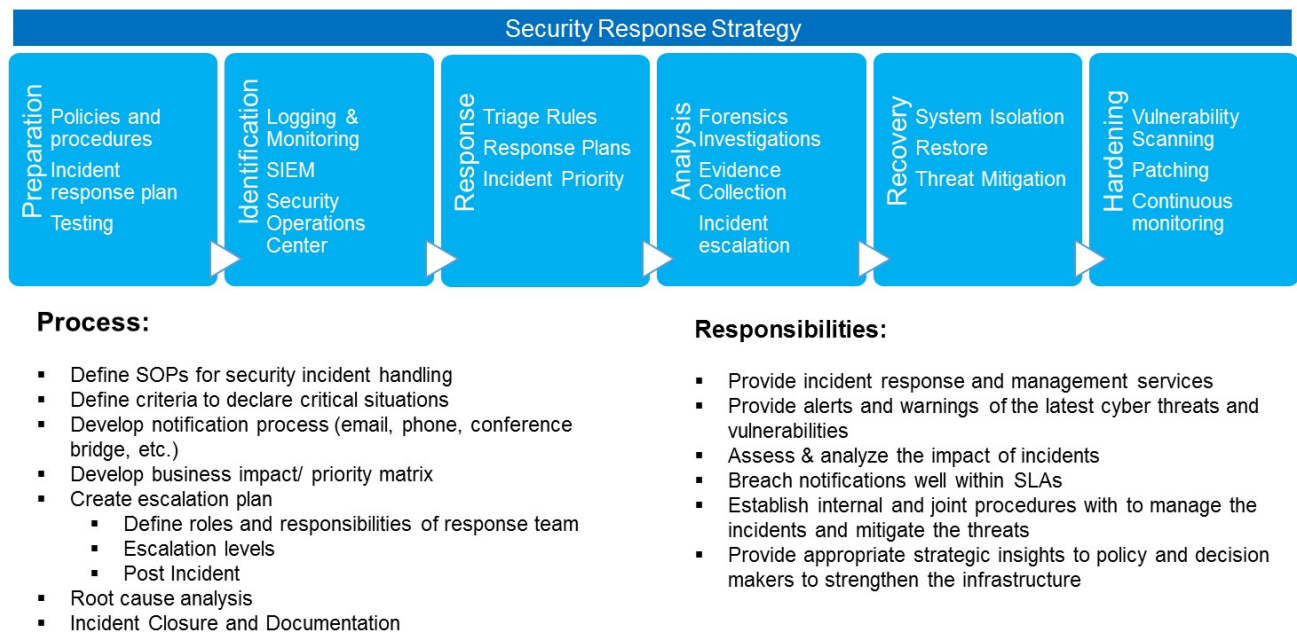


Figure 58. Critical security incident response plan

Incident reporting is done only after Infosys has reasonably determined that a security incident impacts the State of Maine or State of Maine's Data. Infosys policies do not allow granting State's any logical access to Infosys systems or networks for the purpose of carrying out investigations. However, Infosys can reasonably support the Data Breach investigation of the States by providing the relevant incident reports and data to the extent it does not result in violation of its confidentiality terms with other Clients.

Infosys will coordinate with respective CSP's in the event of security & privacy breach notification or incident. The breach can be notified by any public / anonymous user or state users or Infosys administrator. CSP's will investigate and as explained in the above section will provide the relevant evidence.

As explained above, in Section 1.2.4.9 Security/Privacy Issue Occurrence, Infosys will coordinate with respective cloud service provider's to gather the data and evidence and report to State of Maine.

Below section highlights the process for security / privacy breach occurrence in SAP Ariba and Infosys involvement in the vendor coordination and providing the reporting and notification to State of Maine. Its important to note, CSP's will provide support to Infosys & State of Maine during such investigations.

Each CSP has a specific procedure in case of Security breaches/Incident. For SAP Ariba,

SAP Ariba Support Policy: What to expect.

Priority	Definition	Initial Reaction Time		Ongoing Response Time		Resolution Targets**	
		Enterprise Support	Preferred Care	Enterprise Support	Preferred Care	Enterprise Support	Preferred Care
P1 Very High	An incident should be categorized with the priority very high if the problem has very serious consequences for normal business processes or IT processes related to core business processes and a work around is not available. Urgent work cannot be performed. This is generally caused by the following circumstances:	1 hour	1 hour	1 hour*	1 hour*	4 hours	4 hours
	•A production service is completely down.						
	•The imminent system Go-Live or upgrade of a production system cannot be completed.						
	•The customer's core business processes are seriously affected.						
P2 High	An incident should be categorized with the priority high if normal business processes are seriously affected. Necessary tasks cannot be performed. This is caused by incorrect or inoperable functions in the SAP service that are required immediately. The incident is to be processed as quickly as possible because a continuing malfunction can seriously disrupt the entire productive business flow.	4 hours	2 hours	6 hours*	6 hours	n/a	3 business days
P3 Medium	An incident should be categorized with the priority medium if normal business processes are affected. The problem is caused by incorrect or inoperable functions in the SAP service.	1 business day	4 business hours	3 business days* (non-defects) 10 business days* (defects)	3 business days* (non-defects) 10 business days* (defects)	n/a	n/a
P4 Low	An incident should be categorized with the priority low if the problem has little or no effect on normal business processes. The problem is caused by incorrect or inoperable functions in the SAP service that are not required daily, or are rarely used.	2 business day	8 business hours	1 week*	1 week*	n/a	n/a

*Unless otherwise communicated by SAP Support

**SAP to provide for issues either a (i) resolution, or (ii) workaround or (iii) action plan

Figure 59. SAP Ariba Support policy

Microsoft Azure

Whenever Microsoft becomes aware of a breach of security involving unauthorized loss, disclosure, or modification of customer data, Microsoft notifies affected customers within 72 hours as outlined in the Data Protection Addendum (DPA) of the Online Services Terms (OST). The notification timeline commitment begins when the official security incident declaration occurs. Upon declaring a security incident, the notification process occurs as expeditiously as possible, without undue delay.

Notifications include a description of the nature of the breach, approximate user impact, and mitigation steps (if applicable). If Microsoft's investigation is not complete at the time of initial notification, the notification will also indicate next steps and timelines for subsequent communication.

If a customer becomes aware of an incident that could have an impact on Microsoft, including but not limited to a data breach, the customer is responsible for promptly notifying Microsoft of the incident as defined in the DPA.

Oracle

Upon discovery of an incident, Oracle defines an incident-response plan for rapid and effective incident investigation, response, and recovery. Root-cause analysis is performed to identify opportunities for reasonable measures which improve security posture and defense in depth. Formal procedures and systems are utilized within the Lines of Business (LOB) to collect information and maintain a chain of custody for evidence during incident investigation. Oracle can support legally admissible forensic data collection when necessary.

If Oracle determines that a security incident has occurred, Oracle promptly notifies any impacted customers or other third parties in accordance with its contractual and regulatory responsibilities. Information about malicious attempts or suspected incidents is Oracle Confidential and is not externally shared. Incident history is also Oracle Confidential and is also not shared externally.

Acquia

“Security Incident” means (i) the loss of, (ii) unauthorized acquisition, use or disclosure of, or (iii) unauthorized access to, Customer Data resulting from a security breach of the Acquia platform. Acquia maintains a response function capable of identifying and assessing the seriousness and extent of a Security Incident, mitigating the effect of a Security Incident, conducting root cause analysis, implementing and documenting remedial action plans, and preventing the recurrence of Security Incidents. Acquia has an established set of procedures to ensure personnel and

contractors promptly report actual and/or suspected breaches of security. Acquia keeps an up-to-date incident management plan designed to promptly identify, prevent, investigate, and mitigate any Security Incidents, as well as performing required recovery actions to remedy the impact.

- a) Security Incidents on Acquia’s platform are logged and reviewed, secured, and retained as required by applicable laws and regulations.
- b) In the case of a Security Incident that relates to Customer Data, Acquia shall
 1. promptly assess and contain such Security Incident,
 2. notify Customer, without undue delay, upon becoming aware of such Incident, and in no case later than forty-eight (48) hours after Acquia has become aware of such Security Incident, via a Support ticket to each of the individuals identified by Customer for distribution of such Support Tickets (or such other addresses as may be provided by Customer from time to time) and provide regular status updates to Customer regarding the investigation at a frequency reasonably requested by Customer depending upon the severity of such Incident,
 3. as applicable, provide reasonable cooperation and assistance to Customer needed to fulfill customer’s obligations related to Customer’s use of the Services, as applicable, and
 4. Immediately take all steps reasonably necessary and within Acquia’s reasonable control, including without limitation, those reasonably requested by Customer, to limit, stop, prevent and remediate such Incident.

Following this initial notification, Acquia will promptly investigate the Security Incident and take all reasonable and necessary steps to prevent any further compromise of the Customer Data. If a security deficiency is identified within any Acquia information system during this investigation, Acquia will provide a report to Customer containing a description of the nature of the Security Incident, an identification of any Customer Data that was disclosed, destroyed, altered or compromised, and any investigative, corrective, or remedial actions taken or planned by Acquia to mitigate the risk of further Security Incidents. Acquia will maintain log files sufficient to enable Customer to determine what Customer Data was accessed and when, regardless of whether such data is physically or electronically maintained.

Infosys after the final diagnosis of the Security Breach/Incident will create a Security Incident report in coordination with State of Maine’s Security officer. The report shall consist of:

1. here and when did the incident occur
2. who reported it, to whom, and when
3. what information or asset was involved
4. what was the security marking and description of the information or asset involved
5. who was the originator of the information or asset
6. for how long and to whom was the information or asset vulnerable to unauthorized access
7. what actions were taken to secure the information or asset and limit the damage
8. was any information or asset lost or unaccounted for
9. what are the recommendations to prevent the incident from re-occurring

1.2.5 Implementation Requirements

1.2.5.1 Project Management

1.2.5.1.1 Project management methodology and approach

Infosys will use our multi-dimensional program management approach to drive the successful delivery and realize the full business value while providing the eProcurement solution to the State of Maine.

Based on our collective experience in assisting clients through multiple business transformations, including procurement and supply chain related transformations, Infosys has developed our proprietary IMPACT™ Framework for strategically driving value-focused transformations and operations of wide-ranging objectives.

The IMPACT™ framework is an integrated approach with multiple value streams applicable to the success of a enterprise-wide initiatives. Each value stream Play Book contains deliverables, activities, tools and techniques, including those relevant for eProcurement transformation programs. IMPACT™ will provide the State of Maine with a “game plan”, an established transformation roadmap and the framework with the necessary accelerators and enablers. Additionally, IMPACT™ takes a holistic view of key initiatives across all capabilities within a program focusing with a value-outcome based approach for distinct insights and decision-making velocity.

We will draw guidance from this framework throughout the term of our engagement and use it to provide State of Maine with a structured “game plan” for how scoping should be approached.

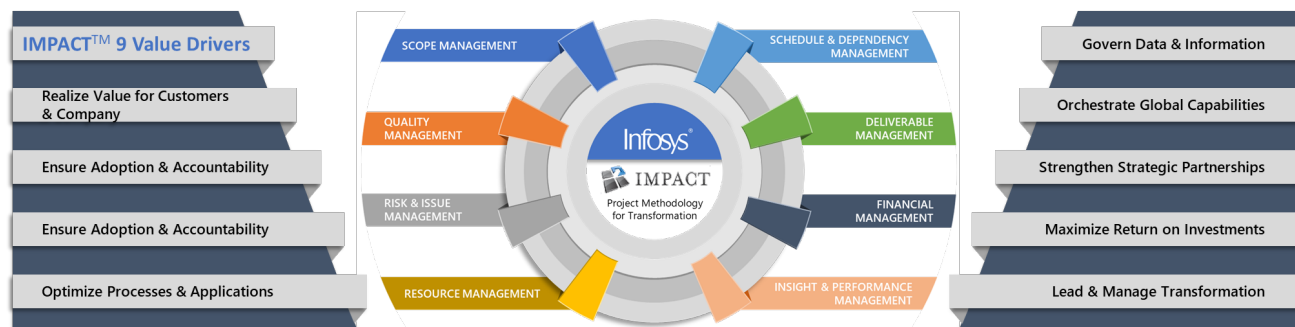


Figure 60. Infosys IMPACT™ “Lead and Manage Transformation” tools, techniques and accelerators for effective project management

Nine value drivers represent the focus areas of the State of Maine’s eProcurement transformation program. Large complex initiatives require a framework that can logically break down effort into more manageable threads, while simultaneously keeping them interconnected. Each value driver brings deliverables, activities, accelerator tools, and techniques tailored for the game plan.

Based on the scope of the RFP, we believe that seven out of nine tenants are directly relevant for the eProcurement Solutions and Services for State of Maine and participating entities as described below:

- **Realize Value for the Company:** This leverages a robust, quantitative value realization method to set direction and guide the transformation for the company.
- **Ensure Adoption and Accountability:** Get the right people, in the right place, at the right time, who knows what they need to do, are committed to doing it, can do it, and are supported by executives and held accountable for its accomplishment.
- **Optimize Processes & Applications:** Create optimized processes for the desired capabilities and design an application portfolio that supports business objectives, process objectives and enables the future enhancement and development of additional capabilities.
- **Govern and Visualize Data & Information:** Create optimized processes for the desired

capabilities. Design an application portfolio that supports process objectives and enables future capabilities.

- **Strengthen Strategic Partnerships:** Build deep, interdependent relationships with partners who provide capabilities to enhance the company strategy and maximize value across the extended enterprise.
- **Maximize Return on Assets and Technical Infrastructure:** Identify, implement and optimize the assets required to provide the desired capability, operating at required service levels and for continuous improvement.
- **Lead and Manage Transformation:** Provide the leadership, guidance, and structure to deliver the desired business capability efficiently and effectively through a global delivery model.

Specifically, regarding our project management approach, we will utilize the tools, techniques, and accelerators in the “Lead and Manage Transformation” thread to put in place an effective program management framework covering spanning across the different process areas to management the eProcurement solutions and services transformation and achieve desired business outcomes

Our project management framework complements the project implementation approach later in this response. For project implementation, we will use a hybrid agile approach leveraging our IDEA-Activate™ methodology, which is an extension of SAP’s Activate methodology. IDEA-Activate™ methodology is our proven approach for Procurement and Ariba based transformations and aligned to the IMPACT framework.

Finally, leveraging the Value for Company and Lead and Manage Transformation threads of the IMPACT™ framework and based on the criteria given in Exhibit 3 of the RFP as well as our experience with eProcurement Ariba based implementations, we have developed a t-shirt sizing approach and customized implementation plans for small, medium and large projects.

1.2.5.1.1.1 Project Management Office - Key Tasks

Infosys will work across the Five Essential Management Processes to ensure an end-to-end proactive leadership and follow-through for an “active lead from the front” approach to project management, and not only taking inputs and keeping scorecards.

Infosys targeted Program Management Office (PMO) solution for the State of Maine brings our experience in eProcurement programs in the public sector. Foundationally, we establish use our Impact Playbook to quickly establish a working PMO and addressing critical processes, standards, and governance framework to enable “lead from the front”. As Infosys and State of Maine partner to evolve the PMO, we will advance ahead with the next execution activities and start introducing monitor and control for continuous improvement. As procurement is one of the major bottom-line expenditures in any organization, we share our client’s objectives and actively use the breadth and depth of Infosys’ eProcurement experience to enable value levers for top and bottom-line advantages.

The following figure shows key tasks that the Infosys PMO carries as our core functions aligning with the major processes.

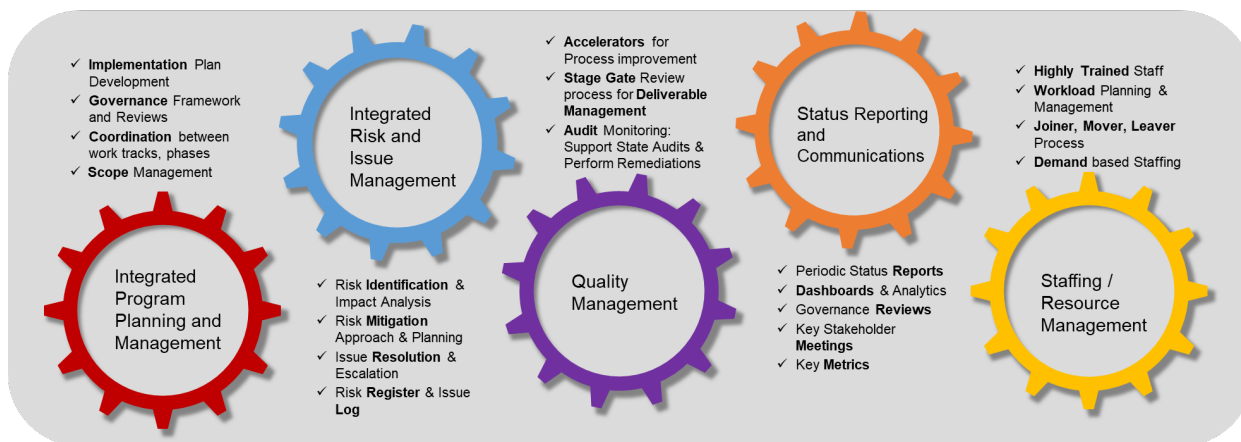


Figure 61. Project Management Key Tasks

Infosys' PMO will facilitate regular cadence with the above-mentioned work streams as part of Weekly Project Status.

For Deliverables Management Infosys will utilize the Stage Gate Review process for standardization and quality assurance for deliverables. This coupled with a Quality Management Framework leveraging our proprietary BriTe methodology ensures quality assurance and streamlined processes.

Table 34. Key Tasks across Process areas

Key Tasks across Process areas
- Integrated Implementation Plan – Infosys will develop an implementation plan based on understanding the different workstream activities, individual technical tracks plans and activities, and after requirements gathering interviews and workshops with various State of Maine stakeholders. - The Infosys PMO will work with State of Maine stakeholders to further refine and operationalize this integrated plan. Also included in the plan will be any deployment constraints, environment constraints and cross track dependencies. For more details see sub-section Deploy under Implementation Approach.
Schedule –Infosys' PMO will also develop a schedule aligned with the implantation plan, which will contain detailed work breakdown, effort, timelines, dependencies and key milestones/gates with associated deliverables and approvals required.
- Status Reporting and Communications – Infosys' PMO will facilitate regular cadence of meetings for key discussions and status updates as well as publish Weekly Project Status Reports on a regular basis (e.g. weekly, monthly, and quarterly). - The PMO will also maintain a calendar for events like status meetings, stage gate review meetings etc., stakeholder's contacts and responsibility assignments.
Risk/Issue Management -- Critical project risks that must be managed, tracked, and mitigated will be formally documented and reviewed via Risk Register. Issue will be tracked and managed via an issue log. For more details see sub-section Risk Assessment and Mitigation and Issue Management.
Deliverable Management -- For Deliverables Management Infosys will utilize the Stage Gate Review process for standardization and quality assurance for deliverables.

Key Tasks across Process areas

- Quality Management – The Infosys PMO will develop a robust Quality Management Framework leveraging our proprietary BriTe methodology to ensure quality assurance and streamlined processes.
- Staffing / Resource Management – Infosys will put in place comprehensive resource management processes to staff the right resources based on project requirements, ensure they up to speed on State of Maine specific trainings as well as manage onboarding and off boarding as part of joiner, mover, leaver process.

Strategy for Streamlining and Accelerating the Key PMO Tasks

The Infosys PMO will focus on standardizing and accelerating the project management processes by using the following levers to deliver the desired strategic outcomes for the State of Maine:

- PMO Suitcase is a collection of processes, tools & templates (Delivery Structure, Standard Processes, Tools Setup and Automation, Project Artifacts, and Standard Templates). The suitcase is based on Industry Best Practices, our collective experience with leading PMO engagements and PMI guidelines. A key lever, it establishes a working PMO, adhering to industry program management standards.
- Leading industry expertise by deploying our best-in-class resources who have successfully delivered similar projects for other clients.
- Streamlined Governance to ensure adherence to processes, ensure quality deliverables and timely outcomes. This will also include aligning with the State of Maine's approval processes.

Based on our experience of performing similar Procurement and Supply Chain projects for other government entities, an important aspect of project management is to plan and manage business user engagement. Via standardizing and accelerating key processes, the Infosys PMO will also ensure that business user engagement is closely planned and schedules are adhered so as to have minimal disruption to the business. Infosys' PMO will also closely work with the Training and OCM teams for completing user trainings and ensuring a smooth go-live.

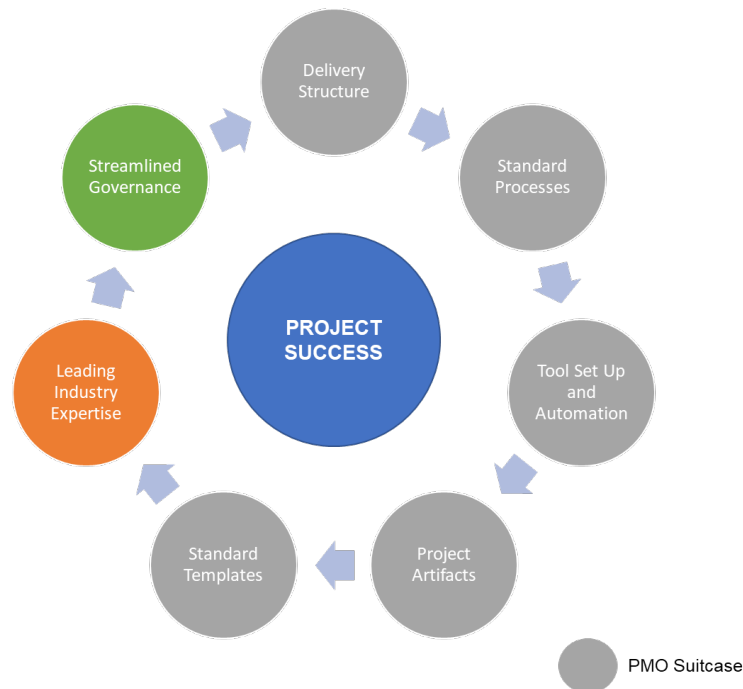


Figure 62. Illustration of Infosys Strategy

Infosys has an inventory reusable artifacts that make up the PMO. They aid accelerating the completion of process and requirements definition tasks, bring in the PPM best practices based on similar work that we have done for other clients, and enhance the quality of the pre-work that gets accomplished prior to engaging with the business stakeholders. A snapshot of a few of these accelerators are represented below:

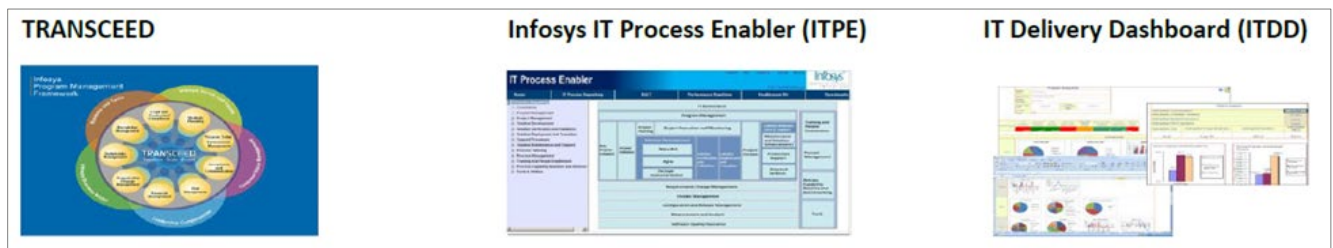


Figure 63. Example Accelerators

1.2.5.1.1.2 Implementation Plan Development

Leveraging IMPACT for the eProcurement program template and assessing the public sector's trends, patterns and ways of working with proposed schedules in the Implementation Methodology section.

- We start with an introductory session to outline and double-click into the key Infosys IMPACT program methodology.
- Next, with a solid starting point to eProcurement programs, we conduct structured planning workshop with your project managers and leads to enhancing the plan (and approach to stakeholders) for detailed 7/14/21 day action plan. This session includes critical parties ranging but not limited to: non-Ariba system business and IT owners, network, infrastructure and et al that will have input to the design, build, test and deployment of the program
- Enabling the workshop through the Playbook, we leverage "show-and-tell" for quick alignment and prevent misunderstandings.

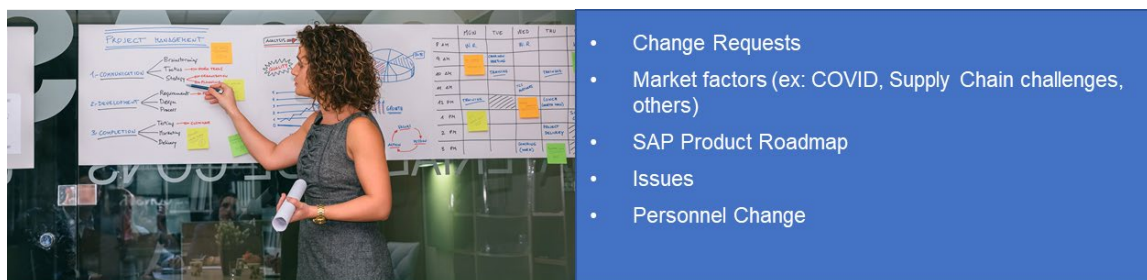
The proposed plans in this response have considered key factors but we will confirm with the State of Maine on the impact/scope of the following (but not limited to):

Table 35. Factors Impacting Scope

No	Topic	Scope/Impact
1	Municipalities, Political Subdivisions and Schools	Process design, testing, and approval sign-off
2	Commodity Groups Assigned to Buyers	Volume, historical records, others
3	Master Agreements	Volume, historical records, others
4	Program design, approvals and testing decision makers	Governance, audit evidence, activity duration, coordination
5	Multi-State Cooperative Purchasing	Scope and timing
6	Major themes for contracting in State of Maine (% figure within 10 states list) ¹ Managing mobile devices – 3% Improving construction process – 6% Monitoring climate & Weather – 6% Outsourcing Lab Testing -6% Decontaminating Gov't Facilities – 3%	State of Maine's initiatives that may intersect this program

1 10 Hotspots in State & Local Government Contracting for 2021, GovWin

With the progression of the schedule, continual refinements to the schedule will be handled through a controlled procedure.

**Figure 64. Examples that could materially affect the plan**

A Live Plan that is transparent and accessible to each stakeholder reduces status checks, follow-ups while increasing the right level of empower and responsibilities. Thus, we will work with State of Maine for the enabling project plan management tool that factors an inclusive, near real-time status that factors the right level of effort and processes for status to be dynamically up-to-date. For example, we have used SaaS program tools to bring the right data at the right time:

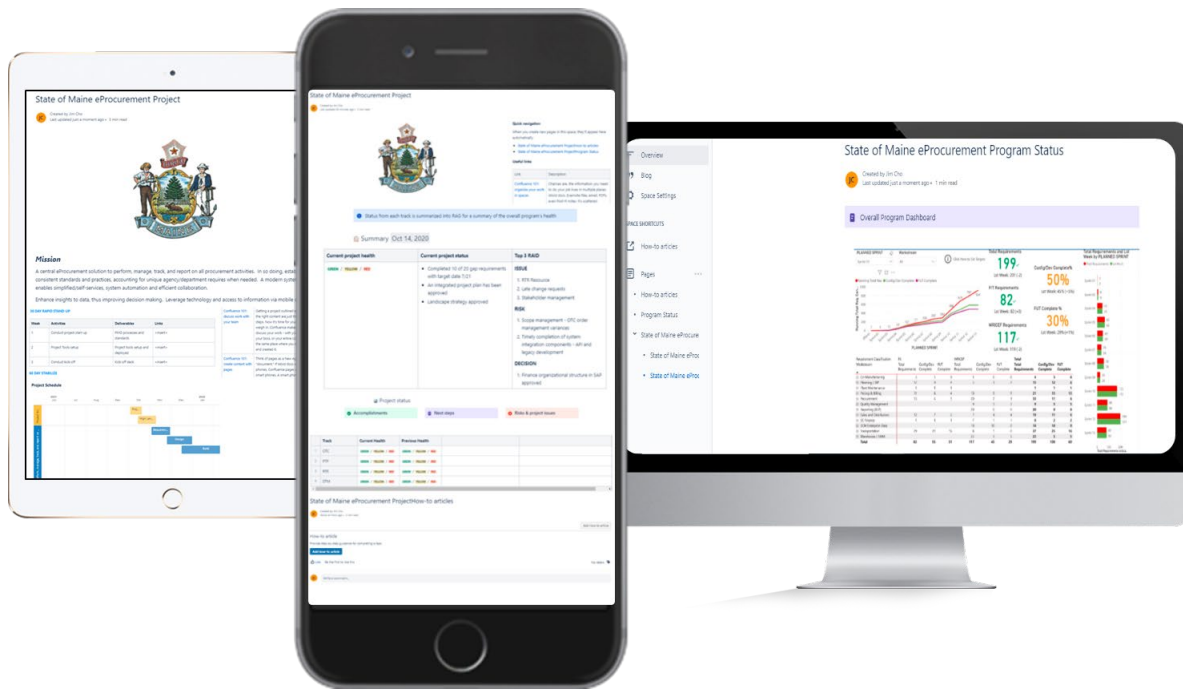


Figure 65. Mock-up of SaaS Tool

The plan is a partnership across the program and the progress closely monitored for deviations, risk and proactive management by the PMO. Proactive PMO for Infosys is a blend of our IMPACT™ framework, project managers with experience in the procurement domain that is able to understand advanced indicators that could materially impact the plan, quality and nuances that are required for a top-down and bottom-up understanding.

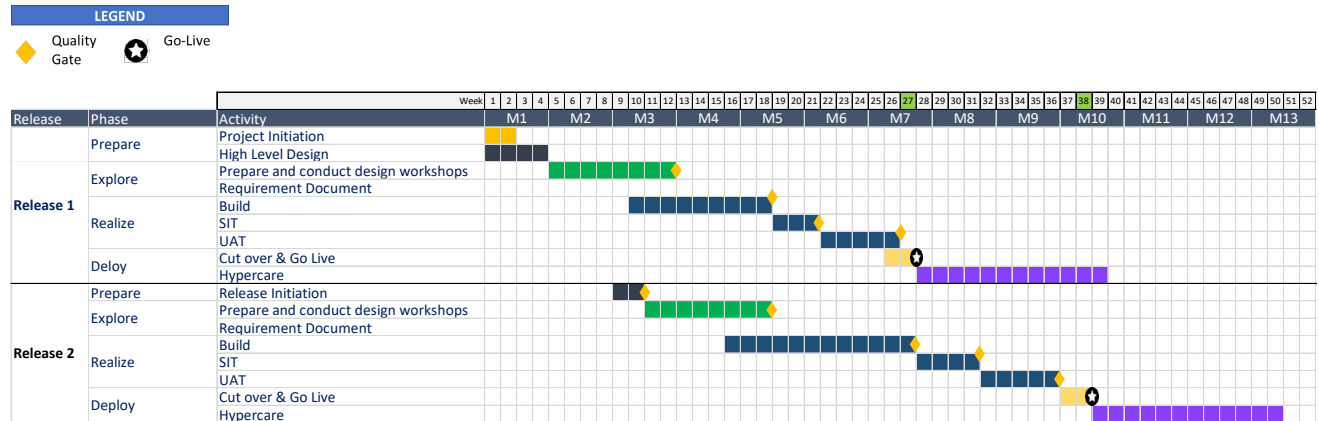
Implementation Plan Examples

Leveraging the Value for Company and Lead and Manage Transformation threads of the IMPACT™ framework and based on the criteria given in Exhibit 3 of the RFP as well as our experience with eProcurement Ariba based implementations, we have developed a t-shirt sizing approach and customized implementation plans for small, medium and large projects.

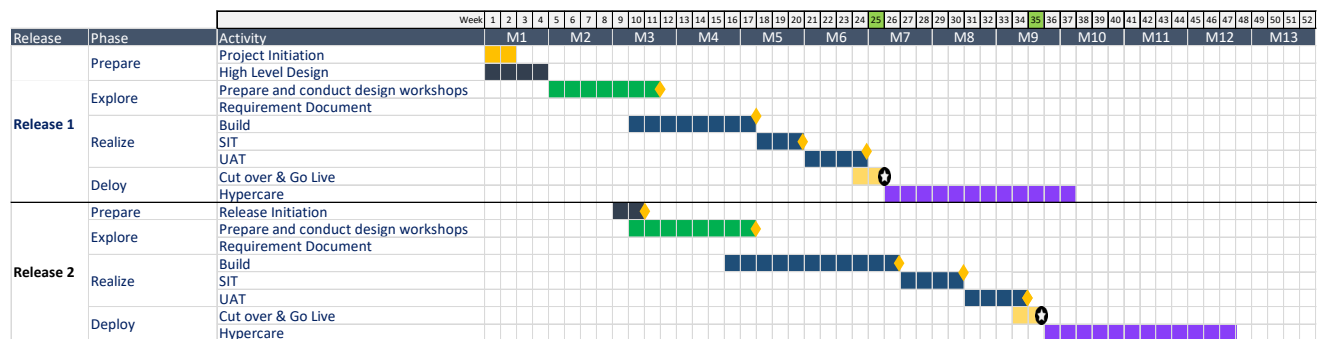
To ensure smooth transitions for the business and allow sufficient time for training, each plan has two releases. Each plan has two releases:

1. Release 1: Consists of Supplier management, Sourcing and Contract Management implementation
2. Release 2: Consists of Buying and Invoicing implementation.

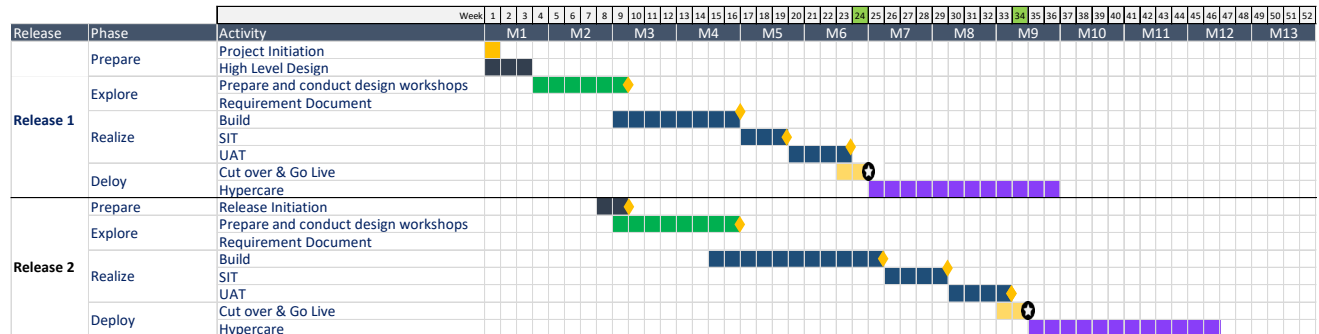
Large



Medium



Small



1.2.5.1.1.3 Organizational Chart

Delivering a successful cloud-based procurement solution requires effective and efficient organization. Our proposed project organization model and structure for the State of Maine's eProcurement Program aligns to deliver best value through synergy and a strong delivery model in all areas:

- Project management
- Leadership alignment at all levels
- Functional areas alignment for delivery
- Change management

The proposed organization model also helps leverage key success factors from previous eProcurement engagements throughout the program delivery:

- Foster a joint team-oriented for accelerated decision making

- Collaborate extensively with State of Maine resources on both project planning and execution
- “One team” to deliver an integrated business solution as outlined in the RFP
- Infosys and EY eProcurement subject matter experts to transform business processes using best practices and leveraging standard feature-function, factoring in the future product roadmap
- Emphasis on data strategy from migration to refresh frequency
- Strict quality control and stage gate process with transparent and accessible program metrics
- End-to-end solution from design, build, deploy and on-going helpdesk services
- Comprehensive change management strategy for the different levels of stakeholders
- Early focus on benefits achievement and strategies to obtain the benefits

The following diagram further illustrates the organization we envision for the State of Maine’s eProcurement Program:

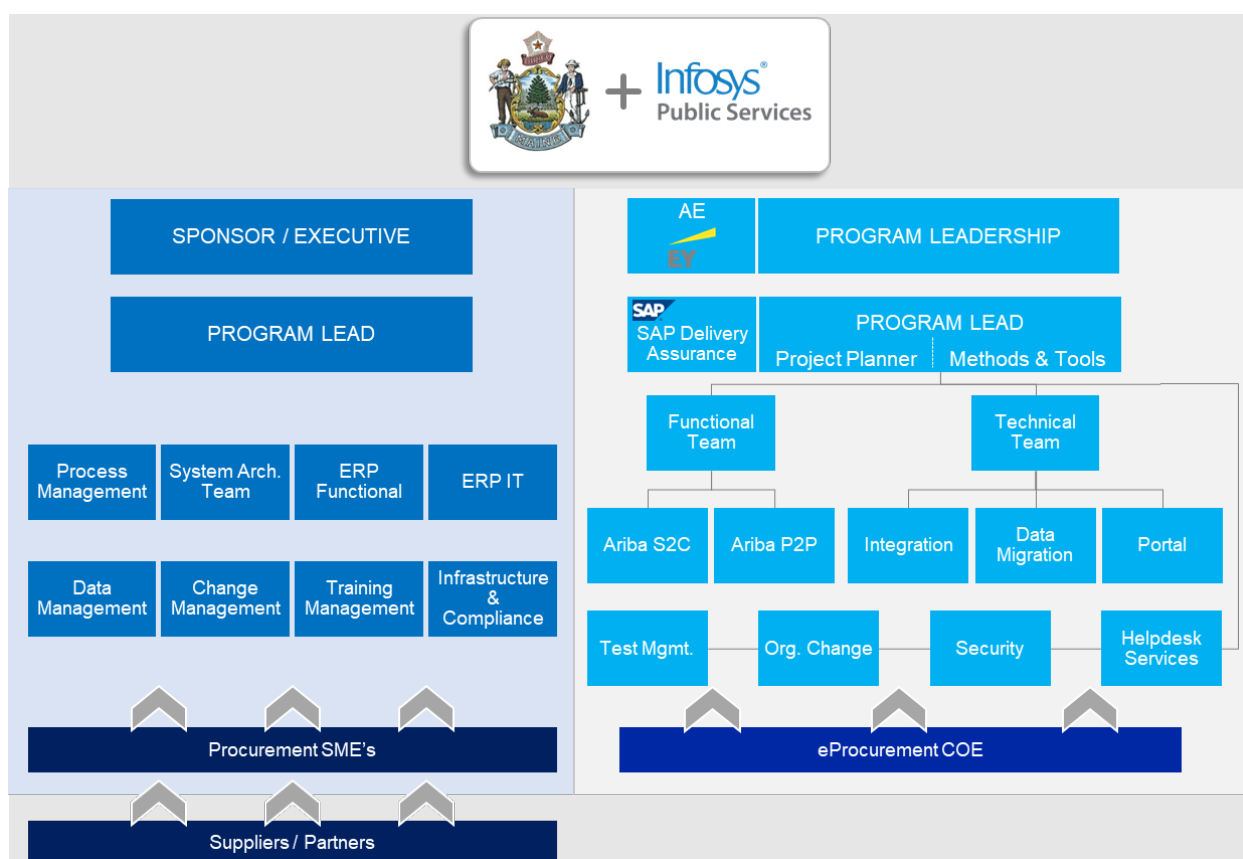


Figure 66. Proposed Organization Chart

Table 36. Proposed Organization Role Descriptions – Infosys Team

Implementation Team Roles	Description
Program Leadership	Infosys’ executive sponsor for program delivery. Responsible for advising client counterparts on industry practices, trends, value drivers from other related programs. Provides directions for the Infosys team. Escalation in the governance model for all critical issues regarding Infosys.

Implementation Team Roles	Description
EY Account Executive	Advises Infosys program leadership and program lead eProcurement leading practices, supports project delivery. Client relationship management and alignment as required.
Program Lead	Responsible for the delivery of the program for Infosys that includes scope, project plan and resources. Manage day-to-day program operations, including project status, resources, risks, and issues. Manage the Infosys team
Project Planner	Part of the PMO dedicated to planning and monitoring the project from beginning to end. Responsible for monitoring and controlling project scope, schedule, cost, RTM, and resources to make sure the project remains on track and within budget.
Program Methods & Tools	Supports project management with detailed knowledge of Ariba standard methodology. Define and configure program tools (using synergies with customer's input). Define templates for status, RAID, KDD, others. Maintain project handbook
Integration	Create technical designs, build and unit testing for complex custom interfaces. Facilitate/actively engage in joint application design workshops with point-to-point system SME's. Development of mapping, testing, and deploying code.
Portal	Work closely with business analysts to understand business and functional requirements regarding eProcurement portal, and ensure application development meets those requirements. Design, document and develop new functionality according to design and industry best practices. Integrate third-party libraries and APIs to bi-directional transfer data.
SAP Delivery Assurance	SAP Ariba Delivery Assurance provides delivery advisory and quality assurance services. A team of experts will actively participate in eProcurement program delivery throughout the program cycle to minimize delivery risks, improve delivery quality, and ensure compliance with SAP Ariba's future product roadmap. The team is composed of a Project Advisor, an Ariba Solution Architects, and several Ariba subject matter experts for various modules.
Ariba S2C	Infosys process team provides detailed functional designs for source to contract (S2C) that is used for technical engineering, defines and delivers the configuration worksheets, conducts functional unit test, user roles/personas and interfaces with State of Maine counterparts throughout the program, assists with training materials and curriculum, assists with data load when needed.

Implementation Team Roles	Description
Ariba P2P	Infosys process team provides detailed functional designs for procure to pay (P2P) that is used for technical engineering, defines and delivers the configuration worksheets, conducts functional unit test, user roles/personas and interfaces with State of Maine counterparts throughout the program, assists with training materials and curriculum, assists with data load when needed.
Data Migration	Participate in or facilitate key tasks of data migration. Defines overall data strategy. Defines rules and processes for data management. Performs load and produces post-load reports. Assists with load error outs and resolution. Facilitate knowledge transfer to other project team members.
Test Management	Infosys provides an experienced test team that is proficient in testing methodology, tools, and management of different test cycles. This team manages test plans, test scripts, and coordinates test executions.
Org. Change	Ensure project organization readiness goals and deliverables are clearly communicated to the business. Develop the stakeholder management approach, Communications Plan and End User Training Plan. Assign people to Change Team Roles and ensure they are suitably trained. Manage the execution of all organization readiness plans and activities to ensure the organization is fully prepared to implement when scheduled. Lead the determination of project team training requirements. Lead the development of a communication plan to ensure stakeholder involvement and participation. Lead the development of an end user training plan.
Training	Develop and manage project plan and strategy, including scope, schedule, resources, etc. for training and documentation. Work closely with implementation team to ensure effective and efficient integration of the documentation and training effort into the overall implementation plan. Finalize training curriculum and assist with communication to end user community. Approve and enforce training and documentation standards.
Security	Security design, development, implementation and provisioning across various environments. Provide subject matter expertise in implementation of system/role/user/process compliance controls. Provides technical expertise in implementation support. Collaborates with cross-functional team members. Manage Segregation of Duties (SoD) Remediation.
Helpdesk services	Service as first point of contact for customers seeking technical assistance. Perform remote troubleshooting. Determine the best solution based on the issue and details. Direct unresolved issues to the next level of support. Record

Implementation Team Roles	Description
	events and problems and their resolution in logs. Follow-up and update customer status and information. Responsible for defining Help Desk procedures/. Communication procedure on how issues will be reported and resolved. Set up the Help Desk infrastructure.
eProcurement COE	Infosys has an extensive internal network of experts and knowledge bases. These technology SME resources will be tapped and leveraged throughout the P2P PHASE II program to accelerate and improve quality of the delivery.

Table 37. Table 4. Proposed Organization Role Descriptions – State of Maine Team

Implementation Team Roles	Description
Sponsor/Executive	Executive sponsors of the program and responsible for providing direction and State of Maine resources. Key decision maker. Leads executive (Senior Leadership Team /Steering Committee) meetings.
Program Lead	State of Maine's project manager responsible for managing the internal project, team members and stakeholders. Working closely with Infosys project management office for planning, RAID, status, deliverable, approvals and resource onboarding point of contact. Internally for the State of Maine, the project manager will be responsible with program financials, charter, change requests and communicating across different levels of the organization.
Process Management	Process management leads represent their respective procurement processes/agencies/departments as the product owner. The team will be responsible for defining S2C and P2P functional requirements, and assisting in design, testing, training and deployment.
System Architecture Team	Provide current system landscape technical expertise that is related to the eProcurement scope. Provide current release management procedures and schedule. Assist on design and technical requirements at the enterprise landscape level.
ERP Functional	ERP Functional team will provide support for the integration between Ariba and ERP and support data cleansing, transformation/enrichment, validation, and reconciliation. Participate in design and testing cycles. The team will liaison/be responsible to provide requirement changes to the existing ERP system for this eProcurement program.
ERP IT	ERP Functional team will provide support for the integration between Ariba and ERP and assist in data migration activities. The team will liaison/be responsible to provide requirement changes to the existing ERP system for this eProcurement program.

Implementation Team Roles	Description
Data Management	Lead data extraction and transformation (ETL) activities from data cleansing, extraction and assist in transformation/enrichment of the stage data. Provide source systems for each data object such as contract, supplier, purchase order and others.
Change Management	Lead State of Maine's organizational change management, provide guidance and insight to key stakeholders and support adopt of the program. Work with Infosys on change impact assessment, stakeholder mapping, change management plan, business readiness assessment and communication plan.
Training Management	Work with Infosys on training plan, training materials, selection of super users, actively participate in TTT. Lead end user training after the 25% threshold for Infosys. Develop business onboarding plan.
Infrastructure & Compliance	Guide the implementation team on standards and compliance for implementing the new procurement solution. Work with SAP Ariba for system readiness (DEV, QA, PROD, other) and SLA's.
Procurement SME	Subject matter experts in the current procurement process and relevant technology from various State of Maine agencies and departments to provide additional support to the program (if required). Engaged and communicated as stakeholders. Program will leverage insight and persona for design, testing, and usability.
Suppliers/Partners	Suppliers and Partners as stakeholders and leverage insight and persona for design, testing, and usability.

As a unique value proposition, Infosys has leveraged our strong global partnership with SaaS product vendor SAP, and included in our service offering **SAP Ariba's Delivery Assurance** services, to minimize delivery risks, improve delivery quality, and endure compliance with SAP Ariba's future product roadmap.

Infosys has collaborated extensively with SAP Professional Services in preparation for this proposal. SAP clearly understands that the objective of the RFP is to leverage standard system functionality (best practices) while providing a stable and scalable system to increase operational effectiveness for Infosys/State of Maine. We have outlined three key reasons why SAP Services is the State of Maine's best choice to support your eProcurement deployment.

- Our proposal provides the lowest risk option for State of Maine and Participating Entities:
 - SAP's experience collaborating with Infosys and SAP's access to its product and delivery teams provides lower risk.
 - The service aims to ensure that the SAP Ariba solutions are integrated into the customer's system landscape following best practices and SAP Ariba recommendations.

- SAP Ariba provides consulting services to work with the Customer and Partner's teams to establish a detailed data configuration and integration approach based upon the customer's processes and SAP Ariba's experience & best practices.
- Intrinsically, SAP Professional Services have more in-depth knowledge of the SAP Ariba product suite and future direction, which ensure that this program will remain fit-to-standard and aligned with SAP product roadmaps.
- As the software provider, SAP Services is held to the highest standard of implementation estimate, design, and success. Including SAP Services as part of this delivery will ensure SAP as the product vendor has a stake in the success of this important procurement transformational progress for all participating entities.

1.2.5.1.1.4 Deliverable Management

Infosys follows a well-defined Deliverable Management Process to manage all deliverables created and/or delivered as part of the program.

- Deliverable Management Process:
 - Deliverable Standards
 - Review Processes
 - Baselining
 - Document Change Control to enable impact analysis and revision of associated Deliverables
 - Backups and Restoration.
- PMO:
 - Facilitate completion of Milestone Deliverables by all parties, with associated Templates and Tools.
 - Leverage State of Maine guidelines where applicable to define Approval Processes and Guidelines, Acceptance Criteria, Entry- and Exit- Criteria for each Project Gate.
 - Deliverable Management Guidelines including Project Repository, Version Control Mechanism, and Owners (RACI) will be identified.
 - Ensure adherence to established guidelines during all phases.
 - Establish Quality Review Processes for Key Deliverables.
 - Establish an overall Governance plan with associated Processes, including detailed RACI across Delivery Partners, Vendors, Business and IT Teams

Stage gate Process

- To ensure Deliverable quality, Infosys will leverage the Stage Gate Process for a structured review and approval of major activities and deliverables required for successful completion of each phase.
- By standardizing deliverables and checkpoints, the Stage Gate Review process ensures proven and consistent project management methods are applied to account for variations in scope, schedule, resources, location, etc.
 - Example: All projects are required by the standard Blueprint Phase Stage Gate to have RICEF Functional Specifications complete. The difference between projects is the number (e.g. scale) of how many specifications there will be for SIT1/2 based on priority, which in turn is based on the scope of that individual project.

- The Stage Gate Review process acts to mitigate potential implementation issues and risks. Stage Gate Reviews are scheduled at pre-defined times such that the status of the project and adherence to timelines can be addressed promptly.

Illustrative purposes only

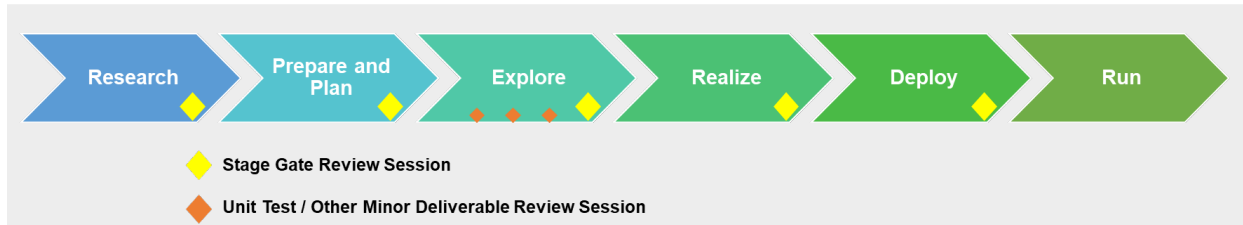


Figure 67. Stage Gate Process

Phase Gate Criteria Examples – Illustrative Purposes Only

Work Package or Phase	Deliverable or Outcome	Required Skills	Acceptance Criteria
Scoping Phase	Documented architectural diagrams that support configuration of products	Familiar with Ariba, Hybris ecommerce, and Procurement expertise	Supplier has delivered architecture diagrams (logical and physical) for Procurement software which shall include integration with existing systems: - ERP systems - CRM systems - Hybris ecommerce (if recommended) - workflow management systems - product catalog(s) - pricing tables

Figure 68. Phase Gate Criteria Examples

1.2.5.1.1.5 Status Reporting

The Infosys PMO will facilitate a regular cadence with the various work streams as part of Weekly Project Status and provide consolidated status reports for the consumption of the program leadership and other stakeholders. Examples: Weekly, monthly, quarterly reports

Status reporting in general will include:

- Status by Scope Items
- Updated on risk register and risk management strategies
- Latest Project Schedule and Schedule Status
- Red/Yellow/Green Status for Schedule, Quality, and Cost

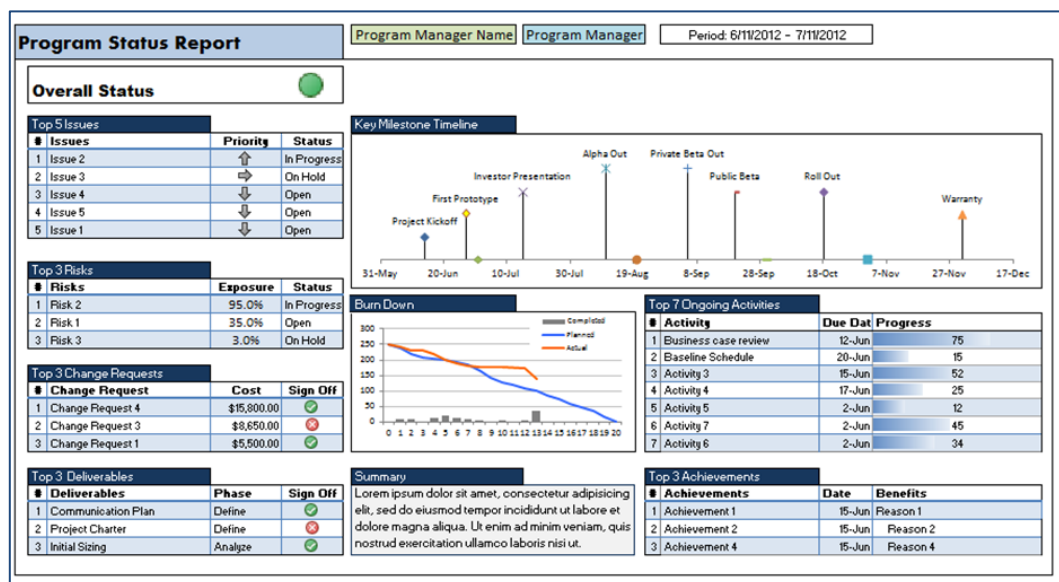


Figure 69. Example Status Report

Report type examples

The table below shows the type of details that will be included for some example reports:

Table 38. Example reports details – Illustrative purposes only

Report Type	Report to include
Production Release Status Report	- Project Status - Project Description - Project Benefits - Key Updates, Critical Issues, Risks and Mitigations - Requirements Status (depends on the Release and timing) - Red/Yellow/Green Status for Schedule, Quality, and Cost (Resource Utilization/Availability) - Status by Scope Items (content depends on the Production Release) - Milestone Summary - Open Issues - Initial Resource Estimates (Hours) by Resource Type and Actuals expended so far - Testing Status (Defect and Fix Status) in alignment with FNS Test Plan requirements
Weekly Status Report	- status of system activities, including all performance standards - status of defects found or worked on during the report period - Helpdesk incidents logged or worked on during the report period

Security Status Report	Security status for all solution components, with updates on assessments, defect fixes, security testing, and mitigation activities for all scope
Ad Hoc Reports	Ad hoc status reports at the request of the State of Maine

Infosys has also implemented status reporting solutions based on modern visualization platforms like Microsoft's Power BI, Spotfire. Such options will be discussed with the State of Maine stakeholders and the approach will be decided based on inputs from the State of Maine.

The following image shows the example data sources that will be considered while generating periodic status updates and management reports.

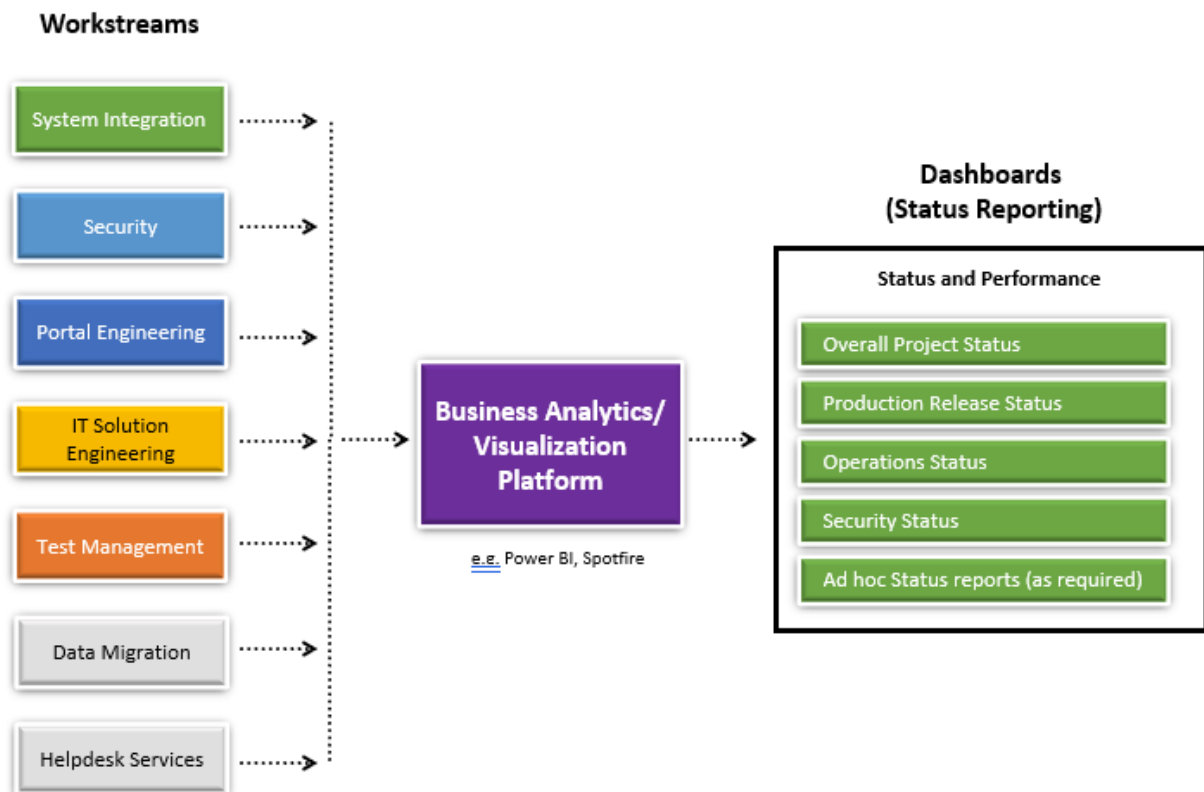


Figure 70. Status reporting Using Business Intelligence

1.2.5.1.1.6 Risk Assessment and Mitigation and Issue Management

Risk Management

Critical project risks that must be managed, tracked, and mitigated will be formally documented and reviewed via the Risk Register. Each risk identified will be assessed in terms of our IDEA-Activate™ implementation methodology for the impact it could potentially have on the success of the project and appropriate mitigation strategy identified

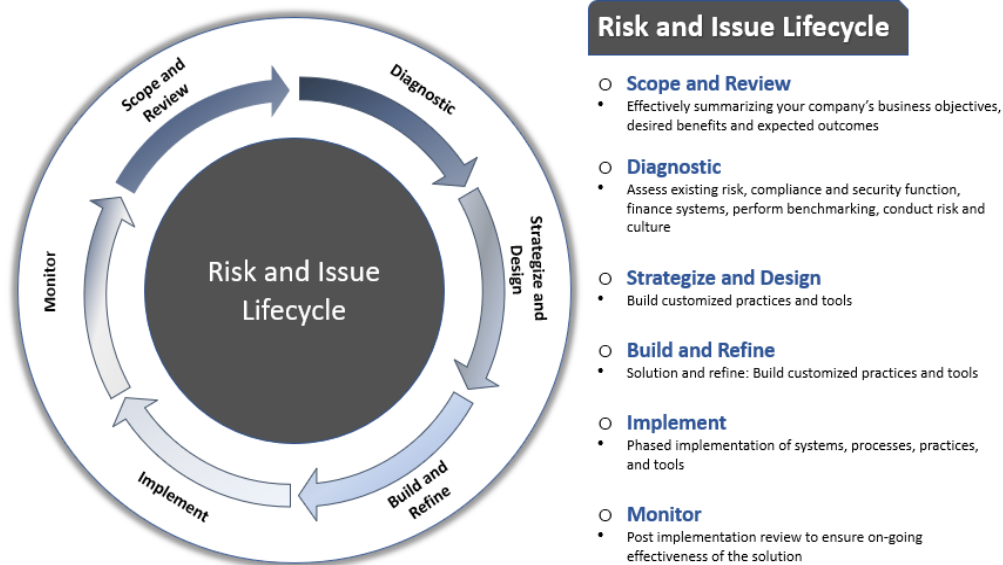


Figure 71. Risk and Issue Lifecycle

Infosys PMO activities related to risk will include but is not limited to as follows:

- Define program-level risk management plan, including risk/issue impact levels, risk probability levels, Risk Matrix (e.g. 4x4 matrix)
- Define guidelines and process to mark items from Issue Log and Risk Register for escalation to governance board (e.g. Manual or automatic flagging of risks for escalation to the governance board based on risk rating)
- Conduct periodic issues/risk review meetings
- Develop Risks and Issues Dashboard
- Identify continuous improvement opportunities (e.g., automated notification for risks, mobility)
- Infosys PMO will review and seek approval for the overall program-level risk management plan.
- Infosys can provide unique accelerators in Risk dashboard designs and automation of processes related to risks (e.g., system notifications for risks nearing target closure date)

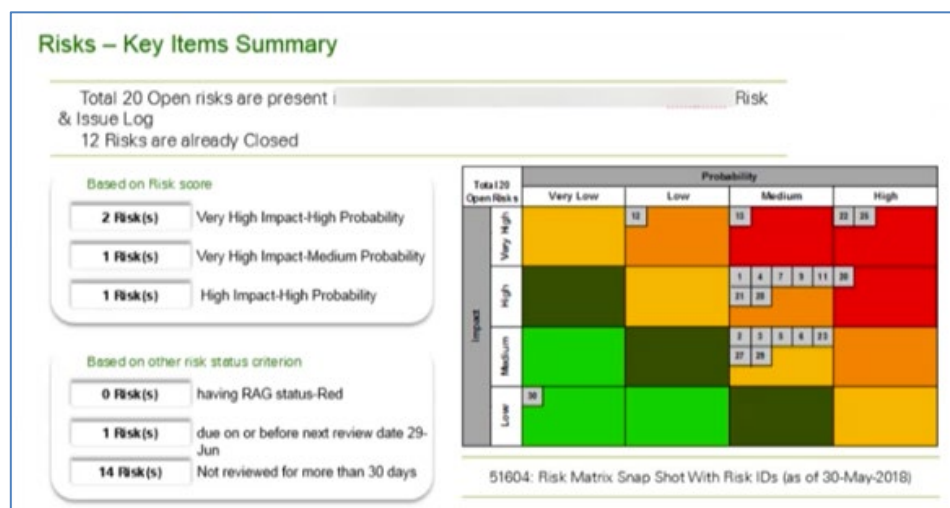


Figure 72. Example Risk and Issues Dashboard

Based upon our extensive Ariba implementation experience with clients such as, AstraZeneca, Novartis, United Health, and Freddie Mac (Fieldglass), we have identified several critical risks that have surfaced throughout these implementation programs:

Table 39. Major risk areas for eProcurement Solutions implementation

Major risk areas for eProcurement Solutions implementation	
	• Program management – includes risks related to project schedule, resourcing, scope, benefits management, and cost management
	• Business readiness – includes risks related to buy-in for the solution, sufficient and adequate training, communication effectiveness
	• Technology readiness – includes risks related to the solution build, cloud/SaaS technology, security, and master data (migration of legacy data, management of data quality, etc.)
	• Operations – risks related to ongoing service delivery after EPS go-live (applicable to each major release)

A core part of our solution is how we address these risks through our eProcurement approach, reflected in our implementation plan, and the value-added services we have included to further mitigate risk. As referenced below, our solution includes addressing key risks related to program, business readiness, technology readiness, and operations.

Issue Management

Issues are the incarnation of risks. It is important that these issues are identified and resolved quickly by the appropriate person. The first step in effectively dealing with these issues is to make the entire team aware of the importance of identifying issues and achieving prompt and proper resolution. We will use the following procedure to track the identified issues:

- Identify issues. Beginning at project prep, the team will start identifying any issues that could affect our ability to meet the objectives of the project. Issues can be identified by anyone involved with the project.
- Document the issue.
- Assign responsibility for resolving issues. The responsible person must be an individual who has the knowledge and authority to make decisions regarding the issue. The team will also assign a priority to the issue.
- Monitor and control progress. All issues will be tracked on an issues log that will be maintained to formally track the status and resolution of the issues.
- Report progress on issue resolution. The issues log will be a part of the weekly status report and discussed in the weekly status meeting.
- Communicate issue resolution. The issues log and documented resolutions of issues will be made available to all team members.

If an issue cannot be resolved in a reasonable period to the mutual satisfaction of Infosys and the State of Maine, we will use the escalation process to escalate it to the appropriate level of management.

1.2.5.1.1.7 Staff / Resource management

Infosys has a large pool of talented and certified program management and technical resources from which it will draw resources. Infosys will develop a staffing plan based on the requirements and implementation plan to onboard and manage resources.

For any changes in demand during to scope changes, Infosys will employ a Core and Flex model with a “core” team staffed as per plan while leveraging a “flex” team to respond to variable demand.

As part of Staff management, Infosys will also implement Onboarding and Off boarding processes including activities such as orientation and any State of Maine specific trainings needed.

The onboarding and off boarding process for program management and technical resources is outlined below:

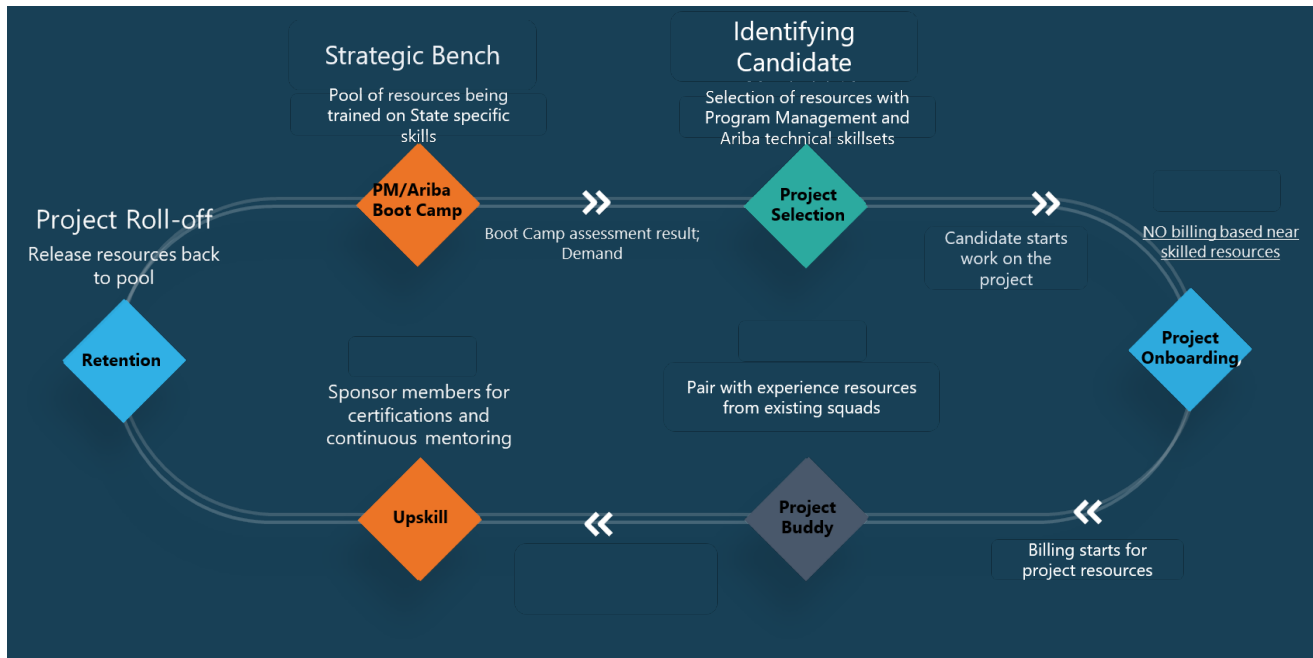


Figure 73. Onboarding and Offboarding Process

1. Prior to onboarding, candidates will spend time on our strategic bench where they will undergo any needed Ariba training as well as any State of Maine required training and orientation activities.
2. A candidate will become available for project selection once all training requirements are complete.
3. Once selected, resources will spend some time familiarizing themselves with the project prior to project onboarding.
4. Next, the resources join the project and billing will start.
5. Once on-boarded, a resource is paired with a “Project Buddy” who will help the new joiner up the learning curve.
6. Infosys will support team members by sponsoring any needed certifications and provide continual mentoring.
7. Whenever “flex” resources are rolled off due to decreasing demand, they will return to the strategic bench.

1.2.5.1.1.8 Quality Management: Framework and Accelerators

Infosys follows a robust process architecture that defines and describes the major process groupings required to provide repeatable and reliable services to our clients and to manage our business. This architecture is based on Infosys’ decades of experience as an IT organization, and it is aligned to a

number of best practice methodologies such as the Capability Maturity Model Integrated (CMMI), ITIL, Six Sigma, ISO 9001 and Project Management Institute (PMI).

We leverage our proprietary BriTe methodology based on Six Sigma and Lean Principles which focuses on process improvement and variation reduction, and i-Trim methodology which focuses on eliminating non-value-added activities and increase process throughput to deliver sustained value. The picture below depicts the Infosys BriTe methodology.

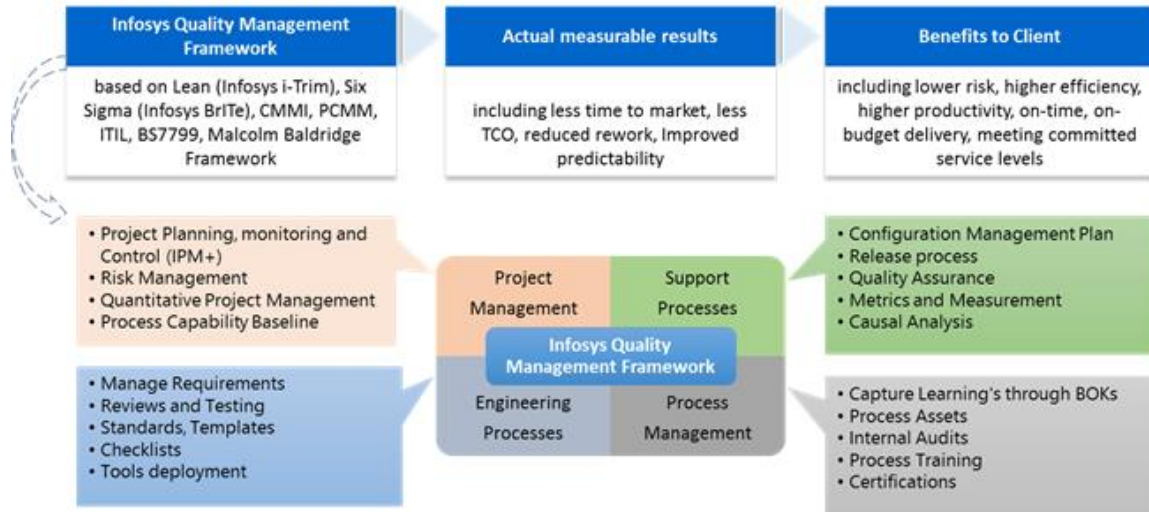


Figure 74. Infosys Quality Management Framework

1.2.5.1.1.9 Program Audit & Monitoring Support

Audits play a key role in ensuring that the program comply with related standards, policies, procedures, KPIs etc. defined internally by the program, State of Maine, or outside agencies.

Considering the importance of audits and ensuring that every program-related audit is a success, the Infosys Program Management Office adapts a comprehensive approach weaving audits and related activities in the overall program schedule. This approach helps mitigate risks related to audit gaps and increase audit success rate.

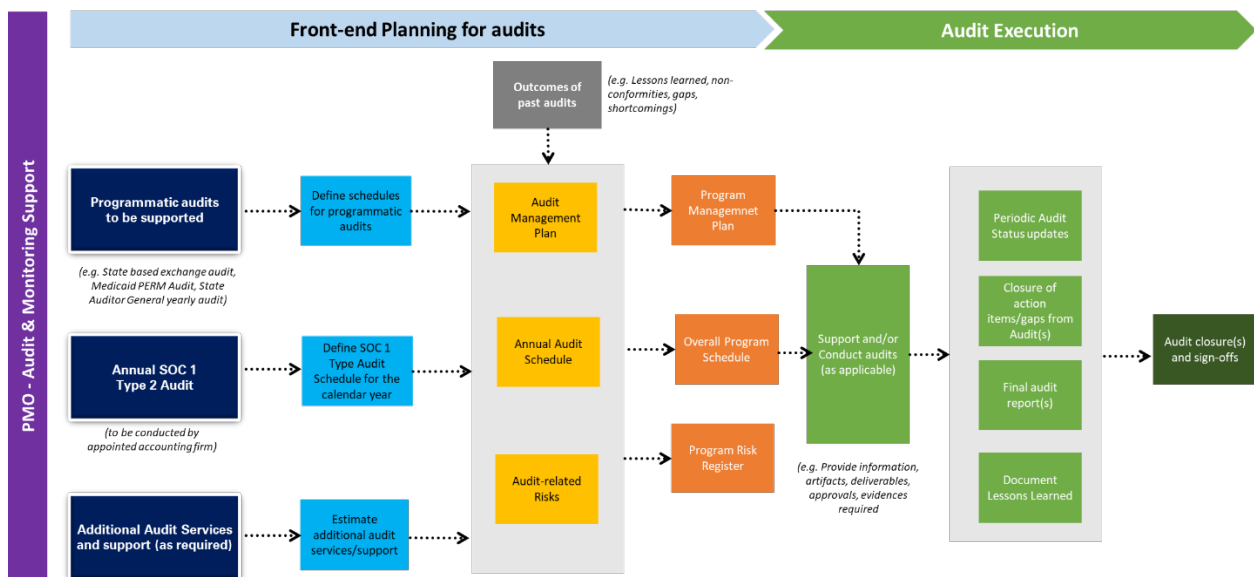


Figure 75. Example of Audit Process

1.2.5.1.2 Project Manager and Project Management Qualifications

We bring the highest level of executive commitment to this engagement along with our A-team with a proven record of accomplishments for delivering complex programs.

Infosys has a large pool of people dedicated to PMO support projects who are highly trained and continually updating their skills and certifications. At Infosys, training and certification is mandatory for all our employees, aligned with their role & subject matter expertise. Infosys has a repository of 500+ certifications for IT professionals ranging from Domain, Technical, and Process, Behavioral and Project Management skills. Infosys has a centralized and dedicated area-wise Center of Excellence (CoE) which enables development of high performing teams in the areas of Project and Program Management as well as Agile Delivery.

Infosys Project / Program managers are trained on:

- “Infosys Project Management Certification (PM Elite)” – This certification has 3 Levels PM Elite Lite, PM Elite & PM Elite Advanced for Jr. PMs, PMs and Sr. PMs respectively.
- “TRANSCEED (Transform-Scale-Exceed)” - Comprehensive, patented program management framework aimed at successfully managing large business transformation programs.
- “Infosys Global Agile Certification” – This certification and associated internal trainings accelerate build-up of differentiation in Infosys Agile execution capabilities.

- **2,200+** PMP certified
- **400+** Prince2 certified
- **10,000+** PM Elite
- **4000+** Agile certified (CSM, CSPO, PSM, PMI-ACP)
- **25+** SAFe Program Consultants

We also encourage PMs to get certified by several external entities like PMI and PRINCE2. Infosys is a Registered Education Provider and a Global Executive Council member at PMI.

Additionally, Infosys Project managers are supported by continuous learning through the Infosys PMCoE (Project Management Center of Excellence) trainings, workshops, seminars, and discussion forums to keep them up to speed on latest project and program management practices.

For this RFP, we have formed a PMO with practitioners that have PMP, Prince and/or Six Sigma certification(s). Additionally, the PMO compliment their core leadership competencies with business/functional/technical experience in procurement processes. This give our PMO a unique approach to leadership through a contextual understanding of the challenges, industry trends, best practices that translates to a proactive program leadership.

1.2.5.1.3 Project Deliverables

The following table shows key project deliverables that the teams will create for an eProcurement implementation. Note that this is for illustration purposes only. Actual deliverables will be decided after requirements gathering in the planning phase of the project.

Table 40. Project Deliverables

Phase	Deliverable	Description
Prepare	Kick-off Deck	Presentation introducing project objective, scope, organization, guiding principles and overall timeline
Prepare	Governance Model & Procedures	A document describing which types of decisions and changes that are approved at which levels in the organizations.
Prepare	Detailed Project Plan	Integrated project plan with key milestones and dependent activities

Phase	Deliverable	Description
Prepare	Resource Plan	Identified project resources, allocations, forecast and on/off boarding process
Prepare	Communication Plan	Document describing the types and frequency of communications to project, stakeholder, and external audiences.
Prepare	End User Training Strategy	Document describing the types of training delivery models, the tools and approach for training material development, how training scheduling and delivery will, and effectiveness of delivered training will be determined.
Prepare	Risk Mitigation Plan	Definition, process and execution of risk mitigation actions
Prepare	Development Standards	Document describing how the workflow and documentation for functional requirements, technical specifications, coding reviews, and unit testing will work.
Prepare	Infrastructure and Landscape Strategy	Definition and purpose for each landscape type, system integrations, size, SLA and others
Prepare	Testing Strategy	A document describing the risk-based approach to unit, end-to-end, and performance testing.
Prepare	Data Migration Strategy	Document covering data extraction, mapping, transformation, and upload approach.
Prepare	Explore Phase Kick-Off Presentation Materials	Presentation describing project scope, organization, guiding principles, timeline, as well as key approaches to delivering the explore phase.
Explore	Business Process Design User Stories	Detailed documentation of business process and system requirements
Explore	Key Decision Documents	Formal and final disposition of highly impactful decisions for the project that could lead to standard, guideline and/or scope
Explore	Target System Architecture Landscape Diagram	Diagram showing key information flowing in and out of interfacing systems.
Explore	Requirements Traceability Matrix	Documentation of all requirements including business, technical, security, etc. It also includes fit/gap analysis as well as solution overview.
Explore	Functional Specification Documents	Documentation of functional solution for enhancements or integrations to fill application solution gaps to enable relevant business process
Explore	Configuration Workbook	System configuration details of eProcurement solution to enable relevant business capabilities
Explore	User Security Strategy	Document describing how composite and derived roles will be determined, designed, tested, and managed including segregation of duty checks.
Explore	End User Role Definition	Selection of standard roles relevant to in-scope standard processes.
Explore	Change Impact Action Plan	Specific actions to be performed by change agents, process owners, or site representatives to explain how work will change from the current state.

Phase	Deliverable	Description
Explore	End-to-End Test Cases	End-to-end of a process flow that may include system interfaces, reports, forms, others
Explore	Explore Stage Gate Result	Stage gate review and acceptance to move to the next phase
Realize	Technical Specification Documents	Documentation of technical solution for enhancements or integrations to fill application solution gaps to enable relevant business process
Realize	Technical Requirements User Story	Document that is developed for required system development that is traceable from the functional requirement document
Realize	Configured and Developed eProcurement Solution	Configured and developed eProcurement system (development, test and/or training environment) that meets requirements and design specifications
Realize	Unit Test Script Feature and Results	Testing the behavior of a unit of eProcurement solution component
Realize	System Integration Test Plan	Detailed plan for system integration test sequences, dependencies, test data and user roles
Realize	Updated Requirements Traceability (System Objects, Tests)	To facilitate test set creation, assign system objects, both configuration and development, to user stories. Also allocate security roles to user stories.
Realize	Data Migration Mock Report	Data ETL report with volume, load error, validation & reconciliation metrics
Realize	Training Materials	Create training materials using chosen training material authoring tool using representative organizational and master data.
Realize	Cutover Plan	Plan containing all technical, data, and business activities to be performed during the cutover process.
Realize	Transition Plan	Plan containing activities to be performed to enable changes to business and IT roles.
Realize	User Acceptance Plan	A subset of the end-to-end tests that are business critical will be selected and executed by key users.
Realize	Technical Readiness Assessment	Component of go/no-go decision covering readiness of technical infrastructure, interfacing systems, security, and other technology needed to perform work.
Realize	Business Readiness Assessment	Component of go/no-go decision covering readiness of training materials, business partners, contingency plans, and any local procedure updates.
Realize	Train-the-Trainer Plan	Walk through of training materials, hands on transactions, and training messages with key users chosen as trainers.
Realize	End User Training Plan	Matrix showing which role-based courses will be offered during the designated weeks prior to go-live.
Realize	User Acceptance Test Completion Report	UAT completion report confirming the acceptance of the solution/system
Realize	Realize Stage Gate Result	Stage gate review and acceptance to move to the next phase

Phase	Deliverable	Description
Deploy	Go-Live Readiness Check	Assessment document owned by the project sponsors and site leadership covering business partner, user, and system readiness components.
Deploy	Go/No-Go Decision	Documentation of the formal go-live decision
Deploy	End User Readiness Check	Site and project leadership use training retrospective and user role set up information as well as results of change impact actions to assess readiness of users for go-live.
Deploy	Communication to Business Partners	Regular notices provided to customers and vendors about what is occurring, how it may affect them, and whom they should contact in the event of issues.
Deploy	Process / Functional Solution Handover	Knowledge transfer tracking mechanism in place.
Deploy	Technical Solution Handover	Handover of configuration, development, and other technical knowledge to the support organization after relevant part of the system is stable.
Deploy	Lessons Learned Assessment	Retrospective for continuous improvement
Deploy	Project Closure Report	Comprehensive report describing current state of project and how any remaining items will be handled.

1.2.5.1.4 Bidder's (Infosys) and Participating entity staffing plans including key positions, roles and responsibilities

The following diagram depicts the planned structure for the Infosys PMO team and Staff roles on Participating Entity side that will interact with the PMO team for project governance and execution

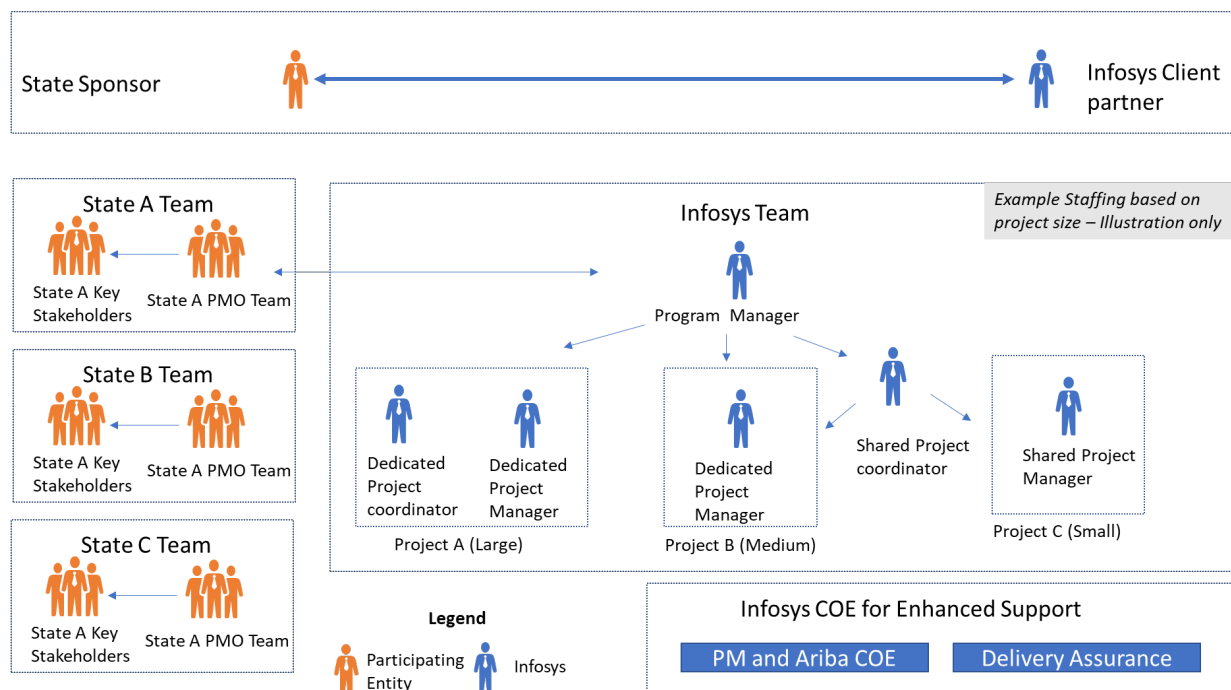


Figure 76. Planned structure for the Infosys PMO team and Staff roles for Participating Entity

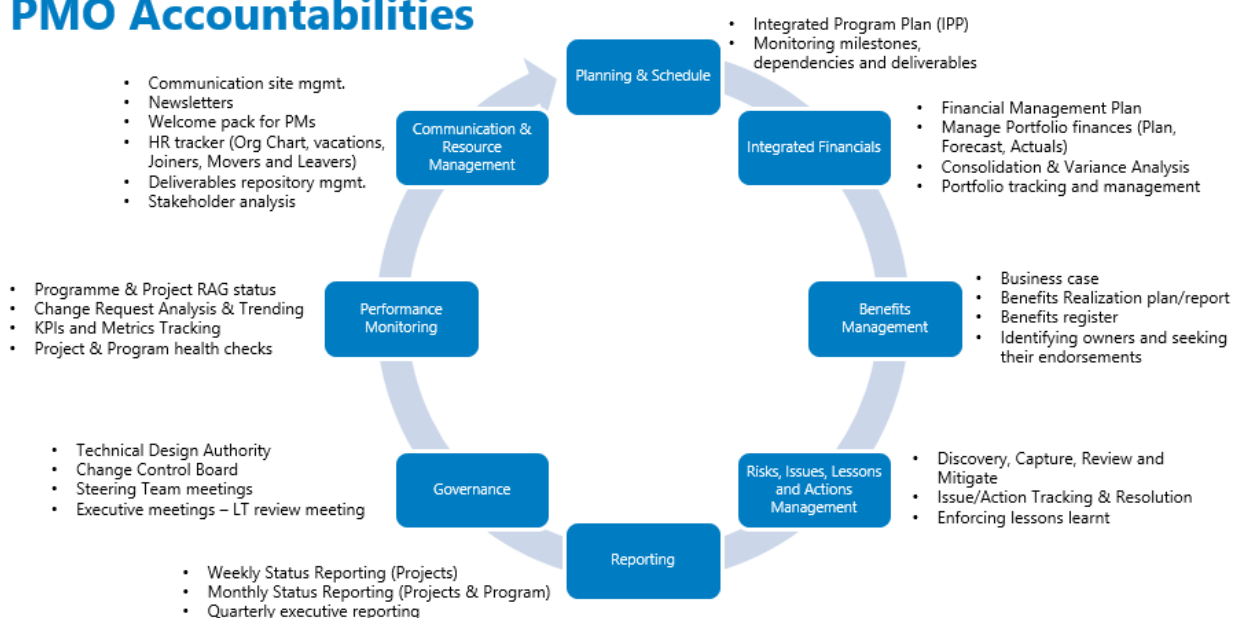
PMO Roles and Responsibilities

Table 41. PMO Roles based relevant PMO Accountabilities

Role	L0 responsibilities	Hi-Level Responsibilities
Program Manager	PMO Office Lead	• Manage PMO Office • Material generation for key meetings (Steering, PLT, status, etc.) • Run key program meetings • Oversee continuous improvement initiatives (PMO/Performance Mgmt. process definition, dashboard creation)
Project Planner	• Program Schedule & Integrated Plan • Change Control (Program)	• Manage Program Schedule/Integrated Plan and dependencies • Manage program status reporting - weekly status report, monthly status report review/compliance • Manage Change Control process
Project Methods & Tools	• Tools and standard operating procedures	• Manage program tools and standards (naming, file types, et al) • Aligns and integrates various SDLC, documentation systems, information, status and et al

Delivery Structure

Deciding the Delivery Structure is the first step for any PMO; therefore we leverage our PMO Suitcase, which has clear guidelines and processes on how to engage with a project and support it throughout its lifecycle.

PMO Accountabilities**Figure 77. Sample PMO Accountabilities**

Roles, Responsibilities and Skills

Table 42. Roles and Responsibilities and Skills

Role	Responsibility	Skills
Project Leadership	• Maintains the final authority to set priorities, approve scope • Secures necessary solution/resource to ensure timely delivery of the project • Participate in periodic Steering Committee, Quality Review of Project Progress and Deliverables	• An executive-level presence within the company • A vision of the organization's goals • A belief that SAP is the solution for the organization • An active relationship with SAP management • The ability to make critical decisions under critical time pressures • Strong leadership skills and effective negotiation skills • A proven record of being proactively involved with organizational issues • The ability to maintain excellent communication skills, including the ability to listen
Project Lead	• Reports to the Program Executive and Steering Committee for the operational success of the project • Secure/manage project resources • Responsible for the completeness of project deliverables • Participate in the development of a Detailed Project Plan • Participate in the development of Project Controls including Scope Control, Issue Resolution, Documentation Strategy, Status Reporting, Quality Standards and Review • Execute project controls • Participate in Steering Committee meetings • Monitor and control project budget	• Understanding of the strategic importance of information systems for the program's success • Experience with similar procurement implementation • Leadership, project and team management, methodologies, negotiations, and communication • The ability to work effectively with all levels of management, providing detailed guidance to project team members • A big picture view of the project's goals, while performing detailed analysis tasks. This includes controlling scope. • Time management skills and multi-tasking capabilities

Role	Responsibility	Skills
	• Manages tactical activities of project team • Fosters team development	• Superior presentation, oral, and written communication skills • Proven negotiation skills • The ability and authority to make timely decisions • Strong organizational and motivational skills • Advanced application software skills, including presentation, spreadsheet, word processing, and project management applications • Basic IT understanding
Program Planner	• Defining and establishing performance measures & monitoring implementation status • Coordinating the budget process; control and report on program costs and deviations from budget/plans • Defining the implementation approach/methodology, program management tools and standards for the program • Maintaining the master repository of key program documentation regarding quality audits, global procedures, processes and standards, key learning's from programs, costs, SAP source code changes, etc. • Assisting in the development and maintenance detailed work schedules • Owner of the change control process for program deliverables	• Program management support experience • Strong analytical skills and team player qualities • Strong time management skills and multi-tasking capabilities • Excellent communication and inter-personal skills • Ability to work independently • Experience in scheduling and agenda planning • Willingness to perform detailed, repetitive tasks • Advanced application software skills including but not limited to presentation, spreadsheet, word processing, and program management applications.

Role	Responsibility	Skills
Program Methods and Tools	• Supports project management with detailed knowledge of Ariba standard methodology • Define and configure program tools (using synergies with customer's input) • Define templates for status, RAID, KDD, others • Maintain project handbook	• Program management support experience • Strong time management skills and multi-tasking capabilities • Excellent communication and inter-personal skills • Ability to work independently • Good contacts within the organization
Solution Architect	• Lead the analysis and design of specific, critical, complex processes and solutions • Provide inputs for high-level process scope • Responsible with the Data lead for the establishment of new data standards • Works with appropriate business users to understand process requirements • Defines and manages process team work plan • Provides project deliverables are on time and of high quality • Communicate changes to business process • Manage team resources and identify subject matter/part time resources • Manage appropriate integration of business design across functional teams • Assess day-to-day potential project risks • Manage team issue resolution and escalate when appropriate • Report to project management on status of team efforts and accomplishment of project milestones and Deliverables	• Expertise and experience business process design and execution • Methodology knowledge, with implementation experience • Facilitation skills • Interpretation skills

Role	Responsibility	Skills
S2C and P2P Team Member	- Document detail design business processes for S2C or P2P - Execute project tasks for applicable functional area - Construct work products according to project and work plans - Provide process knowledge as appropriate - Develop / update Process Design Definitions, Process Workflow, Business Process Procedures (App.'s) and functional specifications for development objects - Perform GAP Analysis of required business processes - Assist team lead in the identification of project risks and development of risk mitigation steps - Identify, document and resolve issues	- Expertise and experience business process design and execution - SAP Activate Methodology knowledge - Facilitation skills - Interpretation skills - Excellent communication skills - Experience in S2C and/or P2P for Ariba implementation - Experience working with SAP field service
IT solution Engineering	- Ensure the technical requirements for the system are met - Ensure the necessary technical skills are available to the project - Ensure the technical design is appropriate and that the design will support future system upgrades - Lead the analysis and design of specific, critical, complex technology solutions - Lead the design of technology components of the solution - Develop high-level technical scope development - Prepare and facilitate technical workshops	- Keen sense to differentiate which issues are crucial to the project and which are not - A strong technical implementation background with either package or custom application systems - The ability to work effectively with all levels of management, with proven ability to assign, schedule, and guide project team personnel - Strong time management skills and multi-tasking capabilities - Excellent communication and inter-personal skills - Active member of the implementation team

Role	Responsibility	Skills
	• Detail technical scope development (e.g.: interfaces, reports, conversions) • Responsible for resolving technology issues • Manage technical team resources and identify subject matter/part time resources • Assess day-to-day potential technical project risks • Manage issue resolution • Report to project management on status of technical team efforts and accomplishment of project milestones and Deliverables	• Advanced application software skills, including presentation, spreadsheet, word processing, and project management applications are desirable • Experience in implementing and supporting the SAP or other ERP suites
System Integration	• Create technical designs, build and unit testing for complex custom interfaces. • Facilitate/actively engage in joint application design workshops with point-to-point system SME's. • Development of mapping, testing, and deploying code.	• Strong hands-on developer of Oracle PaaS products OIC-integrations • Excellent understanding of Oracle PaaS4SaaS extension patterns and Oracle Cloud Infrastructure (OCI) and PaaS4SaaS architecture • Technical problem-solving skills • Good communications skills and ability to produce high-quality deliverables • Excellent understanding of overall Agile development methodology
Portal Engineering	• Work closely with business analysts to understand business and functional requirements and ensure application development meets those requirements. • Design, document and develop new functionality according to design and industry best practices.	• Proficient in web portal development languages • Experience developing customer-facing user interfaces • Knowledge of HTML/CSS • Experience working with Web Services •

Role	Responsibility	Skills
	- Integrate third-party libraries and APIs to bi-directional transfer data. - Assist in planning and conducting various testing cycles and defect resolution. - Promote technical objects to production environment.	
Testing Management	- Develop testing strategy - Plan and conduct SIT and UAT - Conduct test defect resolution and coordination - Provide test results - Carry out template integration test	- Strong Communication and time management skills - Able to collaborate across teams - Knowledge of business processes - Experience in testing/defect management tools and approaches
Data Migration Lead	- Participate in or facilitate key tasks of data migration - Defines overall data strategy - Defines rules and processes for data management - Facilitate knowledge transfer to other project team members	- Broad knowledge of key business processes - Methodology knowledge, with implementation experience - Knowledgeable regarding legacy system data and information flow - Facilitation skills - Interpretation skills
Org. Change	- Ensure project organization readiness goals and deliverables are clearly communicated to the business - Develop the stakeholder management approach, Communications Plan and End User Training Plan - Assign people to Change Team Roles and ensure they are suitably trained - Manage the execution of all organization readiness plans and activities to ensure the organization is fully prepared to implement when scheduled - Lead the determination of	- Works effectively with all levels of management; provides detail guidance to project team members. - Maintains a 'big picture' view of the project's goals. - Possesses time management skills and multitasking capabilities. - Has superior presentation, oral and written communication skills.

Role	Responsibility	Skills
	project team training requirements • Lead the development of a communication plan to ensure stakeholder involvement and participation • Lead the development of an end user training plan	
Training	• Develop and manage project plan and strategy, including scope, schedule, resources, etc. for training and documentation • Work closely with implementation team to ensure effective and efficient integration of the documentation and training effort into the overall implementation plan • Finalize training curriculum and assist with communication to end user community • Communicate plans, issues, and status to management • Approve the schedule for all writers, instructors, and classes to provide high-quality documentation and instruction when needed • Approve and enforce training and documentation standards • Manage and mentor team leads, instructors, writers, and training coordinators • Manage training logistics plan, including facilities and scheduled classes for all end users • Develop longer-term project plans for continuing education and system enhancements	• Extensive technical knowledge about SAP's services • Conversant with organizational development concepts and organizational analysis techniques • Conversant with accepted Training methodologies, principles, and practices • Understands business process re-engineering concepts • Detail oriented • The ability to explain technical information in a clear and simple manner • Good negotiating skills • A strong understanding of business • Team working and team management experience • Good project management skills • Good organization and problem-solving skills

Role	Responsibility	Skills
Security	• Security design, development, implementation, and provisioning across various environments • Provide subject matter expertise in implementation of system/role/user/process compliance controls • Provides technical expertise in implementation support • Collaborates with cross-functional team members • Manage Segregation of Duties SoD Remediation	• Experience with User administration & Central User Administration • Roles and Authorization Management • Design and creation of Roles • SAP security for development, Quality assurance, sandbox, training, and production systems • Understand of SOX, Audit and Segregation of Duties issues and role remediation • Good understanding and working experience on LDAP technologies, Active Directory, security groups • System Trace Analysis • Security in Interface communication
HelpDesk Services	• Service as first point of contact for customers seeking technical assistance • Perform remote troubleshooting • Determine the best solution based on the issue and details • Direct unresolved issues to the next level of support • Record events and problems and their resolution in logs • Follow-up and update customer status and information • Responsible for defining Help Desk procedures • Communication procedure on how issues will be reported and resolved; • Set up the Help Desk infrastructure	• Proven experience as a help desk technician or other customer support role • Working knowledge of office automation products, databases and remote control • Good understanding of computer systems, mobile devices and other tech products • Ability to diagnose and resolve basic technical issues • Excellent communication skills • Customer-oriented

1.2.5.1.5 Project Governance Model / Approach

Infosys believes that governance is one of the critical investments in the success of programs. This view has been built over our delivery experience across a diverse range of similar engagements, reinforced by industry research and analysis showing a direct correlation between successful project outcomes and governance.

To effectively address inherent implementation complexities, remove barriers and ensure that deliverables are met in a quick and coordinated fashion while maintaining quality, Infosys will establish an integrated 3-Tier governance framework.

Each tier in the governance framework will:

- have clearly identified roles and responsibilities and ways of working.
- have key roles from both State of Maine and Infosys embedded strategically to complement each other's expertise.
- collaborate and seamlessly enable other tiers with minimal intervention and oversight from State of Maine.

In terms of their focus, the three Tiers can be characterized as:

1. **Vision Tier:** Focusing on providing vision, organizational enablement, relationship and guidance to program teams; this tier consists of executives from State of Maine and Infosys.
2. **Enablement Tier:** Focusing on providing management oversight, facilitation and advisory with the objective of removing impediments and enabling execution and strategic decision-making. This tier consists of the PMO, PMO leadership and representation from teams like Organization Change Management (OCM) and Solution Architecture
3. **Execution Tier:** Focusing on day-to-day activities, refinement and delivery of the Product Backlog, this self-organizing, self-sustaining tier consists of the Technical Implementation teams from Infosys and related teams from State of Maine, Helpdesk Services

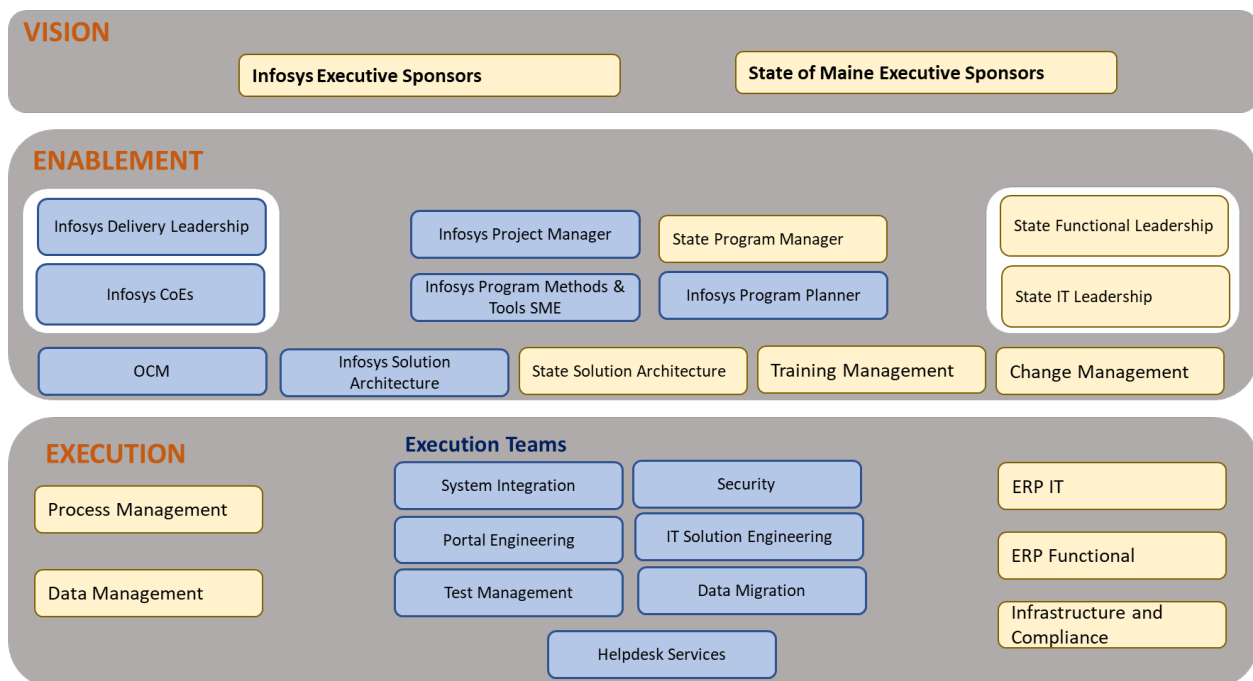


Figure 78. Governance Framework

The governance model put in place will drive the policies and procedures that will be employed to confirm the timely completion of tasks as well as the decision-making responsibilities at each project level and decision escalation process.

The State of Maine and Infosys will jointly be responsible for the management of the program and for providing the necessary resources to the program. Joint management objectives are focused on tightly monitoring, controlling, and balancing the project's three key constraints — Scope, Budget, and Schedule — while focusing on providing business value. Our approach for managing a program is predicated on establishing:

- An agreed-upon baseline: The baseline for project performance would be defined in a Statement of Work document. This document must be reviewed and approved by State of Maine and Infosys.
- A process to monitor progress: Infosys defines this as the approved detailed work plan. Project Team members will need to report their progress against completing the task outlined in the plan using actual hours spent as well as hours estimated to complete the activity.
- A clear means of communication: Infosys will use an agreed upon Status Report and Weekly Status Meeting for formal communication. The format Infosys uses for status reporting includes the following sections:

Infosys provides a high level of service excellence, achieved through accessible and monitored governance processes. The governance and Process Management tool package consists of a governance library, performance assessments, and a balanced scorecard.

The detailed Implementation plan is the key vehicle for measuring progress and verifying completion. The specific activities that each team member works on, and their progress against completing those activities, will be managed via the project plan. This will allow project management to measure performance against the schedule and budget.

The following image shows an illustrative schedule for governance meetings.

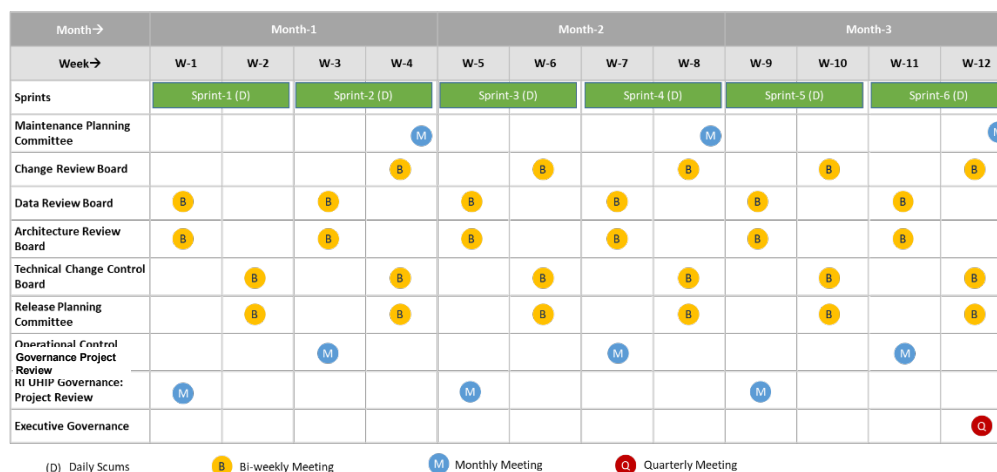


Figure 79. Governance Schedule (Illustrative)

1.2.5.2 Project Implementation Methodology

IDEA-Activate™ Implementation Methodology

Infosys' IDEA-Activate™ utilizes SAP Activate methodology, enhanced with Infosys' experienced consultants using proven Infosys accelerators, consisting of tools, templates, and leading practices; to simplify and streamline your transformation project. Using a hybrid-agile framework that uses Industry best practices and SAP standard solutions for Ariba and other SAP systems to achieve results

and deliver value quickly. Combined with the implementation constructs, Infosys' IDEA-Activate™ includes proven program management tools, change management, robust communication plan, deployment approaches and others to form an integrated, compressive methodology.

IDEA-Activate™ supplies best practices, tools, and methods on WHAT, HOW and WHEN to enable business transformation. Our IDEA-Activate™ framework is designed specifically to drive value levers out of business transformation programs. It provides a comprehensive, holistic approach to achieve organizational transformation and objectives, cutting across business and/or functional lines. It outlines a guiding framework and key principles for the effective project and program governance, communication and integration required for program success.



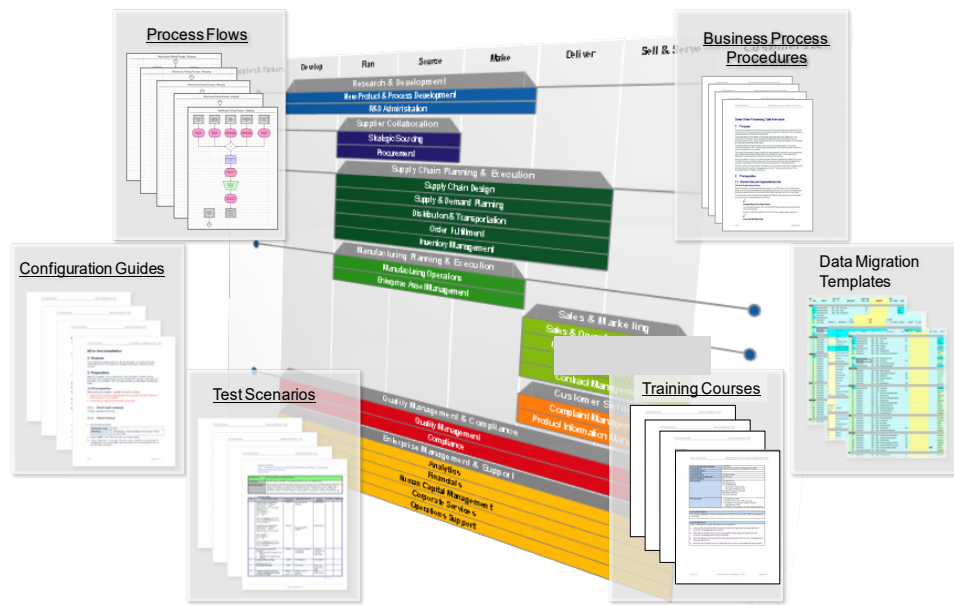
Figure 80. IDEA-Activate™ Methodology

- Provides a comprehensive, holistic approach to achieving business transformation.
- Enables client-acclaimed solutions via an ongoing dialogue
- Value realized is used to set the direction and guide the transformation
- Information is the key enabler of value-creating and decision-making
- Cuts across organization and/or disciplinary lines
- Ensures that effective governance, communication, and integration is available across work streams to achieve success

Accelerating Successful Projects

A preconfigured system with associated Ariba process and documentation to accomplish an accelerated, successful project. Additionally, the project must include practitioners that understand how to leverage the system and focus on differentiating processes. Best practices, templates and guided procedures are Infosys' comprehensive set of integrated enablers that encompass key industry processes. Infosys provides services around these preconfigured systems and RDS using our industry expertise, enhanced business processes, and other implementation accelerators.

The IDEA-Activate™ approach streamlines our customers' implementation to be "On Time," "On Budget," "On Quality," and "On Value." IDEA-Activate™ is an out-of-the box template that provides the foundation of critical functions to run a competitive business. Our pre-configured templates are based on leading practices from Infosys and Ariba and enhanced with our leading practices developed from our client experiences and provide the foundation for a highly effective project.



Infosys Templates

We realistically do not expect a 100% fit of the template to any business, including the State of Maine. Every business has its own unique processes that differentiate them in the market, which we take into consideration, as we will begin to use the template as a springboard during the Lean Blueprint. Leveraging the built-in industry leading practices, the template will provide business value and demonstrate process simplification that will allow State of Maine to “Get Back to the Basics.” Our concept is to define high value add processes that differentiate State of Maine and concentrate time and resources on those while implementing more standard processes in areas that produce little value.

Advantages of Infosys’ Approach for SAP Ariba Transformation

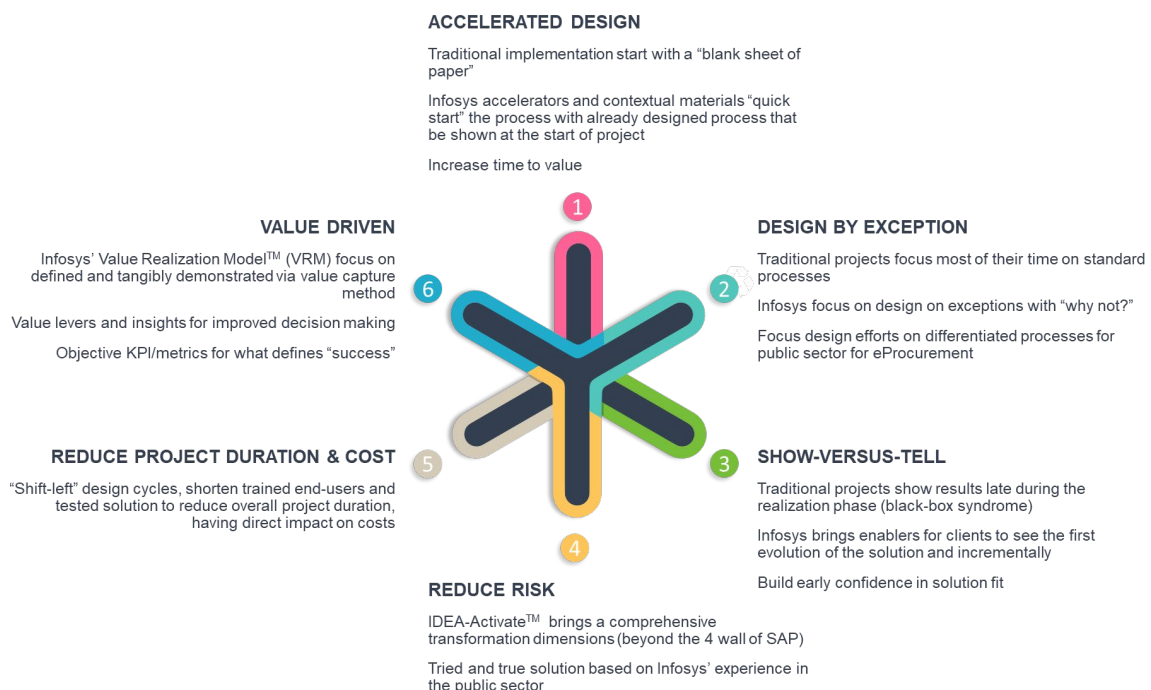


Figure 81. Advantages of Infosys’ Approach for SAP Ariba Transformation

IDEA-Activate™ compared to SAP Activate

IDEA-Activate™ is an “extension” of SAP Activate, which is the implementation approach for Ariba projects. Through eProcurement and other SAP engagements, we have developed a framework that addresses the “total” transformation journey and not only the SAP four walls. Clients have disparate application systems, and IDEA-Activate™ brings a prescriptive and tool-box approach to system integrations, subject matter experts, integrated project plans and more. The high-level process and activities are shown below and its alignment to SAP Activate phases. It’s important to note that SAP Activate is the foundational layer and will continue to be in partnership with the broader SAP methodology.

Going forward in this document, we will use SAP methodology terminologies for quick adoption and ease of comparative nomenclature.

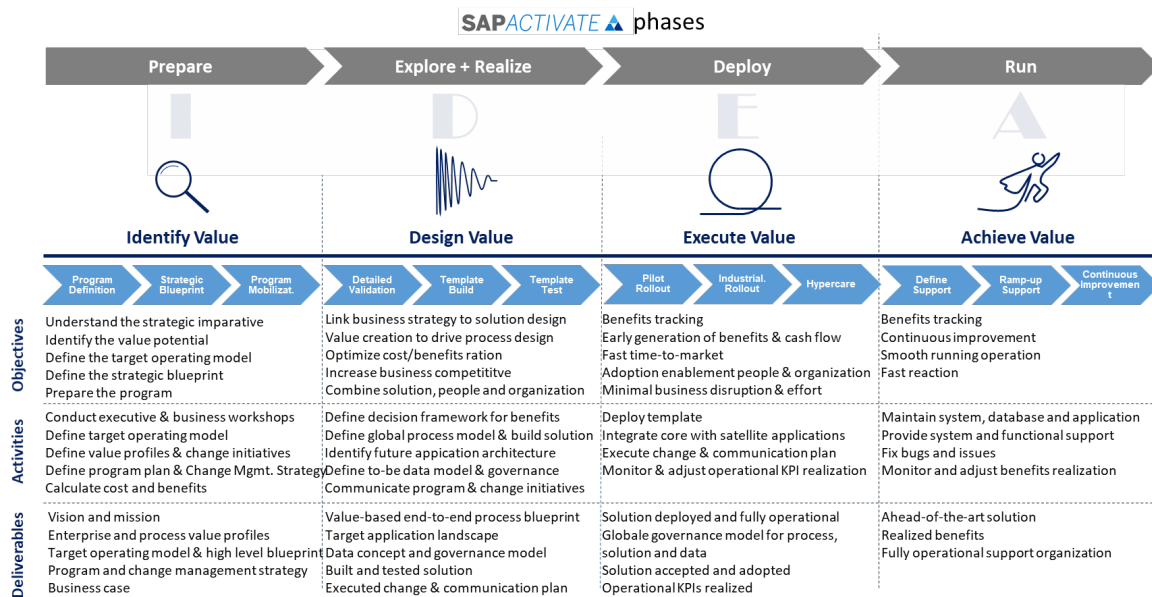


Figure 82. SAP Activate phases

Delivery approach, methodologies, and best practices

The Team Infosys targeted PMO solution for The State of Maine meets all aspects of program management by reducing risk and project delivery cost, improving productivity and project delivery quality, providing metrics and reporting that assist with monitoring performance and prioritization, which in turn will maximize realization of benefits and project goals.

Team Infosys leverages the IDEA-Activate™ Framework’s ‘Lead & Manage Transformation’ thread to manage all Program level processes covering scope, schedule, cost, quality, people, governance, communication, issues and risks, performance mgmt., and yearly planning. The figure below shows the dimensions of responsibilities that the Program Management Office (PMO) will carry in its day-to-day functions, and Team Infosys will support it.

Project/program management is a critical element of successful SAP implementations. From the very beginning of the project, this will be a focus of Infosys’ in order to drive the overall success of the project. We will provide guidance and best practices to State of Maine as well as leverage our proven tools and the successful strategy we have already used in several implementations.

We have a comprehensive and proven program management approach to managing the different work streams, which are in the scope of the RFP. Our approach is a finely tailored, proven approach for the State of Maine EProcurement project.

The principles we follow in the work stream are derived from Infosys' experience of managing multiple similar initiatives with clients globally. Our approach is based on following principles:

- **Value-driven** – this is a critical principle as we have seen programs succeed when decisions are taken, and conflicts resolved when there exists a framework that emphasizes the value
- **Quality focused** – we strive to ensure quality assurance and quality control through our Program Management Office (PMO) organization across all work streams
- **Collaborative** – we adopt a consensus-based, collaborative approach to decision making and resolving differences of opinions through a logical objective framework and not on emotions.
- **Engage stakeholders** – we draw upon the latent knowledge of all stakeholders of RI Bridges system and organization dynamics to ensure accountability among stakeholders
- **Best practice based** – we bring standardized and simplified PMO operations through our Project Capability offering. Team Infosys team utilize standard tools as used by the State of Maine. Also, our offering optimizes overall project management delivery by leveraging our 'Suitcase' toolkit of templates and tools (Ex. content management, trackers, dashboards, reports, risk register, lessons learned) to minimize setup time. The use of these standardized templates enables automation in areas such as reporting, analysis, and alerts (Ex. Automatically send status reports or automatic notifications to PMO and relevant stakeholders when issues are open)
- **Making everyone successful** – we respect the different partners of the State of Maine and are appreciative of their interests and goals. We work with all parties to make them successful and expect the same from others as well
- **Focused and Ethical** – we pride ourselves in demonstrating ethical practices and behavior in our work and interactions with stakeholders with a “get-it-done” attitude.

Hybrid-Agile Methodology

The Infosys hybrid agile methodology deals with building large and complex eProcurement transformations that is optimized for SaaS applications and integration with other technology stacks, such as on-premise, non-SAP and others. Our flexible model considers integration partners and their SLDC which may not be agile, thus bringing complexity to logical units of work within a sprint.

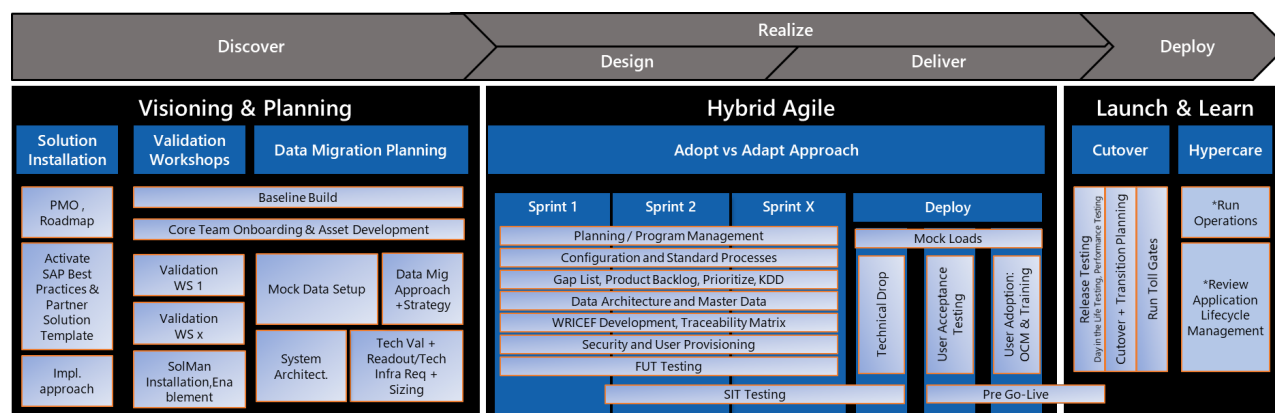


Figure 83. Infosys Hybrid Agile Methodology

Once the solution (e.g. shippable product) is ready, comprehensive System Integration Testing (SIT) cycles are conducted to ensure end-to-end processes, technology and personas with the right user role access validated, requirements traceability documented, GRC satisfied and more. Additionally, the SIT outcomes are communicated to stakeholders and partners to further growth enthusiasm and high-touch as the schedule proceeds to go-live. Finally, User Acceptance Testing (UAT) is conducted

to key user community for final acceptance of the solution, data and training, thus leading to the approval for cut-over and deployment.

Leveraging an agile construct, it enables our solution, multiple independent development scrum teams to work in parallel, thereby increasing velocity of development and time-to-value. One of the key roles is the scrum of scrums to coordinate integrated activities, solutions, data, reusable processes and risk mitigation, collaborating across scrum masters. Regular scrum of scrum meetings allow for predictable and controlled sessions, while the scrum of scrum lead has the discretion to orchestrate sessions as required.

Sprint Execution:

Various agile methodologies have evolved to cater to the changing business needs and reducing time-to-market. Infosys has an expert in-house agile methodology revolve around closely knit motivated individuals, being flexible to changes, delivering working software frequently and keeping the least amount of process overheads. Below is a basic example of our Agile Methodology.

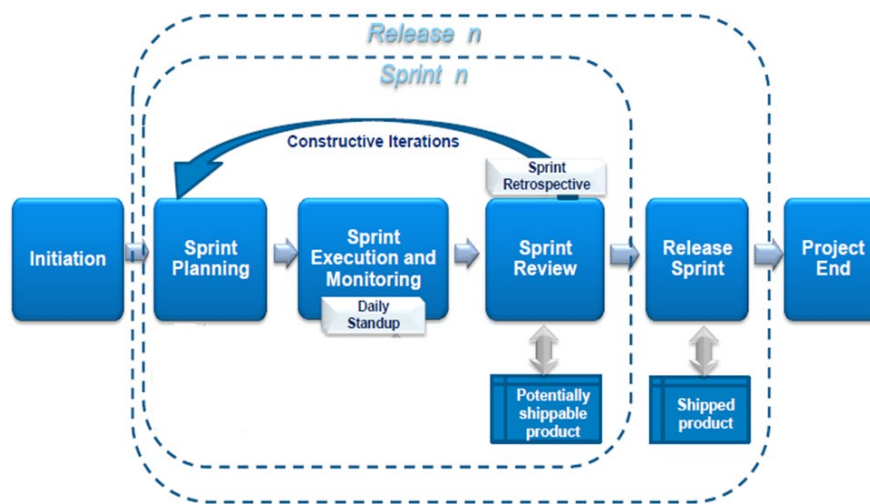


Figure 84. Agile Life Cycle Phases

The Scrum Team

Following common practice with agile standard and experience, scrum size is kept relatively small ranging from 6 to 10 team members. In case the story size exceeds this team limit, the stories can be further divided into smaller stories to be distributed across smaller, multiple teams. This ensures high velocity scrum team execution and accomplishable work products within a given sprint cycle.

Each scrum team consists of combination of domain, business subject matter experts, experienced and junior developers, testers and project manager who would act as a scrum master for individual sprints.

The Infosys Scrum master is assigned to one or two scrum teams. The Infosys scrum master is part of the State Scrum of Scrum team led by the State of Maine Scrum Master.

The Scrum team size is consistent for the duration of development of each module. Any spikes in sprints resulting from a need to do research, Proof of concept, technical design will be addressed by adding additional team members to an existing scrum team or by adding a temporary scrum team.

Scrum Team Roles and Responsibilities

Table 43. Scrum Roles and Responsibilities

No	Role	Scrum Team	Responsibilities
1	Product Owners (from State of Maine)	Sprint Management	- Define Product Roadmap and provide inputs for Release planning - Develop product backlog and provide user stories, issue resolutions, prioritize user stories - Perform User Acceptance testing and defect prioritization - Formally accepts / rejects product at completion - Provide direction to Project Management team on issues IDEA-Activating triple constraints - Review and audit of the project at regular intervals - Formally accept project at completion
2	Scrum Masters	Sprint Management	- Responsible for the overall project (Sprint) success and deliverables - Helps resolve impediments, ensures the team is fully functional and productive - Provide prioritization of Architectural changes vs. User Story development - Facilitate Sr. Management reviews, provide status updates and sign-off process - Manage project communications, issues and risks
3	Technical Lead/ Technical Analysts	Development Sprint Team	- Conduct planning and break-down of user stories to task level & create Sprint Backlog - Perform estimation of the tasks, plan and commit user stories for the Sprint - Design, development and unit testing of the user stories / technical architecture changes - Facilitate design review, code review sessions with Technical Architecture team - Co-ordinate with QA team for defect triage, support Release team during implementation - Report development progress, create burn-down charts, metrics and status reporting - Provide lessons learned/retrospective inputs to the Project Management, QA and Release Team
4	Technical Experts or Subject Matter Experts (SME)	Development Sprint Team	- Define Technical Architecture Strategy and Technology Roadmap - Develop technical change backlog and prioritize architectural changes with Product Owners - Advise development teams on best practices, standards, tools and security architecture

No	Role	Scrum Team	Responsibilities
			Review and approve technical design, configuration documentation for application deployment
5	Test Analysts	Test Sprint Development & Execution	- Co-ordination with development team / Product Owners, obtain clarification on user stories - Define Test plan and develop test cases by products / modules, create regression test plans - Execute test cases, log defects, and facilitate defect triage - Track and report progress, defect status and metrics

RACI

Table 44. RACI Definition

Type	Responsibility Description
Accountable	The 'owner' of the deliverable and authorized to hold accountable those responsible
Responsible	Those who do the work and are responsible for the result. They report directly to the person accountable.
Consulted	Those whose opinions are sought as part of the decisions and / or steps are taken to achieve the result (two-way communication)
Informed	Those who are informed after decisions have been made or results have been achieved. They have no influence over the result

Table 45. RACI Matrix

	Activities	State	Infosys
1	Program Leadership		
1.1	PMO		
A	Integrated Project Plan	A,R	R
B	Implementation Methodology	A,C	R
C	Project Management Execution	A,R	R
D	Project Tools	C	A,R
E	Onboarding Materials	C	A,R
F	Mobilize Required Team Members	A,R	A,R
G	Scope Change Control	A,C	R
2	Solution		
2.1	Solution Architecture		
A	Solution Architecture	A,C	R
3	Process Teams		
3.1	High-level requirements		
A	Requirement gathering/validation	A,C	R
B	Develop requirements traceability matrix	A	R
3.2	Business Process Design (Release 1 and 2)		

A	Business Process Hierarchy	A,C	R
B	Business Process Design (Release 1 and 2)	A,C	R
C	Business Process Documentation (Release 1 and 2)	A,C	R
3.3	eProcurement Solution (Release 1 and 2)		
A	Functional Design (FSD, Functional Unit Test)	A,C	R
B	Develop Configuration Workbook	A,C	R
C	Configuration for DEV, QA, Training, PRD	A	R
3.4	State Legacy Application Solution		
A	State Legacy Application Design (Design, Documentation, Functional Unit Test)	A,R	C
3.5	Security Governance & Management		
A	Security Access Authorization (Design, Build, & Test)	A,C	R
B	Security compliance	A,C	R
3.6	Reporting & Analytics		
A	Ariba Reporting (Design)	A,C	R
B	Ariba Reporting (Build & Test)	A,C	R
4	Development		
4.1	Development (eProcurement)		
A	Develop Configuration and Development List	A,C	R
B	Technical Design, Build, & Unit Test	A,I	R
4.2	Development (State Legacy Applications)		
A	Develop Development List	A,R	C
B	Technical Design, Build, & Unit Test	A,R	I
5	Testing		
5.1	Testing: Approach, Plan & Schedule		
A	Testing: Approach, Plan & Schedule (for Release 1 and 2)	A,C	R
5.2	Testing: Support & Execution Mgmt. (for Release 1 and 2)		
A	Testing: Execution Management	A	R
B	Integration Test Script Development	A,R	R
C	Integration Test Execution - eProcurement	A,C	R
D	Integration Test Execution - State Legacy Applications	A,R	C
E	Integration Test Results Approval	A,R	C
F	User Acceptance Test Script Development	A,R	C
G	User Acceptance Test Execution & Signoff	A,R	C
5.3	Testing: Performance (SaaS platforms will not be tested)		
A	Performance Test Requirements (SaaS application excluded)	A,C	R
B	Performance Test (SaaS application excluded)	A,C	R
6	Deployment & Cutover		
6.1	Cutover Plan & Schedule		
A	Detailed Cutover Plan (for Release 1 and 2)	A,R	R
B	Cutover/ Go Live Plan and Scorecard (for Release 1 and 2)	A,R	R
6.2	Business Deployment		
A	Detailed Deployment Plan (for Release 1 and 2)	A,R	C
B	Business deployment	A,R	C

7	Data & Conversion		
7.1	Data Conversion		
A	Data Migration Strategy	A,C	R
B	Data Integrity/Quality Issues	A,R	C
C	Rule based Data Cleansing	A,R	I
D	Manual data Cleansing	A,R	I
E	Legacy Data Extraction into CSV format	A,R	C
F	Mapping sheets for Legacy and Other Legacy/Ariba	C	A,R
G	Migration of Legacy & other legacy system Data into Ariba	A	R
H	Mock & Dry run	A,R	R
I	Production Data migration	A,R	R
8	Change Management		
8.1	Change Management		
A	Define Change Management Ways of Working	A,C	R
B	Identify and Activate Key Sponsors and Stakeholders	A,C	R
C	Conduct Stakeholder Segmentation	A,C	R
D	Conduct Leadership Alignment and Engagement	A,C	R
E	Conduct Change Impact Assessment	A,C	R
F	Define and Develop Change Management and Communication Strategies	A,C	R
G	Develop Communications Plan	A,C	R
H	Execute Communications	A,R	C
8.2	Training Development (Release 1 and 2)		
A	Conduct Training Needs Analysis	A,C	R
B	Analyze and Develop Training Strategy	A,C	R
C	Develop Training Materials (in English, client to translate where required)	A,C	R
D	Develop Training Logistics/Schedule	A,C	R
E	Deliver Train-the-Trainer Training	A,C	R
F	Deliver End-User Training (25%)	A,C	R
G	Post Go-Live Support	A,R	R
9	Post Production		
9.1	Post-Production Support		
A	Hypercare: Twelve (12) Weeks of program Support & Break/Fix	A,C	A,R
B	Transition to Steady state support	C	A,R
10	Operations		
10.1	Incident Management		
A	Tier 1 Support	C	A,R
B	Tier 2/3 Support	C	A,R
C	Knowledgebase Management	I	A,R
D	Incident reporting (daily, monthly, annually)	I	A,R
10.2	Service Request Management		
A	Service request submission	A,R	C
B	Service request assessment and approval	C	A,R

C	Service request fulfillment	A,C	R
10.3	eProcurement Application Maintenance		
A	Application patches and regular updates	I	A,R
B	New business capability releases and platform changes	A,C	R

Sprint Planning and Execution

Infosys understands that the product owner and the scrum master from the State of Maine will work closely with the scrum development team. The Infosys Team will work with the State of Maine for defining & implementing Agile process to define Sprints, Product Backlogs, Sprint Backlogs, Scrum Meetings, Sprint Planning, Sprint Reviews, Sprint Retrospectives, and Burn down Charts during this engagement.

Below are the key phases of the Agile Life Cycle:

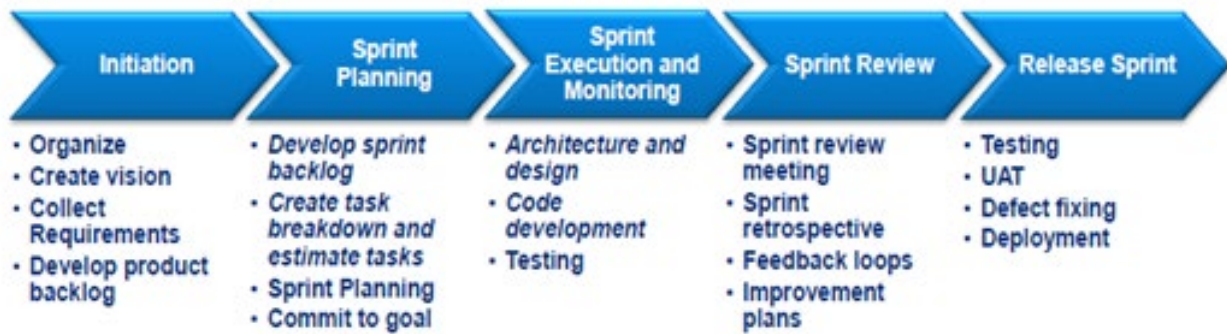


Figure 85. Agile Phases – Activities

Any user story de-prioritized moves back into the product backlogs. The Release retrospection defects, or clarifications are well sought during the Scrum of Scrum calls and the product, business owner's perspectives are taken in to improvise the efficiency of the subsequent Sprints.

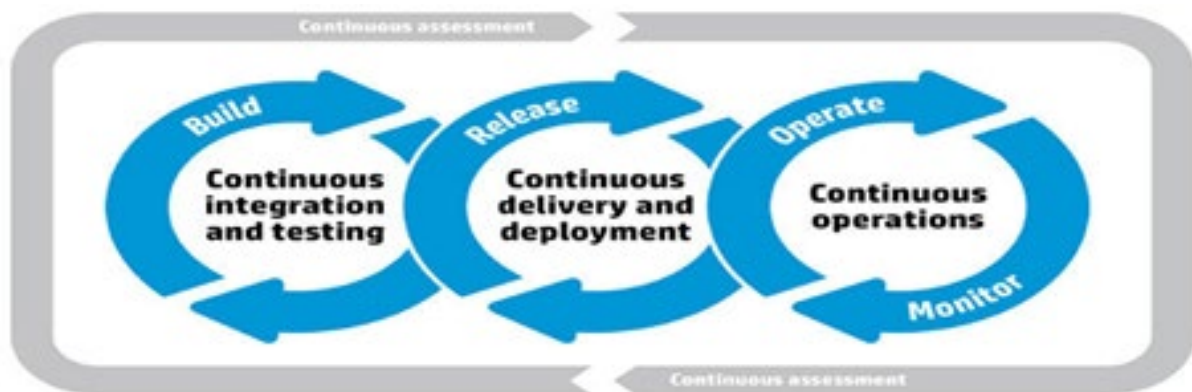


Figure 86. Continuous Assessment

Continuous assessment is carried out by incorporating monitoring tools and processes early in the development. This provides valuable insight into the application before it goes into production. This automation of information collection and consolidation process leads to lower costs.

Many existing problems in DevOps and SDLC are handled effectively in this process, and it offers numerous advantages such as:

- Automated Continuous Delivery will handle various Environment Issues relating to stability,

consistency, and reliability. Automated Deployment will be done simultaneously to various environment in the proposed process to ensure Consistency in Environments.

- Manual process is non-repeatable and can lead to human error. Automation is leveraged to maximum in each activity in the proposed process to ensure minimal manual intervention, by using automated testing tools for Unit Testing, Build Verification Testing, Performance Testing and Security Testing.
- Collaboration between Development, Testing and Operations Teams will be improved by adhering to the proposed process there by improving the work culture and working environment.
- Continuous Monitoring will ensure reliability and stability of the RI Bridge's Application. Any issues will be immediately notified and addressed. Early detection of issues is one of the main advantages of the proposed process.
- A streamlined, automated, and continuous code management is achieved by adhering to the proposed process, which will ensure continuous and faster delivery of features.

By leveraging latest automation features in modern tools, our proposed code management process will enable us to deliver quality, scalable and maintainable code swiftly.

PREPARE

During the "Prepare" phase, business executives define the case for change, the process and technical teams confirm the solution and pre-assemble demos, and design/configuration sprints are planned. Agile and method training is provided to new project team members

Prepare Phase

□ Work products that are additional/unique to IDEA-Activate™

Prepare Phase				
Work Streams	Mobilization	Process/System Classification	Scope	Solution Preassembly
Project Management	• Team mobilization • Agile Technique Education • Method and Tools Adoption Workshops • Solution Manager Strategy • SCRUM Operating Model	• Method and Tools Roadmap • Prioritized Backlog • Design/Prototype and Build/Automate Sprint Plans • Release Plan • Definition of Done		• Testing Strategy • Governance Model and Procedures • Explore Phase Kick-Off Presentation Materials • Project Status Dashboards • Validation Master Plan
Process	• Business Process Hierarchy (BPH) • Process Step Scope (Requirements) • Industry Solution Demo List	• Leading Practice Process Flows • Pre-configured Ariba Environment □ • Process Step Sizing • Global/Local Configuration Objects		• Initial SAP Organizational Hierarchy • Initial "Standard" Process Configuration (with Representative

	Prepare Phase		
Work Streams	Mobilization	Process/System Classification Scope	Solution Preassembly
		Pre-Assembly Questionnaire (Organizational and Master Data) □	Data – where applicable) - Role-Based “Adjusted” Process Flows - Demos of “Standard” User Stories in Panaya (additional service)
Data and Analytics		- Data Migration Strategy - Key Report Inventory	
Technical	- System Landscape Strategy - Reference Environment	- Initial WRICEF Scope - System Integration Strategy	- Project User Roles - Development Standards
OCM/Value Management	- Stakeholder Analysis - Interview Questionnaire - Case for Change	- Key Performance Indicators - Business Case - End User Training Strategy	- Stakeholder Management Plan - Communications Strategy

EXPLORE

During the “Explore” phase, the team confirms and builds the “standard” components of the preassembled solution, conducts detailed design workshops and develops proofs of concept for approved “adjustments” and “additions” to the standard solution. Integration sprints are conducted at the end of the phase.

Explore Phase

□ Work products that are additional/unique to IDEA-Activate™

	Explore Phase			
Work Streams	Standard Process Build/ Showcase/Document (>70%)	Differentiating Process Design/ Specify/Prototype (<30%)	Pilot Localization Solution Confirmation	Design/Interim State of Maine Integration Sessions
Project Management	Template Standardization Metrics □	- Sprint Iteration Plan □ - Prioritized Backlog □	- Sprint Iteration Plan □ - Prioritized Backlog □	- Build/Integration Sprint Plan □ - Prioritized Backlog □

Explore Phase				
Work Streams	Standard Process Build/ Showcase/Document (>70%)	Differentiating Process Design/ Specify/Prototype (<30%)	Pilot Localization Solution Confirmation	Design/Interim State of Maine Integration Sessions
	Prioritized Backlog ☐			Sprint Retrospective ☐
Process	- Role-Based 'Standard' Process Flows - Playback Demos of "Standard" User Stories (Panaya in Client Environment) ☐ "Standard" Process Configuration and Rationale Documents - Showcase Sprint Outcomes ☐	- Final Role-Based Process Flows - Proofs of Concept (Visualization) ☐ - Final Configuration and Rationale Documents - Initial End-to-End Test Cases - Functional Requirements - Showcase Sprint Outcomes ☐	- Final SAP Organizational Hierarchy - Localization Solution Confirmation - Local User Stories ☐ - Showcase Sprint Outcomes ☐	- Regression Assessment of "Standard" Processes ☐ - Final WRICEF scope - Final End-to-End Test Cases ☐
Data Analytics &	- Data Governance Approach - Data Quality Assessment "Standard" Report Selection	- Source to Target Data Map "Standard" Report Activation - Final Analytics Scope	Source to Target Data Map	First Master Data Load for Unit Testing
Technical	- Security Strategy including SoD - Standard Security Role Build/Test	- Final Security Role Design Incl. SoD - Proofs of Concept (Development)	- Local Technical Readiness Assessment - IQ of Environments	- Non-Functional Requirements - QA Environment
OCM/Value Management	Initial End User Role Definition	Change IDEA-Activate Action Plan	Change IDEA-Activate Action Plan	Interim State of Maine IDEA-Activates and Procedures

Explore Phase				
Work Streams	Standard Process Build/ Showcase/Document (>70%)	Differentiating Process Design/ Specify/Prototype (<30%)	Pilot Localization Solution Confirmation	Design/Interim State of Maine Integration Sessions
			Final End User Role Design and Mapping Templates	

Explore Phase: “Process Design” Sprint

This Sprint involves best practices and business scenarios with a prototype to drive the design to enable a comprehensive and accelerated process adoption. Key users are actively engaged during the workshops visualizing the future State of Maine capabilities and to define the detailed solution design requirements. Combining agile “Design, Build, and Test” iterative cycles, we accelerate the timeliness of solution “validation” and user acceptance consensus. Our approach is flexible for interfaces between existing system(s) to Ariba where a traditional waterfall development framework using Joint Application Design (JAD) sessions could be well leveraged. We will work with the State to determine the optimal construct for high velocity throughput.

During this phase, we conduct a series of design workshops with functional leads and bring in leading practices to influence the future State of Maine design.

Our key differentiator is our ability to demonstrate various Ariba functionalities in our pre-configured demo environment, which will greatly help the functional stakeholders design the State of Maine’s future state procurement processes.

Our design workshops will provide an understanding of the State of Maine’s current state processes, pain points, business needs, current capabilities, and help us in designing future-state procurement processes which are streamlined, harmonized, and drives maximum efficiency.

At the end of these workshops, we will be able to capture the State of Maine’s future-state requirements, which will help us to develop the overall functional and technical documents including configuration workbooks and the security role matrix.

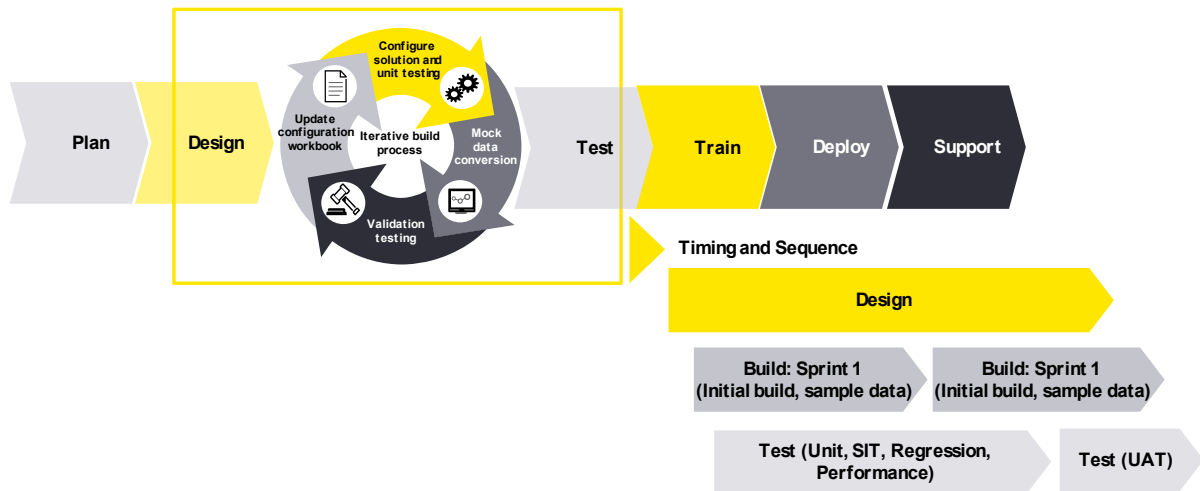


Figure 87. Agile during Explore Phase

Key highlights and benefits of our approach:

- Our design sessions are supported by a pre-configured Ariba environment walkthrough.
- The Demo environment is configured based on leading practices.
- In our Agile development, testing is integrated during the cycle, which means there are regular checkups to see the module is configured to our client's needs.
- This method also reduces the risk of the deployment by accelerating the discovery of any design issues
 - Increasing the transparency of the deployment and allows for quick course corrections as needed
 - Keeps business stakeholders engaged through the development process which helps with user adoption

Additionally, we will bring various accelerators to the table such as the Ariba deployment toolkit and templates which are based on leading practices and are proven to accelerate the design-through-deployment activities. These accelerators will be leveraged to bring additional speed and value for you. In the image below, you will see a variety of these accelerators and leading practice models which could bring the best possible outcome for the State of Maine.

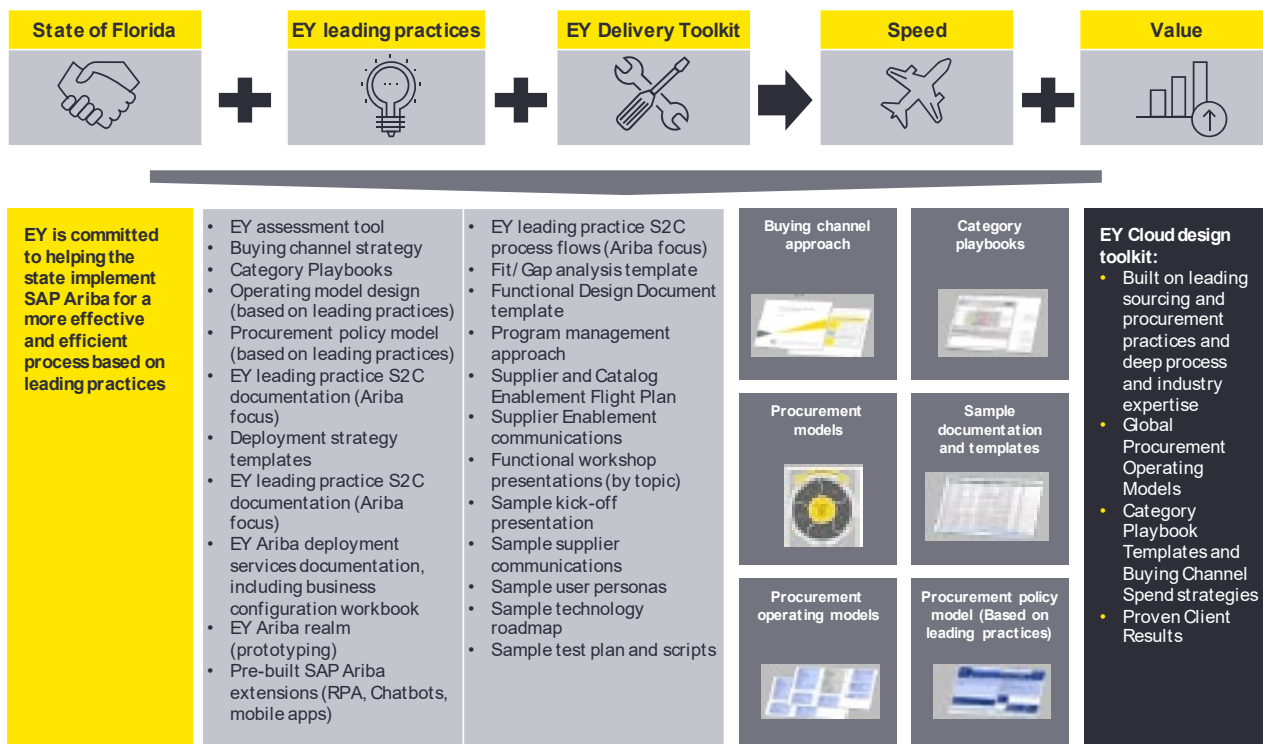


Figure 88. Best Practices and Toolkit for EPS Implementation

Key Roles during phase (illustrative)

Table 46. Key Activities and Roles

State of Maine	Infosys and EY	SAP Ariba shared/field services
- Actively participate in design workshops (Functional and Technical SMEs) - Responsible for review and sign-off of design documents, determine org impacts/redesign needs - Identify integration requirements (Interface modifications), & data design - Manage master data - Develop supplier flight plan [SAP Ariba] and initiate supplier enablement outreach	- Create requirements document and configuration workbook - Facilitate design validation workshops to review global template against localization requirements - Document to-be design requirements - Kick-off supplier enablement strategy and planning - Complete the SAP Ariba configuration workbooks	- Confirm configuration parameters - Support identification of customizations (fields, interfaces, data) - Review design documentation - Support creation of configuration workbook - Support technical design and integration - Support Supplier enablement

Fit-to-Standard Design Confirmation and Exception Framework

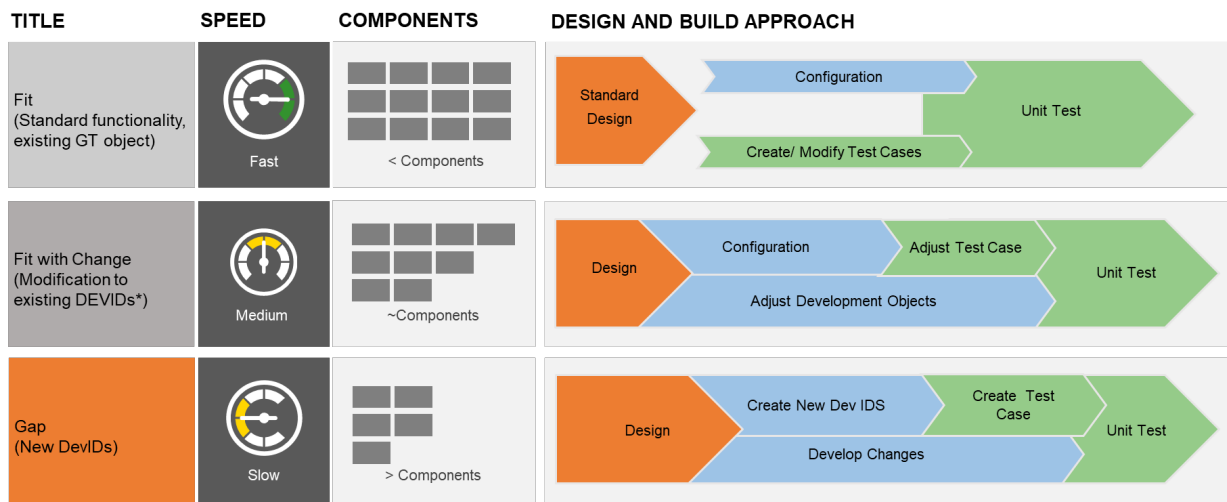
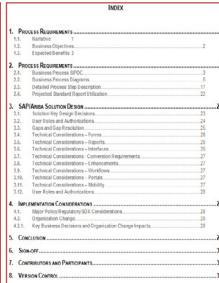
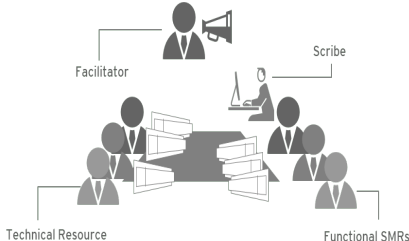


Figure 89. Design Confirmation Framework

Utilizing proven tools and accelerators to help facilitate design workshops will significantly reduce the overall cost and speed up the transformation journey with an unmatched time-to-value for you. These are reliable, proven tools that we have developed over time and have used to drive benefits for other clients and will result in substantial benefits for the State of Maine.

Table 47. Different Types of Design Workshop Accelerators and Enablers

#	Accelerator / Enabler	Description and Benefit	Illustrative example
1	SAP Ariba Demo environment (With sample data)	- A preconfigured SAP Ariba environment based on leading practices - Rapid functionality demonstrating business scenarios Benefit: Early tangible view of the future state system allowing for rich design sessions	
2	Leading Practices and design Blueprint	- Procurement leading practices as seen in the industry - Trending digital procurement practices - The EY Power and Utility Maturity Model (PUMMA) is a repository of sector processes and leading practice which can be leveraged in the design workshop setting as an accelerator to drive process design conversations Benefit: Future state design is based on leading practices	

#	Accelerator / Enabler	Description and Benefit	Illustrative example
3	Business process and functional design documents	- EY's delivery toolkit, a one-stop shop for all templates, sample deliverables, assets and enablers to accelerate delivery and drive high quality work outputs - Future-state process flows, and process documentations helps in facilitation and walking through a high-level business scenario - Templates to capture business process and functional design requirements - No missed requirement for configuration - Guidance on business scenarios Benefit: Template to help accelerate the documentation of requirements Robust methodology to confirm all requirements are captured	 
4	Facilitated workshops	- Facilitated workshop methodology to engage all stakeholders - Supported by technical and functional expertise to answer questions/concerns Benefit: Engage participants to help people build on each other's ideas and rapidly categorize and prioritize the most pressing initiatives. This approach increases the efficiency in design sessions, accelerating speed to outcome.	
5	Virtual workshop tools	- EY has experience delivering deployments in a virtual, Covid-19 world. We leverage our virtual tools (Microsoft Teams, ThinkTank, Murals, Whiteboarding). - EY Wavespace™ facilitate workshops and engage participants in the virtual world to help people build on each other's	

#	Accelerator / Enabler	Description and Benefit	Illustrative example
		ideas and rapidly categorize and prioritize the most pressing initiatives. This approach increases the efficiency in design sessions, accelerating speed to outcome.	

REALIZE

During the “Realize” phase, the tests for “standard” processes are automated in parallel to build/test sprints for approved process “differentiation.” Most of the effort in the end-to-end testing will be spent on “differentiated” processes.

Realize Phase

□ Work products that are additional/unique to IDEA-Activate™

Realize Phase			
Work Streams	“Standard” Process Test Automation with Security Roles /Training Materials	“Differentiating” Process & Pilot Localization Build/ Test / Showcase / Training Materials	E2E Testing including UAT
Project Management	- Sprint Iteration Plan - Prioritized Backlog	- Sprint Iteration Plan - Prioritized Backlog - User Story Traceability (System Objects, Tests) - Sprint Retrospective	- High velocity deployment strategy □ - Cutover Plan - Cutover Rehearsal - Go-Live Readiness Check - Transition Plan
Process	- End-to-End Test Automation and Process Scripts (beyond 4 walls of SAP) - Playback Demos of Final “Standard” Process User Stories	- Final Configuration - End-to-End Test Automation and Process Scripts - Showcase Sprint Outcomes □	- E2E Automated Test Results and Remediation □ - Limited Manual Testing, i.e., Localization □ - User Acceptance
Data & Analytics	Data Extracts & Transformation	2nd Data Load for Unit Testing	Full Data Load for E2E Testing

		Analytics Development for “Adjusts” and “Adds”	Data Verification
Technical	Production Environment	- Security Role Build/Test - WRICEF Development & Acceptance Documentation - Third-Party Integration Testing with Connectivity	- Technical Readiness Assessment - Performance Testing - Disaster Recovery Plan
OCM/Value Management	“Standard” Process End User Training Materials	- Change IDEA-Activate Action Plan ‘Differentiated’ Process End User Training Materials	- Business Readiness Assessment - Train-the-Trainer - End User Training Delivery Schedule

Realize Phase: “Day-in-the-Life” of a Four-Week “Final Build/Test” Sprint

Each final build and test sprint involves finalizing the configuration and/or approved development as well as unit testing to enable the user stories assigned to that sprint. Extended team members participate periodically to incorporate, i.e., security, finalize data field usage to enable the user story, and to develop training materials. The solution is highlighted to the process owner early enough before the sprint ends to allow thorough refinement before completing the documentation.

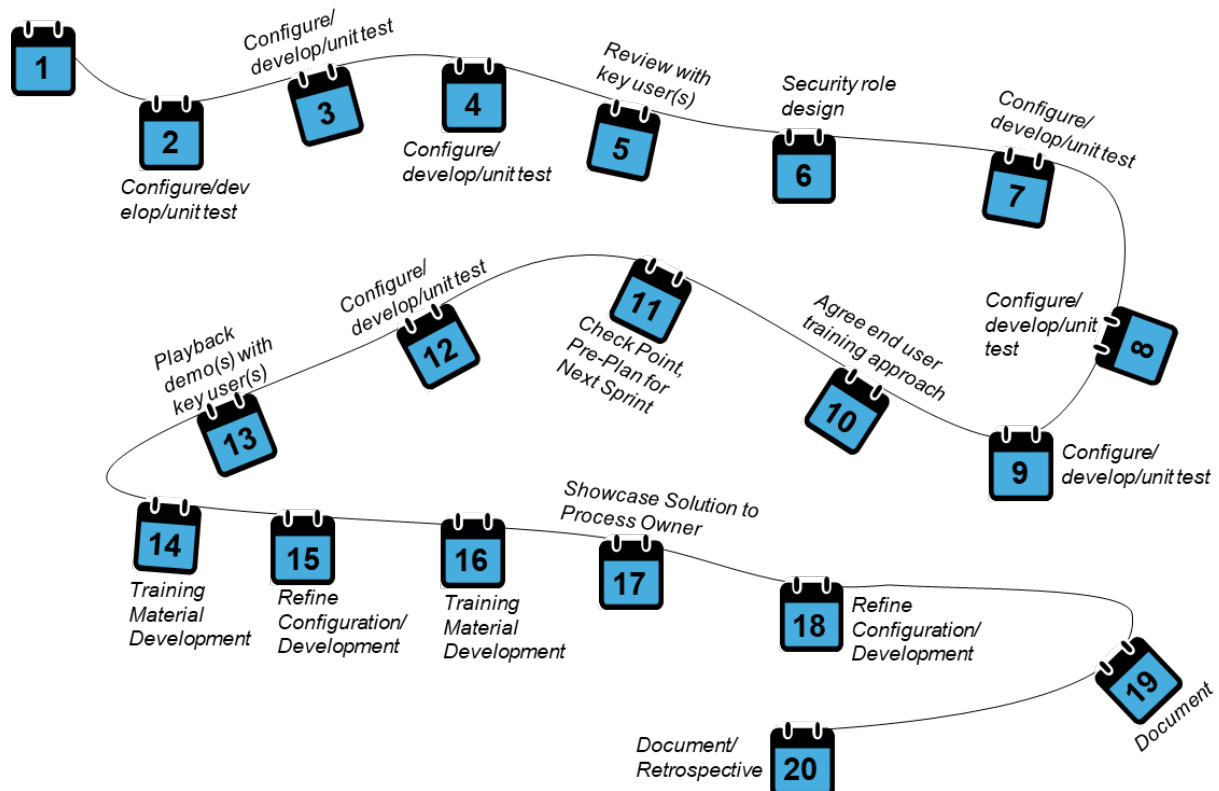


Figure 90. Day in a Life Illustration during Realize Phase

Build

The major activities during this phase is to scrum the system to configure, build, create test data and unit test according to the specified design. Our build approach, based on S2P cloud SaaS, differs from a typical on-premises approach providing numerous benefits for the overall acceleration of the solution deployment.

Our cloud-based/SaaS build approach for State of Maine:

- Leverages our proven eProcurement transformation expertise, accelerating the deployment through build tools and enablers, such as pre-existing configuration workbooks.
- Supports an iterative build process with the State of Maine stakeholders, through solution confirmation providing the State of Maine the flexibility to validate the solution and make adjustments.
- Supports solution scalability through the SAP-Ariba cloud infrastructure for the SaaS deployment.
- Minimizes customization to the solution by leveraging standardized process design from our high-level designs from the Explore Phase.

This major task consists of solution configuration, development of integration(s) and unit testing. The configuration for the State of Maine will be performed in an iterative cycle aligned to the State of Maine's release schedule.

Upon completion of configuration, the team will perform unit testing and ensure that relevant system functions perform according to specifications. Once unit tests are complete and pass, the configuration and test documentation will be base-lined, and the configuration change management process will be initiated for these items.

The table below summarizes the key sub-tasks for the build major task and associated deliverables.

Table 48. Key Sub-Tasks for the Build Major Task and Associated Deliverables

Sub-tasks	Major Task Deliverables
Configure system based on detailed design	• Configuration workbook draft • Configuration and Unit Test Results • Development and Unit Test Results
Develop RICEFW Objects	
Conduct unit testing of configurations	
Enable connectivity and middleware	
Prepare master data files (by State of Maine)	
Load master data and enablement workbook data to S2P for testing	
Conduct solution validation and confirmation sessions	• Solution Confirmation sign-off
Create training curriculum and Initiate build of training material	• Training Curriculum • Draft training materials
Confirm user access and roles	• User roles and permissions matrix

In summary, our proven experience and depth of knowledge in Cloud-based Ariba deployments supports an accelerated delivery of the build major task, while allowing the State of Maine the flexibility to make changes to the detailed design based on our iterative and collaborative approach.

Infosys Testing Methodologies

Overview

The Infosys Testing Practice will bring in best-in-class testing solutions aligned to the State of Maine's requirements. The testing methodologies are flexible enough to seamlessly integrate with the program's software development life cycle (SDLC) methodology. We understand that, the program is leaning towards the SAP Activate methodology which we believe is best suited for the State.

The key construct of our testing solution are:

1. **“test early” and “test often”** – Infosys test manager will drive the program to focus and plan towards left shifting the testing tasks and frequent testing for any iterations.
2. **Static Testing** – The 2 broad categories of testing are “static testing” and “dynamic testing”. Under static testing, which also comes under the overall “Quality Assurance Program” to be implemented in this program, it requires all stakeholders to conduct thorough reviews of all upstream work products, starting with requirements. Defects in the form of “deficiencies in the requirements” if detected during requirement phase itself, are easier to fix and less costly. It is a good practice to log all such findings in the defect management tool and track them for closure. Some of the unresolved requirements usually get deferred or come to the program as change requests during the course of the program.
3. **Dynamic Testing** – Dynamic testing includes validation of the software solution against the expected outcomes of the requirements. It requires elaborate process of test design, data set-up, test execution and defect resolution.
4. **Non-functional requirement testing** – Testing will cover the non-functional aspects of the solution to ensure they are meeting the required expectations.
5. **Test Management** – The process of managing the overall quality aspects of the project including reviews and testing activities throughout all the phases. It consists of strategizing, organizing, controlling, ensuring traceability and visibility of the testing process in order to deliver the high-quality software application.

Phases of Testing Methodology

At a high level, Infosys proposes to follow an industry standard software testing life cycle (STLC) as depicted below. It has all of the broad-based phases like Test Strategizing, Test Design, Test Execution, UAT support and Go-live/Hypercare support aligned to a typical Software Delivery Life Cycle (SDLC).

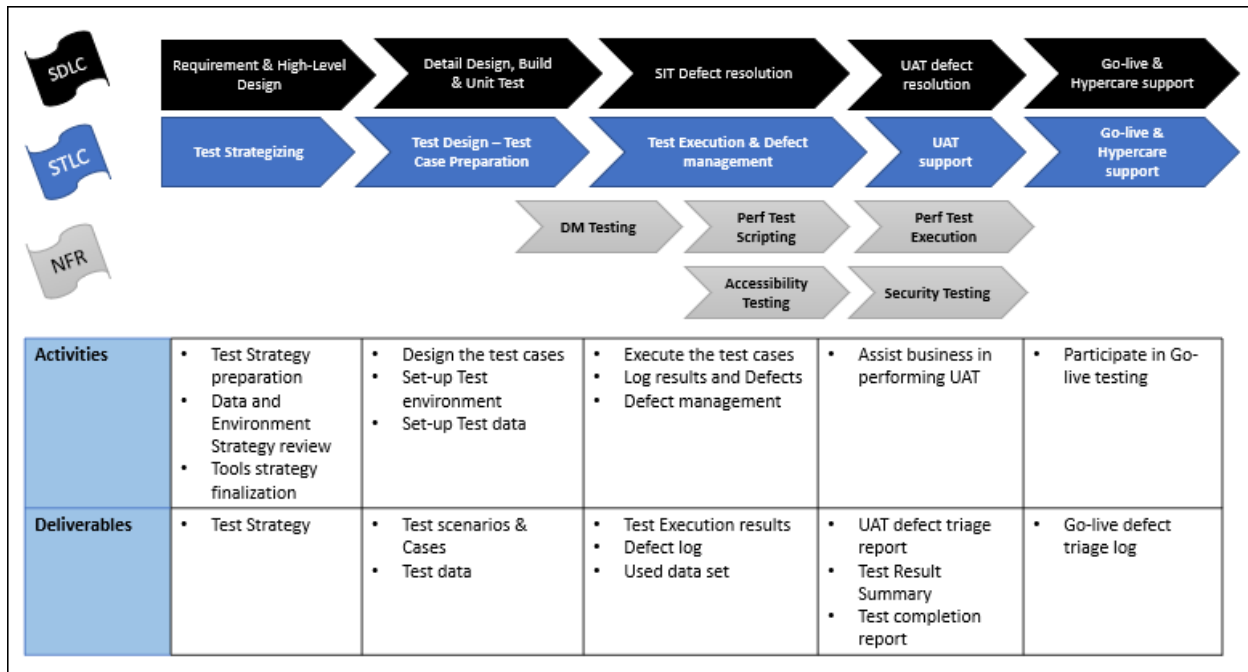


Figure 91. Testing methodology

All these phases flow in a sequence supported by well-designed entry criteria, process steps and exit criteria thereby ensuring quality outcomes at each phase of the project.

Table 49. Testing Entry-Exit criteria

STLC Phase	Entry Criteria	Process Steps	Exit Criteria
Test Strategizing	- High Level requirements are available - High Level design is available - Testing talent pool is available - Environment Strategy is available - Test data strategy is available	- Participate in requirement gathering sessions - Participate in Architecture/High Level design/JAD sessions - Conduct Test strategy preparation workshops for all stakeholders - Identify correlation/dependencies of testing tasks with project tasks	- Test Strategy is baselined - Test Strategy has all the following sections completed: - Testing Scope - Testing Schedule - Testing tools - Testing team and alignment with project team - Test environment and code movement plan - Test data set-up/refresh schedule/frequency - RACI matrix

STLC Phase	Entry Criteria	Process Steps	Exit Criteria
			Defect Management process
Test Design – Test Case Preparation	- Requirement, high level design and Test Strategy is baselined - Test management tool is set-up - Testing team has been identified and onboarded with requisite access	- Review requirements and prepare test cases using test design techniques - Conduct test design sessions within test team and with project team - Align understanding level between BA, Dev team and Test team - Prepare test data requirements	- Test cases are reviewed and baselined - Test data has been identified and available - Test execution module in Testing tool is set-up - Defect management module in testing tool has been configured
Test Execution & Defect management	- Test cases are reviewed and baselined - Test data has been identified and available - Test execution module in Testing tool is set-up - Defect management module in testing tool has been configured - Daily reporting communication template is finalized - Defect triage meetings are set in calendar - Test Environment is available and verified	- Perform test execution as per approved test cases for all positive and negative scenarios - Capture test results, screen shots - Log defects as necessary - Triage defects with BA and Dev team - Produce daily execution reports and circulate with all stakeholders - Re-test defect fixes and failed test cases - Conduct regression testing around re-test cases	- All test cases are executed and marked with status - All Sev1, Sev2 defects are closed or deferred based on Business approval - Action items are documented for any remaining open defects of Sev3 and Sev4. - Test result summary is prepared - Test completion report is prepared
UAT support	- SIT is complete - Test result summary and Test completion	- Assist business team in supplying test data - Review UAT execution results and defects	All UAT test cases are executed by business and marked with status

STLC Phase	Entry Criteria	Process Steps	Exit Criteria
	report with upto SIT phase is available		- All UAT defects are closed or deferred based on business approval - Test result summary and Test completion report are completed after including UAT status - Overall Testing sign-off given to Project stakeholders
Go-live & Hypercare support	- Testing sign-off has been received - Go-live plan has been reviewed and baselined	- Perform production validations in partnership with business - Log test results and defects - Conduct triage and resolution actions - Monitor production behaviors during hyper care phase and conduct triage sessions.	- Go-live is successful - Test results including defects are published to all stakeholders - Daily/weekly report of hyper care phase is circulated with all stakeholders

Types of Testing

Unit testing is an integral part of the development and build. The build team will verify the configurations against the detailed design. It will be executed in parallel to build activities.

System testing is a process through which the work product is validated for conformity to its business and functional requirements. The purpose of functional testing is to identify issues and defects concerning the application's functionality. The test scenarios are identified, and test cases prepared to ensure that all the business requirements are met by the solution. The coverage will be validated by the requirement traceability matrix (RTM). The test cases will be maintained in the test management tool and will be available for multiple iterations and regression testing.

System Integration Testing is to ensure the respective core functionality is integrated smoothly across multiple applications and processes. For the current solution, integration tests will be carried end-to-end among SAP Ariba, PeopleSoft, and State of Maine's existing Portal. System Integration Testing will be process-oriented and will verify if the end-to-end business processes can be supported by EPS system for various user roles and groups.

Security testing is a process to determine if an Information System adequately protects data and maintains functionality as intended. It allows an organization to accurately assess their system's security postures. Also, security testing, allows an organization to view its network the same way a potential attacker would, thus providing additional insight and advantage. Specialized testing tools such as Microfocus fortify will be used by the team to assist in identifying vulnerabilities.

Performance Testing The nature and architecture of a SaaS application already ensures to a large degree that a solution will be scalable and can handle a large volume of users, transactions, and data flows. SAP Ariba, being the largest eProcurement tool deployed in the world, has a mature, scalable architecture in place to support the State of Maine. Nevertheless, for a critical application like this, the performance of an application/system is a measure of its ability to sustain a stated quality of service such as throughput, responsiveness etc. The team analyzes the performance requirements and the

results obtained from the performance testing. Performance gaps are evaluated, and probable causes are identified. The generation of solution approaches are done and a cost effective, best solution is agreed upon and an implementation of the tuning suggestions is performed. Tests are executed again to validate the solutions and ensure the required performance parameters are achieved.

Regression Testing will be carried out to verify that application works as intended even after defect fixes during the test execution phase. As a best practice, regression testing is performed in two kinds – a subset of test scenarios executed after each code movement to test environment and a full suite of test scenario executed before approving UAT test to begin. This helps in calibrating the input and output quality of the software as it moves from Dev to SIT to UAT phases.

User acceptance testing (UAT) is the final stage of validation, performed by the business owners with assistance from our team. UAT is the final quality control procedure to determine whether the application is performing as expected, and ready for deployment into production.

Test Management Tool

Test Management is the process of managing the overall quality aspects of the project including reviews and testing activities throughout all the phases. It consists of strategizing, organizing, controlling, ensuring traceability and visibility of the testing process in order to deliver the high-quality software application. Test management tool plays a critical role in aiding the Test manager in achieving the goal. If the State of Maine or agencies have any existing test management tool, Infosys will use the same. In case the State of Maine does not, Infosys proposes to bring in Azure DevOps as a test management tool.

In this section, a few snapshots are shown as examples from the Azure DevOps tool. A more detailed demo can be arranged for the State.

Progress Report

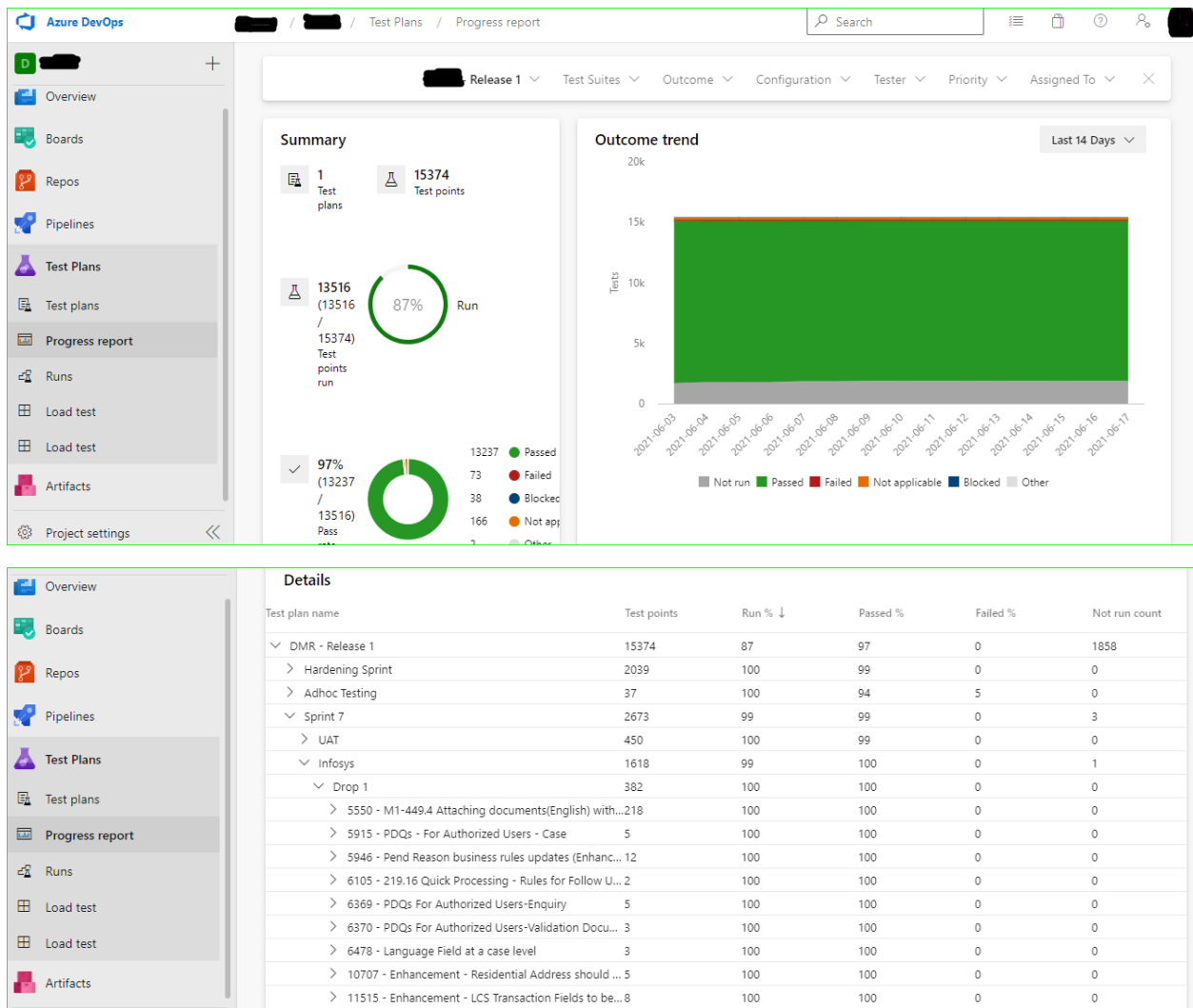


Figure 92. Progress report

Defects dashboard

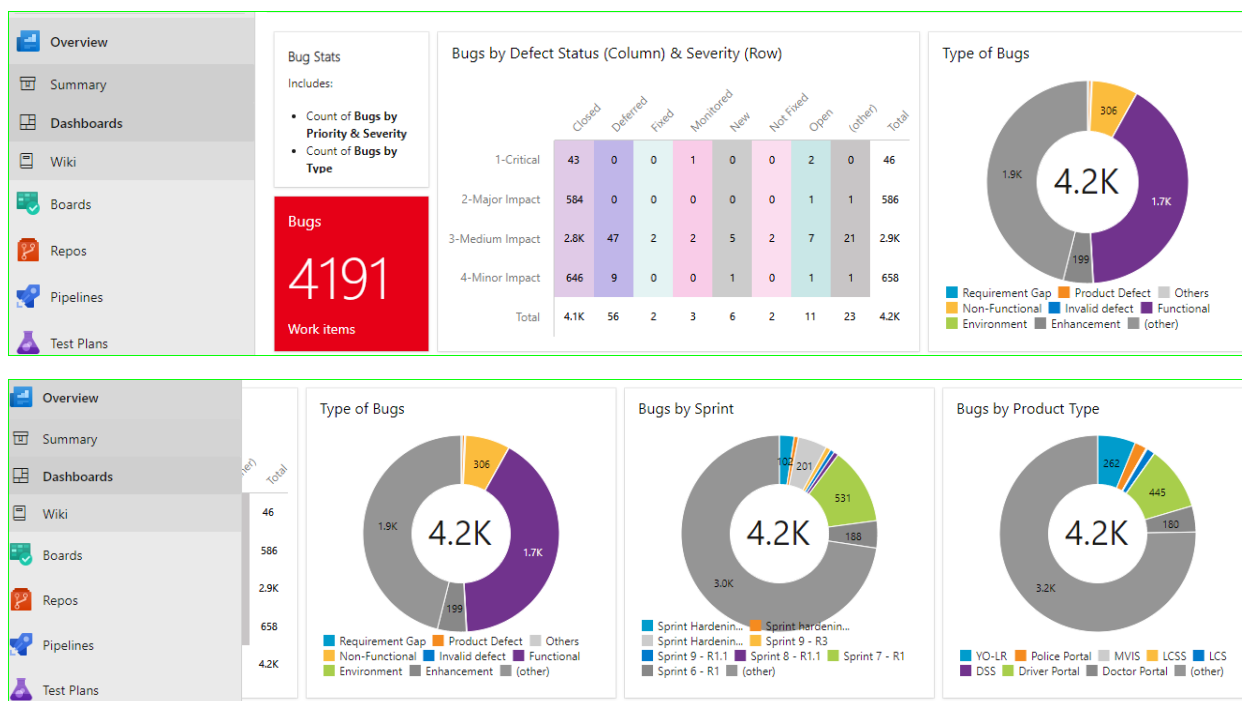


Figure 93. Defect Dashboard

Requirement Dashboard

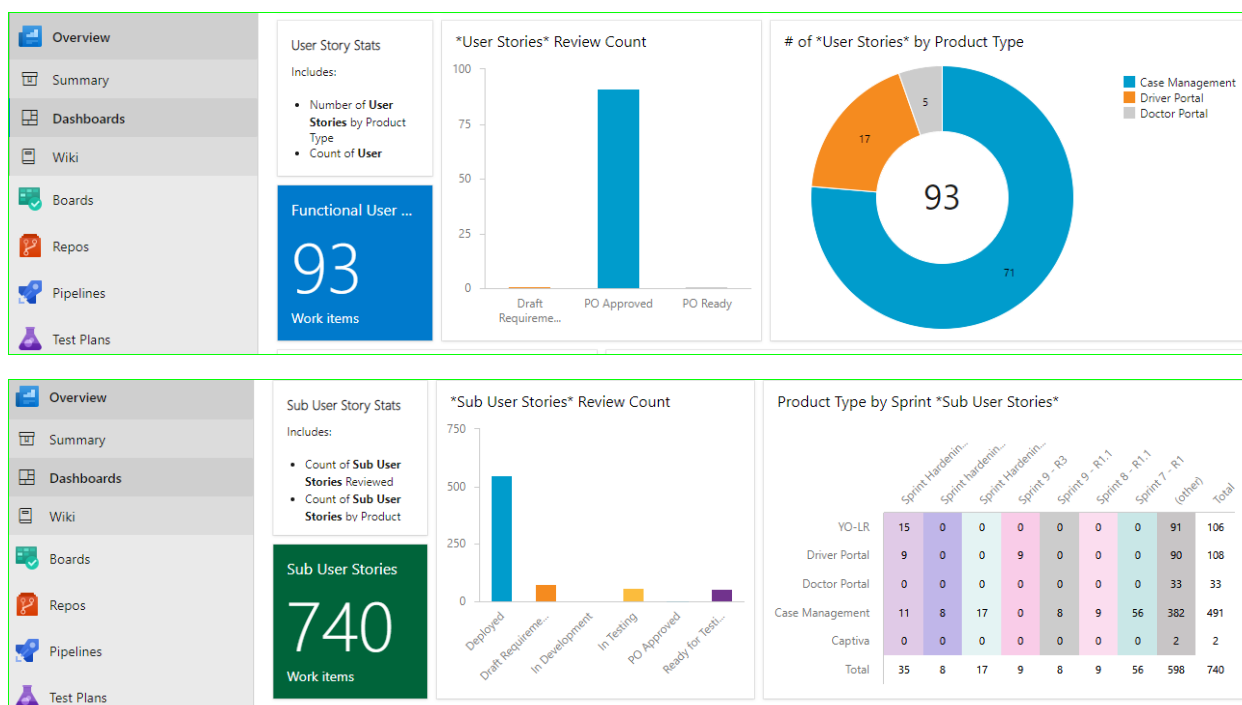


Figure 94. Requirement Dashboard

Key components of Test Strategy

Test strategy is the foundational document outlining the principles and approach of testing for the program in order to achieve the desired result of quality at a lesser cost of ownership. A well thought-out and documented strategy goes a long way in keeping the project team focused on quality from the onset of the program. Our Test manager will own the preparation of this document during the Discovery phase in consultation with all of the stakeholders. The following table provides a glimpse of

all the important sections/subsections of the Test Strategy that we found applicable to State of Maine's solution requirements.

Table 50. Sample Test Strategy Document

#	Section	Sub-Section
	Document History	
	Reference(s)	
	Definitions	
1.0	Introduction	
1.1		Purpose
1.2		Project Background
2.0	Testing Scope – Release wise	
2.1		Release1 Scope
2.2		Release2 Scope
2.3		Out of Scope
3.0	Types of Testing	
3.1		Unit Testing
3.2		Integration Testing
3.3		System Integration Testing
3.4		Regression Testing
3.5		Performance Testing
3.6		Security Testing
3.7		Accessibility (508) Testing
3.8		Data Conversion/Migration Testing
4.0	Software Testing Methodology	
4.1		Testing Schedule
4.2		Test Design Phase
4.3		Test Execution Phase
4.4		Testing Deliverables
4.5		Test Environment and Infrastructure
4.6		Test Data Management
4.7		Entry and Exit Criteria
4.8		Testing Tools
4.9		Defect Management Process
4.10		Communication, Status reporting and Dashboards
4.11		Roles and Responsibilities
4.12		Test Suspension and resumption criteria
5.0	Testing constraints and Assumptions	

#	Section	Sub-Section
6.0	Testing Dependencies	
7.0	Testing Risks and Mitigation plan	
8.0	Code promotion/migration process	
9.0	UAT Support	
10.0	Go-live and Hyper care support	
11.0	Testing Metrics	
12.0	Trainings and Knowledge Management	

Infosys Differentiators in the Testing Space

- Reusable Test Cases for SAP Ariba are available to be used for this project.
- Infosys Testing Practice is a horizontal unit and our CoE covers all types of functional and non-functional testing services, test consultancy and test management functions.
- IP solutions and accelerators are available for easy onboarding after a quick fitment analysis.
- 25000+ career testing professionals supporting 435+ clients, accounting for \$1.5+ Bn USD
- SAP Ariba CoE

DEPLOY

During the “Deploy” phase, system objects are moved to the productive environment, business cutovers are performed in the agreed sequence after business clearance, end users are trained using user story based materials, and systems are stabilized prior to handover to the production support organization.

After go-live, a portion of the project team will transition to support the system, while the remaining team members continue with the other deployments. A strict change control procedure will be implemented to keep the integrity of the system in place.

The objective of the Deploy major task is to finalize the readiness of the solution and to confirm go-live readiness for each major release. The readiness includes the technology and system, business processes and functions, organizational changes and training, deployment plan and activities, and the S2P support organizations. The go/no-go decision is critical and will confirm the readiness of the solution, and the stakeholders and/or decision-makers make the decision on whether to proceed with S2P go-live for the respective phase.

Upon successful completion of this major task, the organizational, business, functional, technical and system aspects of the project should be ready to be used in production. As noted, the deploy task (along with design validation, build and test) will be repeated for each of the five major releases into production.

The primary sub-tasks of this phase are to prepare deployment tools and processes, and to perform a timely and accurate completion of cutover to production, including manual and automated data migration.

Infosys has developed a comprehensive implementation readiness process that has a standardized review mechanism for the infrastructure/system/application changes prior to each production release. The process ensures smooth releases, minimizes potential business disruptions and keeps key stakeholders well informed.

The following is our proposed approach that describes key sub-tasks in every release. During the planning task, this approach will be refined in consultation with the State of Maine.



Figure 95. Stages of Deployment

Deployment Planning

This sub-task begins in parallel with the system testing phase in which all of the activities that are needed for deployment and go-live will be documented. Additional information related to all of the stakeholders that will participate in the deployment phase will be documented. In consideration of the policy needs, the calendar dates will be planned for the actual deployment. The outcome of this phase will be a detailed deployment plan outlining the information above.

Deployment Preparation

This sub-task ensures that all the necessary pre-requisites for the deployment are met. A checklist will be created, such as the sample list below detailing all of the pre-requisites for deployment (including the completion schedule for deployment preparation):

- Cloud production environment is ready – covered in the Solution Environment major task
- System integration testing is complete and signed off
- Security testing is complete and signed off
- Performance / Load testing complete and signed off
- UAT is complete and signed-off
- Necessary organizational changes and process adjustments are arranged
- Necessary communication has been sent to all the stakeholders
- Necessary training for State of Maine staff is complete and signed off
- Deployment plan is in place, and time window for the cut-over has been arranged
- All the operational readiness activities are complete, staff availability, and incident management tools setup

Cutover

During this stage, there are two key activities:



Figure 96. Cutover Activities

The technical promotion to production “migrates” all approved code blocks/program/software into the production environment. This activity could be performed before business go-live. Controls could be placed through user security access to prevent the usage of the production release. Promotion to production includes SAP and non-SAP objects, configuration and data. Technical readiness checklist and approvals are used to thoroughly step through each task.

Business go-live activities brings the users into the system through the activation of user profiles for each user ID. Business go-lives are tightly structured and controlled to manage expectations and timings. The critical predecessor is the end-user training and preparation for onboarding.

To allow for the promotion to production, the cutover plan will be outline steps including go/no-go decision points, responsible, migration/creation of data, and non-transportable object setup, approvals and communication/status. Each step is documented and auditable.

Hypercare

Post go-live, the project team is responsible for the resolution of any production trouble-tickets.

The final deliverable in the Deploy phase is to formally close the project. Closing out the project with sign-off verifies that all activities have been completed and validated, and outstanding issues have been resolved. In addition, the project team captures the learnings from the project and uses those artifacts in the planning of future projects.

Hypercare

☐ Work products that are additional/unique to IDEA-Activate™

Deploy Phase			
Work Streams	End User Training	Cutover	Stabilize
Project Management		- Cutover Execution ☐ - Blackout Period Management	- Production Support Oversight - Project Closure Report - Final Requirements Traceability Matrix
Process	Training Delivery Assistance (as required)	Transaction Ramp Up	Process/Functional Solution Handover
Data and Analytics		- Data Cutover into Production Environment - Analytics Verification	Report and Analytics Distribution
Technical		- Redirect Interfaces - Technology Deployment	Technical Solution Handover
OCM/Value Management	- End User Training Delivery - End User Readiness Check	Communication to Business Partners	Key Performance Indicator Monitoring

Deploy Phase			
Work Streams	End User Training	Cutover	Stabilize
	Training Delivery Retrospective		

Change Management and Procedure

The Change Control Procedure is a crucial mechanism that can affect the success or failure of this project. This process is the primary vehicle for containing scope and ensuring that management has the opportunity to make timely trade-offs between the three key project variables of cost, time and scope. It is imperative that potential changes are identified early, documented carefully, and resolved at the appropriate levels. Infosys' delivery methodology alignment to CMMi ensures that the proper recording and archival of changes happens from change initiation to closure.

Changes are defined as work activities or work products not originally planned for in the statement of work or project charter. More specifically, changes will include:

- Scope items not listed in the statement of work.
- Participation in activities not previously included in the statement of work's list of work activities.
- Provision or development of deliverables not included in the statement of work.
- A change in responsibilities, as defined in the statement of work between Infosys and the State of Maine, including reallocation of project staffing
- Rework of accepted deliverables or completed activities.
- Any State of Maine directed investigative work to determine the IDEA-Activate™ of major changes

To manage change properly, a Change Control Process will be established to identify, record, assess, and approve changes to the project. The State of Maine has defined such a process at a high level in the RFP, Infosys suggests that we use it to create a robust process to cover analysis decisions for all changes. Infosys and State of Maine will follow this process to classify, prioritize, approve, or reject changes. Change requests need to be clearly defined, including potential benefit, projected cost, and schedule implications, to allow management to make appropriate decisions. Infosys will always need prior authorization and approval of expenditures by the State of Maine before starting work on changes to scope.

At the beginning of the project, Infosys and the State of Maine management will institute a mutually acceptable change control procedure.

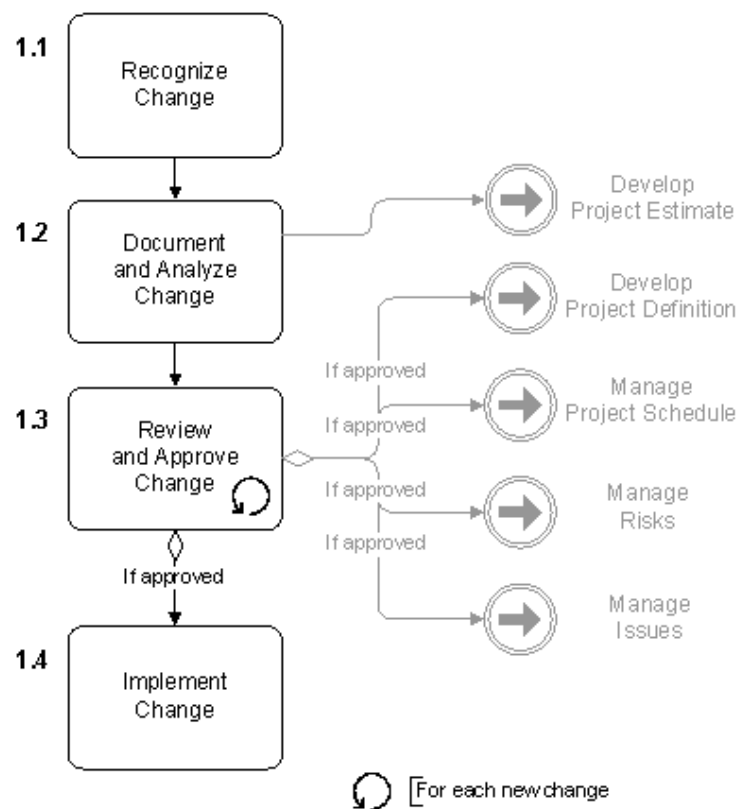


Figure 97. Infosys' Change Process

When a change of scope is identified, Infosys will prepare a change of scope document. The change of scope document may not have an IDEA-Activate™ on fees or billing but may just document a change. If the change of scope does have an associated financial IDEA-Activate™, Infosys will review the change of scope and IDEA-Activate with the PMO to determine if we should proceed with the change. If the change could replace other scope items, that would be evaluated to minimize the financial IDEA-Activate™. All scope changes require a signed change of scope to proceed with the change.

Risk Management Overview

Critical project risks that must be managed, tracked, and mitigated will be formally documented and reviewed via the Risk Register. Each risk identified will be assessed in terms of our IDEA-Activate™ implementation methodology for the impact it could potentially have on the success of the project and appropriate mitigation strategy identified.

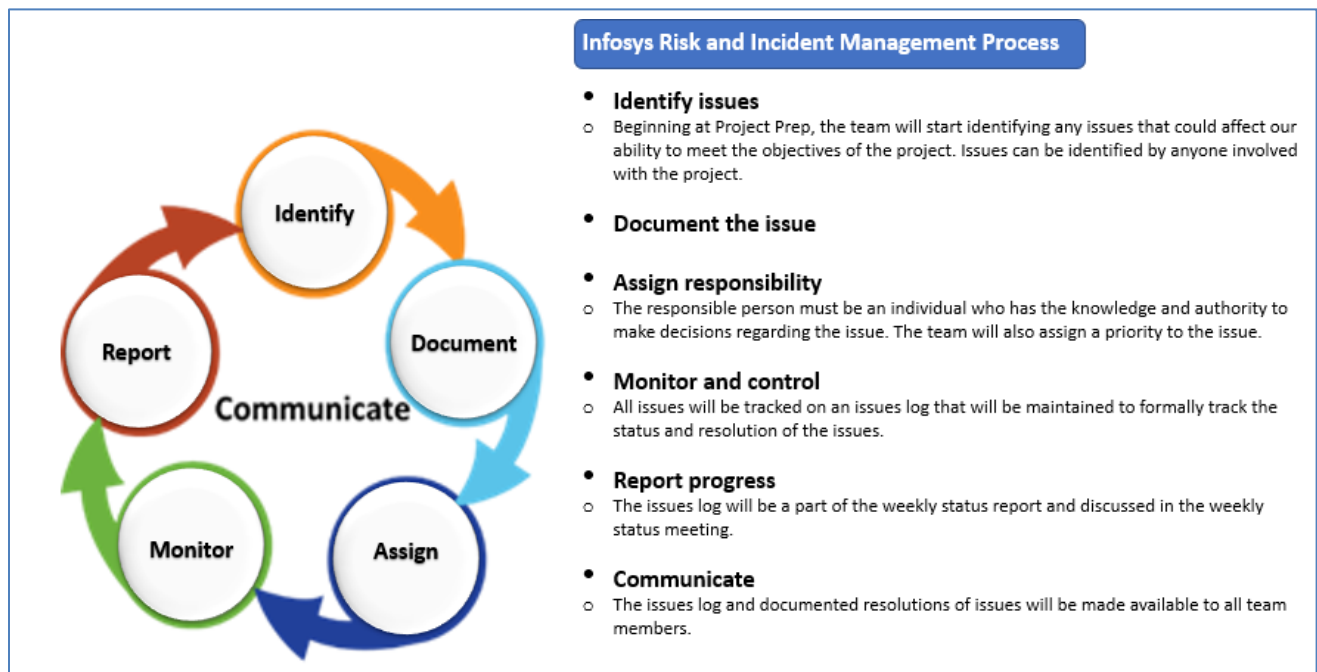


Figure 98. Risk and Incident Management Framework

Infosys PMO activities related to risk will include but is not limited to as follows:

- Define the program-level risk management plan, including risk/issue impact levels, risk probability levels, Risk Matrix (e.g. 4x4 matrix).
- Define guidelines and process to mark items from the Issue Log and Risk Register for escalation to the governance board (e.g. Manual or automatic flagging of risks for escalation to the governance board based on the risk rating).
- Conduct periodic issues/risk review meetings.
- Develop Risks and Issues Dashboard.
- Identify continuous improvement opportunities (e.g. automated notification for risks, mobility)
- The Infosys PMO will review and seek approval for the overall program-level risk management plan.
- Infosys can provide unique accelerators in the risk dashboard designs and the automation of processes related to risks (e.g. system notifications for risks nearing target closure date).



Figure 99. Example Risk and Issues Dashboard

Based upon our extensive Ariba implementation experience with clients such as, AstraZeneca, Novartis, United Health, and Freddie Mac (Fieldglass), we have identified a number of critical risks that have surfaced throughout other implementation programs:

Table 51. Common Risks from Prior eProcurement Programs by Infosys

Major risk areas for eProcurement Solutions implementation	
•	Program management – includes risks related to project schedule, resourcing, scope, benefits management, and cost management
•	Business readiness – includes risks related to buy-in for the solution, sufficient and adequate training, communication effectiveness
•	Technology readiness – includes risks related to the solution build, cloud/SaaS technology, security and master data (migration of legacy data, management of data quality, etc.)
•	Operations – risks related to ongoing service delivery after EPS go-live (applicable to each major release)

A core part of our solution is how we address these risks through our eProcurement approach, reflected in our implementation plan, and the value-added services we have included to further mitigate risk. As referenced below, our solution includes addressing key risks related to program, business readiness, technology readiness, and operations.

Issue Management

Issues are the incarnation of risks. Every project has issues that can affect progress. It is important that these issues are identified and resolved quickly by the appropriate person. The first step in effectively dealing with these issues is to make the entire team aware of the importance of identifying issues and achieving prompt and proper resolution. We will use the following procedure to track the identified issues:

- Identify issues. Beginning at project preparation, the team will start identifying any issues that could affect our ability to meet the objectives of the project. Issues can be identified by anyone involved with the project.
- Document the issue.
- Assign responsibility for resolving issues. The Infosys/State of Maine project team will determine the appropriate individual who will be responsible for resolving each issue. The responsible person must be an individual who has the knowledge and authority to make decisions regarding the issue. The team will also assign a priority to the issue.
- Monitor and control progress. All issues will be tracked in an issues log that will be maintained to formally track the status and resolution of the issues.
- Report progress on issue resolution. The issues log will be a part of the weekly status report and discussed in the weekly status meeting.
- Communicate issue resolution. The issues log and documented resolutions of issues will be made available to all team members.

In the event that an issue cannot be resolved in a reasonable timeframe to the mutual satisfaction of Infosys and the State of Maine, we will use the escalation process to escalate it to the appropriate level of management.

1.2.5.3 *Catalog Support Services*

Provide assessment to identify and prioritize contracts as potential for hosted catalog or punchout.

Contracts as potential for hosted catalog: A contract is an agreement between a buying organization and a supplier that identifies the terms for purchasing goods and services repeatedly over time.

Contract provides the discounting, pricing and payment benefits to both parties involved. Leveraging the term/ tier pricing defined in the contract terms the hosted catalog or punchout can reap out the benefits. Accurate Purchase Orders, easier compliance and more spend visibility are the main attributes in prioritizing the contracts for hosted catalogs or punchouts. Bulk or significantly procured goods or services can leverage contracts to have the high benefits.

- In SAP Ariba, item-level contracts, can be specified to generate a subscription for non-catalog items to allow purchasing users to search the catalog for the item and to automatically apply the contract terms (discounts, term/tier-based pricing) to the item.
- Subscriptions are always created for non-catalog items, fixed-fee items, cost and expense items and milestone items in a contract.

Creation of hosted catalogs

A hosted catalog is the most basic information about a seller's product; raw data such as name, description, and price. Hosted catalog data is provided to the buyer's e-Procurement system manager and loaded into the buyer's e-procurement system.

- The Ariba implementation team defines a set of validation rules for catalog fields to specify the catalog data needed from the supplier.
- Suppliers create catalog files that describe products and services and specify how to publish the catalog. Suppliers then upload the catalog files for a customer that has an active trading relationship on Ariba Network.
- The Implementation team imports the uploaded catalog.
- The team then analyze the catalog to ensure it contains the correct items, approve them and activate it so that the end users can view the catalogs. The implementation team is also able to configure automatic routing of catalogs to designated "Catalog Approvers" who can approve catalog files (post system go-live) before they are activated.
- The Implementation team can also configure how users search for items in catalogs.
- Catalog Views can be created to restrict the specific users from viewing the catalog items.

Setup/configuration of punchout sites

A PunchOut Catalog, more accurately called a PunchOut Website, is a method for a corporate purchasing agent to buy from a supplier's website from within the buyer's own procurement application or hosted e-procurement system.

- The Validation rules for the catalog items are defined by the Ariba Implementation team.
- Supplier creates an interactive website with all the products listed and create a PunchOut catalog in the Ariba Supplier Network referring to the URL of the website and publishes it.
- The PunchOut catalog is now validated against the validation's rules, and errors are sent to the suppliers to get it corrected.
- The catalog is then approved and activated by the Implementation team so that it can be utilized by the end users.
- Catalog Views can be created to restrict the specific users from viewing the catalog items.

Identify and setup commercial retail online marketplaces

Spot Buy is a feature that helps you find and buy non-sourced goods, those goods that have not been previously put under contract and likely never will be. With Spot Buy you can purchase goods within your SAP Ariba Buying solutions without the requirement to source the supplier, enter the supplier in

the vendor master, or even provide the supplier with any payment method, such as a procurement card, or invoice process.

On/off-boarding of Suppliers to prepare them to manage catalog content

Once the catalog published by the supplier, it is validated against the validation rules set, If any errors are found, the suppliers are contacted to correct those errors and update the contents of the catalog such that it clears all of the validation rules.

The contents of the catalog can also be updated by the suppliers. Once the update/ error correction is complete from the supplier, the Ariba Implementation team ensures that the updates are loaded correctly and re-approves them if applicable and then the catalog updates are visible for the end user to use.

Train Participating Entity staff to assume catalog/punchout management roles

The State's staff that have been identified to manage the catalogs will be provided with the 'Customer Catalog Manager' role in Ariba to administer the catalogs post implementation and the staff are trained on the below items:

- Setting up of the validation rules for the catalog.
- Importing the catalogs uploaded by the suppliers.
- Analyzing, approving and activating the catalogs.
- Determining how catalog items are viewed by users.
- Editing, deactivating, revalidating catalogs.

1.2.5.4 *Data Conversion Services*

Infosys proposes NIA ETL for data conversion services. NIA ETL is Infosys' proprietary tool which helps in ingesting, managing, cleansing and transforming data from any source system, this tool will meet the requirement on the data transformation/conversion of any data set (open purchase order, contract meta data and supplier master data) for the State of Maine.

Infosys Nia ETL is an Artificial Intelligence platform which collects and aggregates organizational data from people, processes and legacy systems into a self-learning knowledge base and then automates repetitive business and IT processes, freeing up human effort to solve higher-value customer problems that require creativity, passion, and imagination.

Infosys Nia Data ETL supports an intuitive web interface for building data workflows, enabling data transformation and then publishing the data across on-premises data stores in real time or batch.

It comes with a large library of extractors, loaders, transformers and filters. Data sets from different sources can be combined (join or union) and a single data set can be split and processed in multiple flows. Jobs can be exported to files and imported in another environment.

Data transformation scripts such as currency conversion which can be configured based on input data. You can also leverage workflows to derive KPIs or additional metrics. These scripts can be arranged in a required manner to create a workflow.

Infosys Methodology for Data Migration

For Data Migration, we would recommend the waterfall model, where the steps below would be part of the process.

- Plan
- Design
- Execution
- Validate

- Deploy

These would be iterative processes as the data migration is for suppliers, contracts and open PO's in the different releases.



Figure 100.Data Migration Approach

ETL Capabilities:

These offer data engineer an integrated environment for scheduling, managing and monitoring complex enterprise data workloads. The platform supports multiple data adaptors such as Oracle, Postgres, SQL server and others to connect and ingest data. Users can upload multiple files into the system by creating different data sources.

The Data ETL is a tool that can be used to transform the data and then load it into another data store. Even though regular data stores like FTP servers and relational databases are supported, it is primarily meant for big data ETL.

Conversion needs assessment:

NIA ETL is Infosys proprietary tool which will help on the validation of data for better accuracy output. We deliver 99.99% accuracy and ensure zero data loss during the entire data conversion process.

The tool has the capability to create jobs to do the validation of the developed logics before pushing it to the destination setup. This validator is used to validate based on data row count. If the validation fails, the job stops further processing and is marked as a failed job, and error resolution begins.

Conversion approach/methodology for Supplier data, Users, and active transactions including, but not limited to, open Purchase Orders, active Solicitations, and active Contracts.

As we receive the data, we perform the due diligence followed with a data profile report which identifies the key points of the data conversion. This helps us to determine the nature of the data for further cleaning and understanding the scope of work.

We use the tool by taking a sample set of data and create the job / workflow as per the requirement, we carry out the validation activity on the available sample set of data. Once we have the correct validated output, we run with the remaining data sets on these developed jobs / work flows along with the validations.

Shown below is a high-level approach for Open Transactions:

Table 52. High Level Approach for Open Transactions

SI	Rule	Invoice	Receipt	PO	PR
1	All Open transactions	All (Open and Closed) invoices for open PO's	All receipts (Open and Closed) for open PO's	All PO's that are in open status	All PR's that are in open status
		All open non-PO invoices			All PR's (Closed) that are on open PO's

Below is a high-level rule for Contracts Migration:

Table 53. Contract Migration rule

SI	Rule	Contracts
1	Open Contracts	Central Procurement Office issued, Agency issued. Data conversion of basic data from the Finance System during implementation for all Contracts

Data cleansing

This supports a library of ready-to-use complex data transformation processors, which enable fast tracking while building the data pipelines. This tool has the capability to convert any data format into one format in accordance with the requirements. Duplicate data identification is performed, and removal is done after validation.

Often, one of the main goals of performing a data conversion/migration is to combine multiple data sources into one standardized format. This is referred to as normalizing data. Data is often normalized by structuring database tables logically so that they contain information related only to the items within that table and then linking/joining tables appropriately in order to build the functionality desired by the database user. This is done to minimize unnecessary redundancy and increase data efficiencies.

RACI Matrix

Table 54. RACI Matrix

Activity	Scope			
	Responsible	Accountable	Consulted	Informed
Subject Matter Expertise	Infosys	Infosys	TBD	State of Maine
Deployment Approach	Infosys	TBD	State of Maine	TBD
Migration Strategy	TBD	TBD	State of Maine	Infosys
Process & Data Templates	Infosys	Infosys	TBD	State of Maine
Migration Plan	TBD	TBD	State of Maine	Infosys
Cleanse and Transform Data	TBD	TBD	State of Maine	Infosys
Populate Data Templates	TBD	TBD	State of Maine	Infosys
Data Integrity Testing	Infosys	Infosys	TBD	State of Maine

	Scope			
Activity	Responsible	Accountable	Consulted	Informed
Perform Corrective Action	TBD	TBD	TBD	Infosys
Data Migration	Infosys	Infosys	TBD	State of Maine

Tools/accelerators available to support data conversion.

Support for all of the major big data stores such as Hive, etc. are built in. Streaming real-time data is also supported. Our NIA Extract, Transform, Load tool has been designed from the ground up for handling very large data volumes and is built using a user-friendly web-based designer for creating the ETL jobs.

An extension mechanism is provided to create custom data processors. NIA ETL has integrated job management and monitoring features. Jobs can be run immediately or scheduled.

Additional capability of the Tool:

- Infosys NIA ETL can help with the data transformation provided the file is received and given back in a CSV/Excel format).
- The tool can be used for monthly or quarterly refresh purposes for the jobs which have been developed.
- The NIA ETL tool has the capability to develop any KPI computation field for better visibility.
- Efficiencies in removing any discrepancies in the data.
- Can handle large volume of data without any errors.

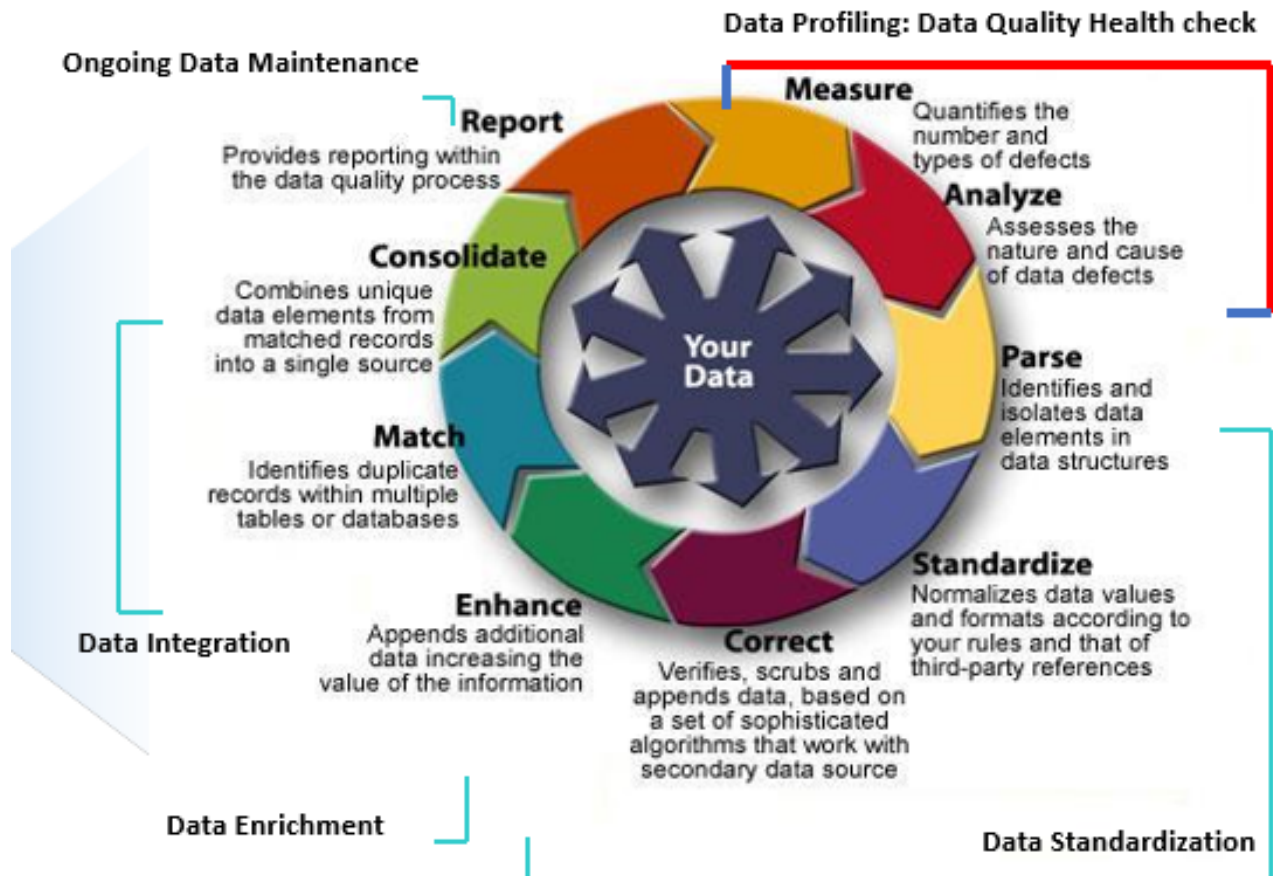


Figure 101. Infosys NIA ETL Tool

1.2.5.5 Interface/Integration Development Services

Infosys will follow our proven integration implementation approach for State of Maine.

Implementation Approach

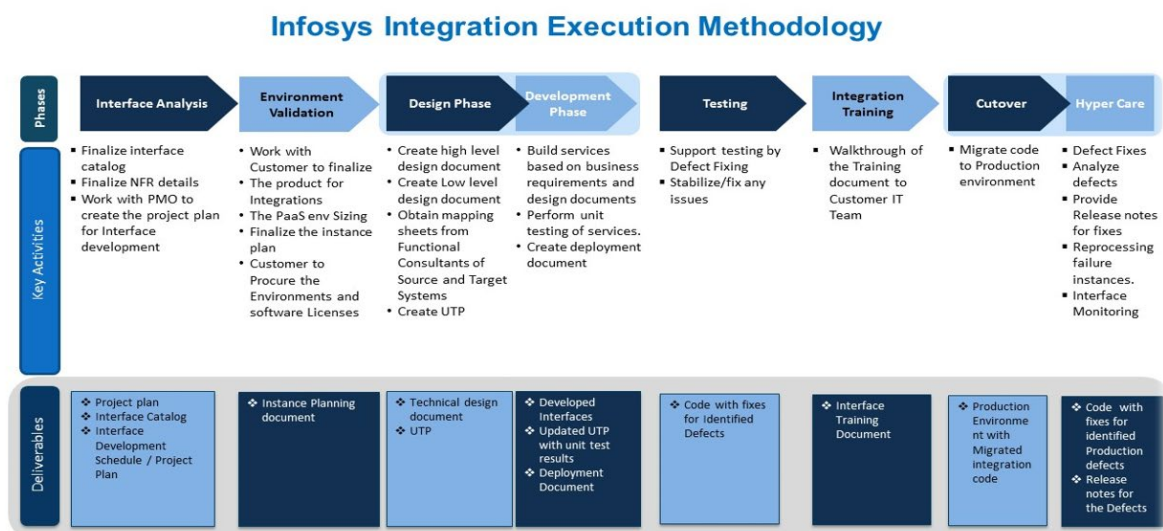


Figure 102. Infosys Integration Execution Methodology

Table 55. Integration Methodology Activities and Deliverables

Phase	Activities	Deliverables
Interface Analysis	- Finalize Interface Catalog - Finalize NFR details - Work with PMO to create project plan for interface development	- Project plan - Interface Catalog - Interface development schedule/Project plan
Environment validation	- Work with customer to finalize the product for integrations - PaaS environment sizing - Finalize the instance plan - Customer to procure the environments and software licenses	Instance strategy document
Design phase	- Create high level design document - Create low level design document - Obtain mapping sheets from functional consultants of source & target systems - Create UTP	- Technical design document - UTP
Development phase	- Build services based on business requirements and design documents - Perform unit testing of services - Create deployment document	- Developed interfaces - Updated UTP Unit test results - Deployment document
Testing	- Support testing by defect fixing - Stabilize or fix any issues	Code with fixes for identified defects
Integration training	Walkthrough of training document for customer IT team	Interface training document
Cutover	Migrate code to production environment	Production environment with Migrated integration code
Hyper Care	- Defect fixes - Analyze defects - Provide release notes for fixes - Reprocessing failures - Interface monitoring	- Code with fixes for identified production defects - Release notes for the defects

Listed below are the identified interfaces for the State of Maine implementation:

Table 56. Master Data Interfaces

Group	Interfaces	Inbound/ Outbound	Solution	Channel
Ariba Accounting Combination	Account assignment categories	Inbound	Ariba P2P	File
	Accounting field display status	Inbound	Ariba P2P	File
	WBS (Work Breakdown Structure) elements	Inbound	Ariba P2P	File
	Asset accounts	Inbound	Ariba P2P	File
	Cost centers	Inbound	Ariba P2P	File
	General ledger accounts	Inbound	Ariba P2P	File
	Internal orders	Inbound	Ariba P2P	File
	Ariba Accounting Combination Files	Inbound	Ariba P2P	File
Material groups	Commodity Code	Inbound	All	File
Currency Conversion	Currency conversion rates	Inbound	All	File
Supplier	Supplier Organization	Inbound/ Outbound	All	File
	Supplier ID	Inbound/ Outbound	All	File
	Supplier Location	Inbound/ Outbound	All	File
	Supplier Location supplement	Inbound/ Outbound	All	File
	Supplier Supplement	Inbound/ Outbound	All	File
	Supplier Remittance Data	Inbound/ Outbound	All	File
	Purchasing Org supplier combo	Inbound/ Outbound	All	File
Payment Terms	Payment terms	Inbound	P2P	File
TaxCode	Tax codes	Inbound	P2P	File
User Data Interface	Shared Users	Inbound/ Outbound	All	File
	Buyer Users	Inbound/ Outbound	P2P	File
	Groups, Roles &	Inbound	All	File

Group	Interfaces	Inbound/ Outbound	Solution	Channel
	Permissions			
SLP	Ariba SLP- RequestIn	Outbound	SLP	Web services
	Ariba SLP- ConfirmationOut	Inbound	SLP	Webservices
	Ariba SLP- RequestOut	Inbound	SLP	Webservices
	Ariba SLP- ConfirmationIn	Outbound	SLP	Webservices
Contracts/BPO	Users and Groups Info to Docu-sign	Outbound	Contracts	File
	eSignature Documents to DocuSign for signature	Outbound	Contracts	File
	Signed Documents from DocuSign	Inbound	Contracts	File
Sourcing	RFX Response to Discovery	Outbound	Sourcing	File
	Ariba Discovery Response to RFX	Inbound	Sourcing	File
	Awarding /Scoring details to Supplier Portal	Outbound	Sourcing	File

Transaction data related interfaces

Table 57. Transaction Data Interfaces

Group	Interfaces	Inbound/ Outbound	Solution	Channel
Purchase Order	Export Purchase Order Create	Outbound	Ariba P2P	Web services
	Export Purchase Order Change	Outbound	Ariba P2P	Web services
	Export Purchase Order Cancel	Outbound	Ariba P2P	Web services
	Purchase Order Header Status	Inbound	Ariba P2P	Web services
	Export Change Purchase Orders	Outbound	Ariba P2P	Web services

Group	Interfaces	Inbound/ Outbound	Solution	Channel
	Asynchronousl y			
	Import Cancel Purchase Order Status Asynchronousl y	Outbound	Ariba P2P	Web services
Receipt	Export Receipts	Inbound	Ariba P2P	Web services
Invoice	Receipt from People Soft to Ariba	Outbound	Ariba P2P	Web services
	Non-PO Invoice from Ariba (Payment Requests)	Outbound	Ariba P2P	Web services
	Payment Requests with Advance Payments	Outbound	Ariba P2P	Web services
	Invoice Remittance from People Soft to Ariba	Outbound	Ariba P2P	Web services
	Invoices from Ariba Network	Inbound	Ariba P2P/Ariba Network	Web services
	PeopleSoft to Ariba Network Remittance Info	Outbound	Ariba P2P	Web services

1.2.5.6 *Organizational Change Management (OCM) Services*

Based on our eProcurement and procurement transformation experience in the Public Sector, we understand the importance of an effective change management program to dramatically increase stakeholder buy-in, adoption and sustainment. Addressing these effectively is pivotal to achieving and sustaining the benefits associated with an Ariba implementation. To modernize each State of Maine's procurement practices and applications, robust internal change management capabilities are imperative to reduce operational risks and help drive desired outcomes and value.

Our change management philosophy is grounded in providing a human-centered experience. We do not believe that Change is managed as a mechanical, linear process that happens to people. Rather, we consider how change is experienced within an organization's culture, through employees' lens.

Our Change Experience methodology is an agile, user-centric, behavioral and insights-led approach. It will support the State of Maine's transformation, while adapting to specific regional and agency-specific nuances to deliver sustainable value and a superior workforce experience.

The methodology is grounded in the following principles that will be applied to enable a robust business transformation framework of processes, tools and accelerators tailored to each organization's needs:

- **Purposeful:** balance people's heads, hearts, and hands by constantly focusing on value-creating behaviors aligned with the "why" and "how"
- **Personalized:** insights on behaviors, needs and expectations inform better transformation interventions to accelerate adoption
- **Insightful:** data and analytics ground design and refine interventions throughout the transformation life cycle
- **Interactive:** continuous listening and responsible delivery reduces risk, increases engagement, and improves ROI

These four principles will be leveraged to create an effective and tailored change management approach and plan that will help each State of Maine adapt to and navigate through its Ariba implementation. To support this agile, complex and continuous transformation, the Change Experience approach will follow an iterative change cycle, involving the eight core change steps illustrated below.

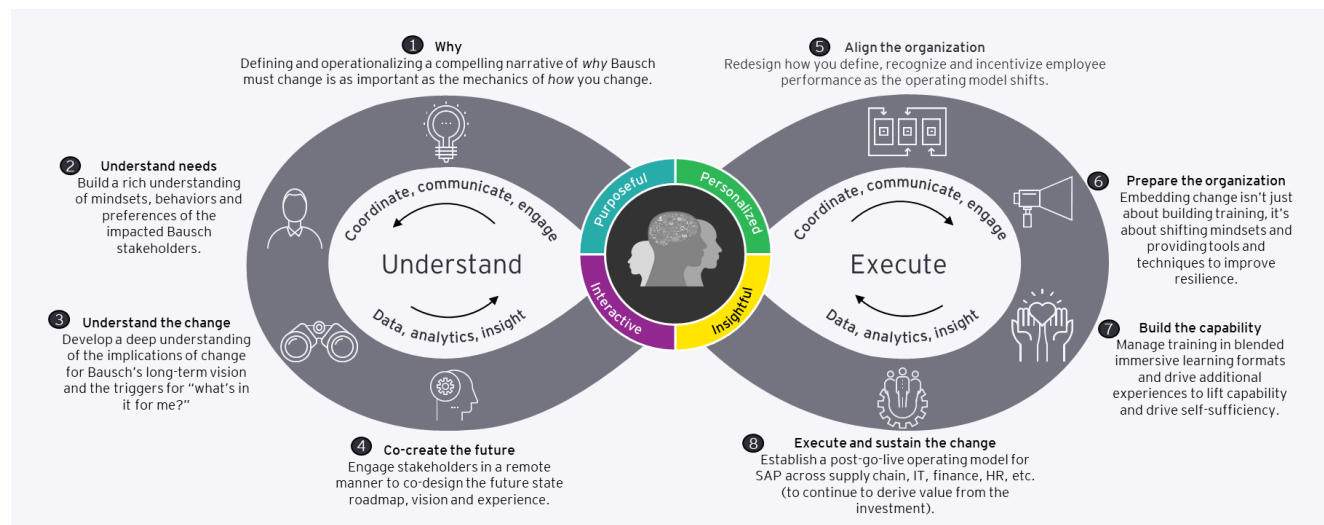


Figure 103. Change Experience Approach

Our proven change management methodology and experienced team will enable the necessary attention to organizational impact and change readiness, while partnering with the State of Maine to develop a tailored, pragmatic plan to transform procurement. Our strategic change management approach, which will be underpinned by our four principles, and will draw on six distinct dimensions: Leadership, Stakeholder Management, Communication and Engagement, Organizational Alignment, Measures and Evaluation, and Training and Knowledge Transfer.

Together, these dimensions drive effective change to reduce implementation risk and increase the value of the transformation for the State of Maine. We leverage these dimensions when partnering with our clients to actively manage change throughout the transition to the new system and the new ways of working. Our goal is to ensure that internal Change Management work streams and each of the State of Maine's unique objectives remain on track throughout the duration of the respective

projects. We will work collaboratively with the State, providing guidance through the full set of change interventions specific to the new eProcurement Ariba solution.

To ensure a foundation of simple and modern public procurement processes that can be tailored to fit any of the State of Maine's needs, we will focus on:

- **Leadership:** Leadership needs to be aligned and engaged, with roles and responsibilities clearly defined, to communicate the vision and equipped with the necessary tools and information to make that vision happen
- **Stakeholder Management:** We work to understand how each stakeholder group will be impacted by the new system, processes and any modifications to their roles with insights gained through the change impact analysis
- **Communication and Engagement:** Communicating effectively about upcoming changes to create awareness, generate enthusiasm and build a committed end user community is key
- **Organizational Alignment:** Implementation of new process and systems will have a ripple effect that may impact employee accountabilities and roles. It is important to identify how these changes will impact the State of Maine involved, and then align the organizational structure to reinforce the new ways of working
- **Measures and Evaluation:** Measuring and evaluating the progress of any new system implementation is vital to a successful project to ensure that all work stream activities are aligned, on track and the stakeholders are engaged
- **Training and Knowledge Transfer:** A key element in planning and delivering a successful transformation is transitioning knowledge and technical capabilities to the end-user post-deployment. A robust knowledge transition strategy strengthens the partnership between the program and end-users, those who will support the solution and will accelerate benefit realization

Our Organizational Change Management (OCM) Services

OCM Strategy Development

An impactful change journey is based on purpose, designed by and for the organization, and begins with the development of a change strategy and plan. Maine's change strategy will be grounded in the business case (the "why"), shaped by prior change experiences with a focus on metrics to make sure measurement of readiness and adoption is possible.

Further, the strategy we define will take into consideration each of the State of Maine's specific needs, allowing for specific tailoring to enable a successful transformation across multiple stakeholder groups. Leveraging the future state vision and quantifiable benefits aligned on by the State of Maine's leadership, we will build a comprehensive and effective change strategy that inspires and motivates people to change.

The State of Maine's change strategy will be further refined with insights gathered through leader alignment sessions, stakeholder and change impact analyses, organizational alignment sessions and the development of personas. This will lead to the development of a detailed change plan and roadmap that will pull together the right mix of core and innovative approaches, tools, and tactics to be executed at the critical times throughout the transformation.

Leadership

Any successful business transformation starts at the top, with a committed and well-aligned leadership team. It begins with a successful visioning session to align on future-state outcomes, but it is important to understand that sponsor engagement is not a "one and done" process. We will establish regular leadership touchpoints so key leaders across the impacted agency can make critical program decisions and understand the business impacts of those decisions.

We will start by understanding the ‘why’ with the State of Maine’s ‘mission’ being the guiding light for its procurement transformation. We will use our immersive and interactive technology, the EY Real-Time Collaborator Tool, to continuously engage government leaders in a collaborative and accelerated environment to drive collective understanding and alignment on the future state vision and business value, objectives and intended outcomes. The EY Real-Time Collaborator Tool enables real-time sessions using the platform’s flexible and robust brainstorming, prioritization, and assessment activities to achieve the desired session objectives.

Additionally, we know from our transformation experience that leadership’s involvement in the alignment process is not a one-time event; it must be continual and at all levels of leadership. At a more tactical level, we will not only establish regular touchpoints with leadership teams, but also assess their current understanding of the program, look at ways to support them through the change process, provide them with change leadership training, develop a leadership engagement playbook/action plans that will guide them along the change journey, and for those that elect to, we will also craft a leadership coaching plan.

Leadership Coaching Plan: A coaching based leadership program differentiates itself from other training models, as it is based on thorough scientific testing and measuring. Each of the State of Maine’s programs will be uniquely tailored to the business context and informed by their strategic intent, leadership principles, vision, mission and values. It will be based on transformational methodologies, scientific theory and experiences including:

- Neuroscience leadership
- Emotional Intelligence
- Linguistic understanding and language renewal
- Visualization of vision making it tangible, clarification of mission makes it relevant and meaningful
- Integration of values and wanted behavior based on the organization’s leadership principles
- Stress mastery, tools and techniques are added for the benefit of each leader’s sustainable high energy
- Practical and concrete utilization of a coaching approach to learning, workshops and all conversations

The benefits of the coaching are profound. Coaching greatly accelerates the rate at which an individual learns and contributes from this learning. Being coached helps a person gain vision, motivation, and skills in leading and developing oneself and others leading to a strong pipeline of leaders to take on key positions. Coaching has been demonstrated to overcome performance challenges and thereby improve personal productivity, team effectiveness & other professional relationships.

Stakeholder Management

Most large-scale transformations fail not because of the solution, but rather because of stakeholder mismanagement. There is often a fundamental misalignment between who the stakeholders are and how organizations choose to engage them. It is important to make stakeholders a cornerstone of the design experience and the change journey. A stakeholder analysis is integral in understanding how employees and employee groups have experienced change in the past and what they perceive this

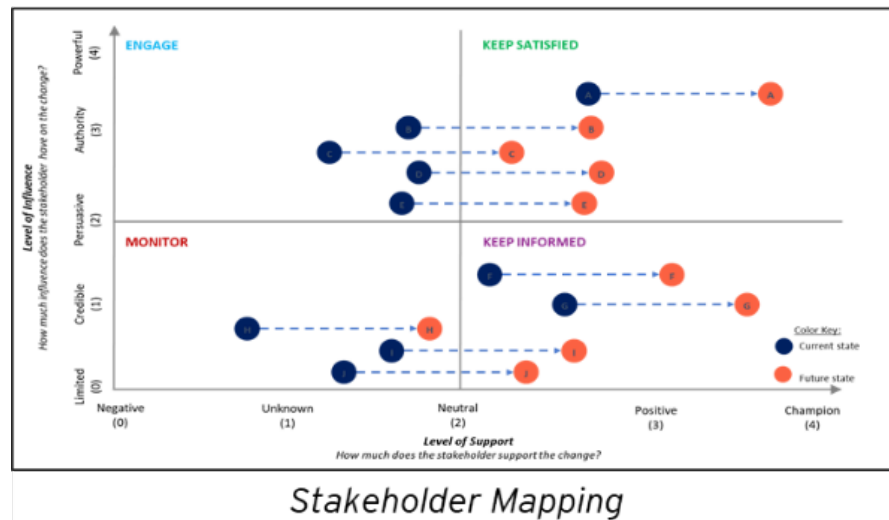


Figure 104. Stakeholder Mapping Chart

change will mean to them. Early in the Change Experience journey we need to identify the key stakeholder groups and individuals impacted by the forthcoming changes. Then we need to understand the implications of these changes, and identify the level of influence and support of key stakeholders to determine the level of engagement and involvement required to drive acceptance and buy-in.

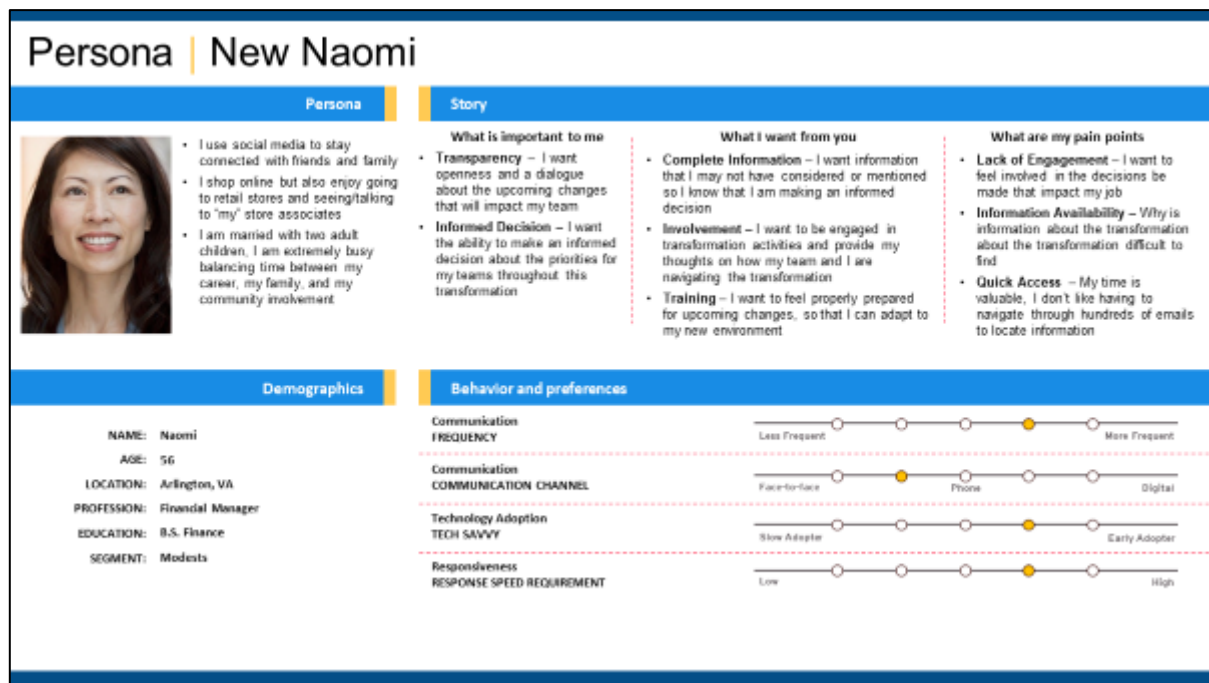


Figure 105. User Persona

Once inputs to the stakeholder analysis are organized and consolidated, personas will be built to contextualize the impact to stakeholders, which will help to articulate and communicate changes by stakeholder group in a way that resonates across the program. Personas are fictional characters created based on understood values, behaviors, beliefs, attitudes, motivations, learning/communication styles, and demographics of real users. Although a persona is represented by one character, many users can be characterized through the single persona. The time spent

developing detailed personas will enable us to design an effective change program centered around how your people work.

Drawing on the findings and insights from stakeholder interviews, assessments, and pulse survey checks conducted throughout the organization, a tailored and pragmatic initial strategy will be developed to support stakeholder buy-in and adoption of the changes for each specific stakeholder group. We will also conduct readiness and impact assessments to refine and further tailor the change strategy, taking into consideration each of the State of Maine's unique needs and requirements.

A stakeholder engagement plan will be created and tailored based on the insights gathered by the persona/stakeholder group. This document will layout activities planned to proactively engage stakeholders during the implementation lifecycle, encourage commitment and buy-in and overcome any resistance to change. A plan developed with early and ongoing engagement will also mitigate the risk of misunderstandings and rumors and provide a channel for two-way communication to help impacted stakeholders clarify, consider and accept changes. In addition to strengthening our understanding of the impacted stakeholder, the activities mentioned above will create the framework for the State of Maine's communications plan by providing awareness of the overall program and identifying preferred engagement and communications channels.

Communications and Engagement

The various assessments described in the Stakeholder Management section above, as well as the overall change management strategy, provide the foundation for the development of a communication strategy and plan. The aim of this strategy and plan is to outline communications and events for the various stakeholders involved in the implementation in an effective and timely manner. It will also be important not to overwhelm different audience segments with information. A balance between 'need to know' and 'nice to know' messaging delivered through two-way communications will need to be carefully monitored. This will be a particular emphasis while drafting supplier communications, which will seek to continuously inform and drive new supplier registration.

To develop the communication and stakeholder engagement strategy and plan, we will segment stakeholders by group. We will plan the relevant engagement and communication tactics based on the unique needs of each stakeholder group according to the project stage and execute the activities according to that plan. We will leverage our gathered insights to help define key messages, audience and timing, and use applicable existing communications channels as key communication vehicles to disseminate messages to relevant audiences. By partnering with each individual State of Maine's communications and leadership teams we will ensure that we align with each State's preferred methods and culture. All communication activities will be planned and tracked through a communication plan in order to ensure messages are audience specific and consistent over time.

Change impact analysis is about understanding the full scope of the implementation changes across people, process, technology, and policy associated with the State of Maine. This is a foundational activity for any business transformation program. Given the scale of the impact, one system change will likely have thousands of cascading effects that — if not identified, monitored, and addressed — can serve as barriers to a full transformation. Therefore, business readiness begins early through the identification of these impacts.

When capturing key data points related to change, impacts should be categorized by degree of difficulty. For an impact rated as Low, for instance, a message from the communications team to the impacted party may be all that is needed. A medium-to-high impact, however, may require an adjustment to the operating model, organization roles, or even organization culture over time. Medium to high impacts often require more extensive hands-on approaches that include change activities that are more tailored and personalized to the impacted user group. Below is an example of what these change impacts might look like, and how they might be categorized. Capturing impacts in this way will

create a solid framework and data foundation for change impact assessment that will enable a more credible, focused, and ultimately successful transformation process.

Evaluating the Magnitude of Change Impacts			
	High	Medium	Low
People	Employee(s) job title or BU/Function is modified, resulting in major changes to roles and responsibilities	Employee(s) job title or BU/Function is modified, resulting in minor changes to roles and responsibilities	Employee(s) job title or BU/Function is slightly modified with few, if any, changes to roles and responsibilities
	Perception that there is a significant increase or decrease in work	Perception that there is some increase or decrease in work	Perception that there is little increase or decrease in work
	High level of technical or functional training needed for a particular group	Moderate level of technical or functional training needed for a particular group	Light level of technical or functional training needed for a particular group
	Significant shifts in accountability (loss of autonomy, responsibility, decision making, or possible organization structure changes)	Moderate shifts in accountability or reporting (loss of autonomy, responsibility, decision making, possible org structure changes)	Small shifts in accountability or reporting (loss of autonomy, responsibility, decision making, possible org structure changes)
Process	Processes were not in place and are currently being defined	Processes were inconsistent, not documented in many cases, and will move toward consistency	Processes were consistent, but not documented, and will need to be documented
	Significant increase in cross-functional work required	Moderate increase in cross-functional work required	Light level of cross-functional work required
Technology	Shift from manual work to automation	Shift from moderate technology use to job enabled by an enterprise wide technology	Shift from using a shared site on a daily basis to using a standardized technology tool
Policy	New policy or significant change to a policy that fundamentally changes a process and requires awareness	Moderate change to an existing policy that requires/removes part of an existing process	Minor change to policy that does not have an operational impact

Change Impact Analysis

Together we will aggregate and monitor system transition impacts to evaluate and sharpen our focus on business readiness. We will leverage a change impact assessment template that will allow us to provide a consolidated and transparent view of the people, process, technology, and policy impacts that will need to be addressed in the future state. Having one centralized location where this information is tracked and recorded will improve ownership, accountability, and consistency of addressing the impacts identified. The Change Impact Assessment will be critical for making go and no-go decisions related to system releases and will therefore be treated as an integral part of our change program activities.

Organizational Alignment

With any large-scale procurement implementation, operating model and state-unique organizational changes are inevitable. We expect roles to change, work to shift between roles, and tasks possibly eliminated as a result of automation. Role and work shifts mean operating models and organization structures could differ from the State's. The State of Maine may envision the distribution of work between functional centers of expertise and back-office functions differently.

We will share operating models and organization design leading practices with all of the necessary stakeholders and we will collaborate with the State on high level, future state operating models and organization structure alternatives that drive efficiencies and align to the new technology. It is assumed that the State will own their own organization design changes, guided by principles established by Sponsor Executives. These options will contain key assumptions, headcount, spans and layers, and potential savings information with pros and cons.

Measures and Evaluations

Measuring and evaluating the progress and execution of any new system implementation are vital to a successful project to ensure that all work stream activities are aligned, on track and the stakeholders are engaged. Our change readiness approach, combined with baseline process performance measurements, is a key enabler for effective management of change readiness. Change readiness assessments will be conducted, as required, throughout design and testing phases for each release milestone prior to go-live, in order to understand the levels of stakeholder change readiness and impact on systems, processes and people. Ultimately, assessments will help to identify adoption risks to be mitigated and other issues/barriers that can be proactively managed prior to implementation.

The assessment can be executed in multiple ways, including surveys, interviews/focus groups, and additional leadership interviews.

Lack of readiness, training, and learning are the most common reasons why large-scale system-enabled transformations fail to deliver expected business outcomes. Business adoption is about making sure employees understand and adapt to a new way of working, fully sustaining the desired changes in the long run. We will bring the State of Maine's staff into the journey at the right time and with the right skills to maintain or exceed customer service levels throughout the implementation lifecycle.

We believe in continuously measuring business adoption. Simply put, what gets measured is what gets done. Rigorous metrics management and tracking are prerequisites to achieving anticipated business outcomes. We will work with the State of Maine to co-develop metrics that enable the right interventions. Our adoption approach includes the following phases:

- **Identify** — using our Change Impact Analysis, we will identify which new ways of working need to be adopted to realize targeted business outcomes. We will also determine which data points and/or information can be collected to measure if the new ways of working have been adopted. Lastly, we will work with the PMO and technical teams to determine the timeline and performance expectations by which stakeholders must demonstrate adequate adoption. In this stage, we will create an adoption template, with defined adoption measures, expectations, and timeline.
- **Collect** — we will begin to collect the quantitative and qualitative data available to the team as outlined in the defined adoption measures. We will then consolidate and synthesize the data into actionable next steps.
- **Analyze and Monitor** — we will use captured information to develop and track organizational readiness metrics using scorecards and dashboards. We will monitor adoption against agreed-upon Key Performance Indicators (KPIs) and Key Behavioral Indicators (KBIs) and, based on analysis, update stakeholder support resources, training plans, and communications as needed.

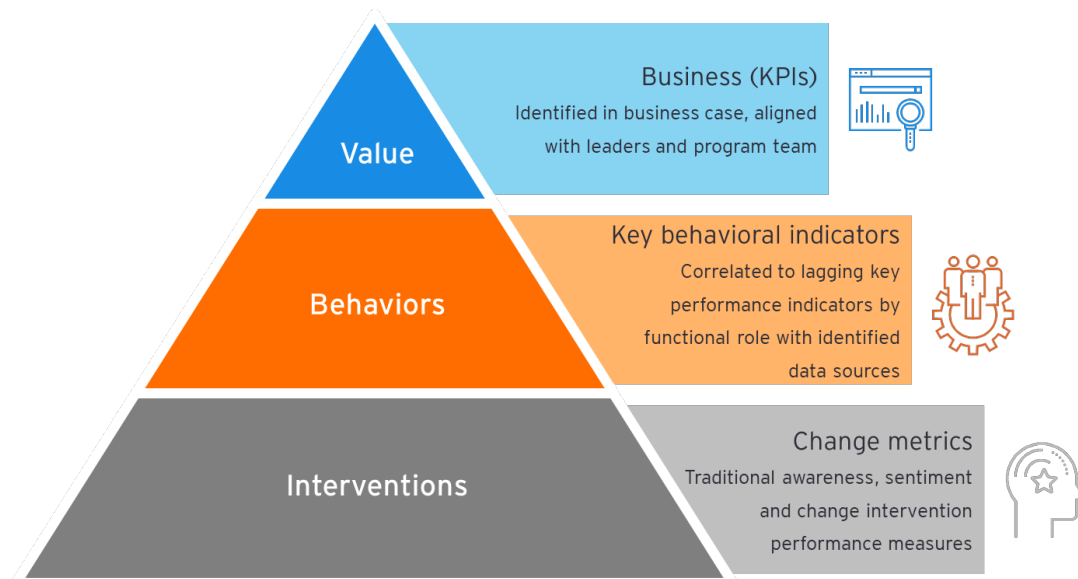


Figure 106. Measurement and Evaluation Hierarchy

We will maintain an agile and user-centric adoption strategy so that we can adapt as we move forward, based on real data and actionable insights. Our approach to change provides the necessary data to prioritize adoption measures that have the most significant impact on the program's expected business outcomes. We believe in partnering with business leadership to embed adoption measures into

program performance expectations, and we will regularly review these measures to understand continuous improvement opportunities. Where possible, we balance manual and automated data collection.

These activities will support the technical transformation by creating comprehensive visual dashboards and scorecards that track adoption and benefits, monitor behavioral changes, accelerate the transition to “business as usual” all while providing lessons learned for future transformations. It is also key to conduct a resistance assessment to determine which functions, and which key stakeholders will be impacted by any possible change.

Training and Knowledge Transfer

To align with the change management strategy outlined above, we will approach training for the State with the following key tenets in mind:

- **Listening and Engagement:** Our team will engage State of Maine sponsors, project team members, and other key stakeholders early and often to gain perspectives on “what successful training will look like” – as well as to build support and enthusiasm for the training to be delivered
- **Delivery and Interaction:** It is important to build training content with the end-user experience in mind (“how do I feel about what I am learning?”; “how will my work change?”; “what do I need to do differently?”) while maintaining flexibility to accommodate changes in approach or direction that may require amendment to training content before it is delivered
- **Content Retention:** We will maintain a relentless focus on clarifying, updating, and incorporating the right knowledge, skills, and procedures to build training on the procurement solution and new ways of working that enables Department employees to succeed in their work after training is delivered – while still being flexible to incorporate new knowledge where necessary (if training requires updates or remediation to confirm all participants are confident in their new skills)

For a detailed explanation of our training approach, please refer to Section 1.2.5.7 Training Services.

As mentioned, the change management approach explained above will be underpinned by our Change Experience Guiding Principles (i.e., Purposeful, Insightful, Personalized, and Interactive). Each principle is human centric, geared towards driving the best and most effective outcomes. Our purpose is to align ourselves with the State’s mission, and to work effectively in helping them reach their goals. We will provide insight, that will help hone and focus the program as it progresses. We will customize our interventions and interactions to fit the specific needs of Maine. Finally, our interactive approach means that we will continuously enhance our approach throughout the roll out of the solution, which will drive more efficient outcomes and further improve ROI.

We propose that the State have a senior executive designated as the Change Management Sponsor, as well as an experienced Change Management and Training Lead. The Change Management and Training Lead will have a specific focus on the quality and success of the “people” side of the Procurement transformation. The Change Management and Training Lead will be supported by our OCM and Training team comprised of a Change Management Lead, Stakeholder and Communications workstream, Organizational Design workstream, and Training workstream.

Day-to-day management of change management and training activities will be overseen by our Change Management Lead, who will be responsible for executing activities in alignment with the change management approach and change experience framework. Each workstream lead will be responsible for managing their workstream’s activities and reporting back to the OCM lead on progress. For example, the Training Lead will report to the Change Management Lead and will provide updates on progress regarding training strategy development, curriculum creation, trainer preparation, and content determination – as well as collaboration on the assignment of end users to required

training modules. Providing additional support to the overall project will be training developers who will provide training content design assistance for the SAP Ariba components, leveraging EY's leading practice approaches to training development and capabilities.

1.2.5.7 Training Services

Prepared end users make the difference between meeting or exceeding desired outcomes. We know from our experience in the Public Sector that even the best-designed solution will not realize its full potential if end users are not trained properly. With this in mind, we will develop a coordinated, robust training approach specifically for this Public Sector transformation. Our innovative approach to learning allows us to focus on building training that considers the “human experience” for all employees and other impacted stakeholders. This approach facilitates higher employee satisfaction with the training delivered, greater adoption of new tools, and skills after training is complete – and in turn, a much better return on investment in staff development.

Our Training Approach

Based on our expertise in the Public Sector and in procurement related implementations, our training approach is aligned with the project life cycle and the recognized industry standard ADDIE model. Our training team will follow this approach throughout the project life cycle:



Figure 107. Training Approach

Analyze

We gather information from the future state process documents to understand who will perform specific tasks in the new systems and verify tasks that a particular stakeholder will perform. We also work to understand the unique requirements that the State of Maine has – including regulatory and geographical – and tailor the training strategy and plan to support those needs. These insights will be used to create a holistic training strategy that ensures that we are building the right training for the right audiences at the right time. The development of this training strategy will include an assessment of needs by stakeholder group or audience. A training needs analysis will be developed to identify and document who will be impacted by changes the Ariba solution will enable. In order to provide end users with the most appropriate learning experience, we will leverage our Public Sector expertise and accelerators to design and deploy content that is benchmarked against “future-focused” capabilities, tailored to the needs of end users and their roles, combined with coaching and mentoring opportunities, and ultimately, positioned to encourage greater employee engagement and improved performance metrics.

Training Needs Assessment: We will apply our training strategy to each of the user groups identified below to determine the most optimal training curriculum and plan for each:

- End Users
- Train-the-trainers
- Suppliers
- System administrators
- State of Maine Help Desk Staff

Each user group will have unique training needs and contexts (shown in the below table), requiring a training approach that can address their needs using the right tools at the right time. The training scope will cover changes in systems, processes, roles and accountabilities. Training will also cover a

holistic view of what is new, what the changes mean to each end-user, and what to start, stop, and continue doing.

Table 58. User Group Training and Regenerative Needs

User Group	Initial Needs	Regenerative Needs
End Users	- Log on, navigation of and how to find help/further information - Material and services masters and catalogues - Sourcing, RFx management, contracting for goods and services - Supplier scorecards and management - Supplier Enablement and Performance Management Projects	- Tips and tricks - Process variations and irregular processes - Periodic reminders and refreshers - Release changes - Performance driven topics - Training for new access rights due to promotion or new joiner
b) Train-the-trainers	- Log on, navigation of Ariba as appropriate, and how to find help/further information - Goods and services requisitions and orders - Approvals of goods and services	- Tips and tricks - Process variations and irregular processes - Periodic reminders and refreshers - Release changes - Performance driven topics - Training for new access rights due to promotion or new joiner
c) Suppliers	- Log on and navigation of Ariba functionality (Ariba and Fieldglass) - New processes and activities – relevant to the suppliers	- Tips and tricks - Release changes - Access to information through integrated portal
d) System Administrators	Viewing, opening, and closing tenders	Access to information through integrated portal

User Group	Initial Needs	Regenerative Needs
e) Help Desk Staff	- Log on and navigation of Ariba and how to find help/further information - Knowledge transfer of functional designs, administrator role and activities	- Issues, workarounds and detailed release information - Release changes - Performance driven topics - Changes to processes, workflows, or data requirements

Identified User Group and Training Needs

Design

Our experience with providing comprehensive training programs for a wide variety of state and local government organizations has enabled us to establish a consolidated set of design principles which we leverage as we collaborate with agencies to meet their training needs. As we design the training program for the State of Maine, we will consider the following:

- Training content should be developed in a way that demonstrates a holistic view of the learning objectives for each impacted audience
- Training will be created with a keen focus on how the agency wants to improve State employee experiences and the corresponding skills that will enable the agency's staff to meet and exceed expectations in their roles
- Content for training should be designed in the context of the State of Maine's current environment and what will likely need to change and/or improve for employees on an individual level –so that they are personally committed to understanding and adopting new practices, policies, and tools
- Training content should include examples or “scenarios” which are relevant to employees, reflecting real cases and work experience scenarios that would seem logical and reflect how they work on a day-to-day basis
 - For procurement process training, as an example, we can incorporate metrics on employee and vendor interactions, as captured in previous or new surveys, as deemed appropriate
- Quick reference guides should be created to supplement training courses, and a variety of innovative development methods should be used to adjust to varied learning styles throughout the organization
- As available and relevant, future state process flows, leadership expectations for growth and improvement (i.e., increased metrics on meeting customer or constituent needs) and other similar content should be leveraged to build training scenarios, quizzes, assessments, and other materials

Leveraging these principles, we will collaborate with the State to develop a customized training curriculum (to address ‘what’ and ‘for whom’) as well as a detailed training plan (‘who’, ‘what’, and ‘when’), which will also define training data and training environment requirements, and align on method of delivery, format, and logistics.

Training Curriculum and Plan Development: Our modular approach to training design will allow the State of Maine to make agile updates to training that will keep materials up to date with less effort. We know that from our experience in the Public Sector, a successful learning experience starts with

creating a meaningful employee experience. In order to improve the employee experience, our approach does not just focus on delivering training courses, but rather leverages training as part of a holistic employee engagement strategy (see diagram below). This approach will allow us to work with the State of Maine throughout the implementation to facilitate high engagement and motivation for use of the new solution – which will enable stronger alignment to the new solution utilization objectives, increased employee motivation, and more targeted training delivery to address both employee and vendor customer service needs.

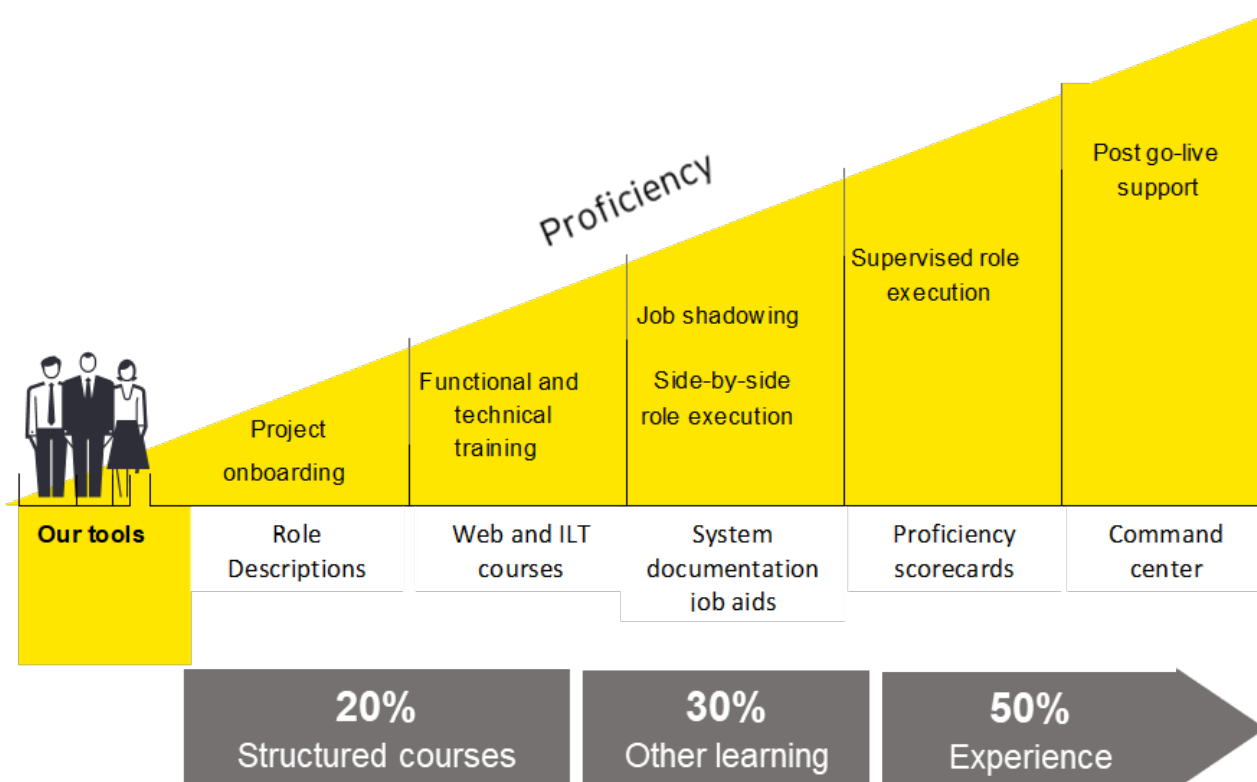


Figure 108. Employee Engagement Strategy

Additionally, by gathering data on both the vendor and the employee experience throughout the implementation, we will work with the State of Maine to design a curriculum that meets the needs of its employees and vendors to create personalized training materials that closes any gaps in employee and vendor experiences with the Maine's eProcurement solution.

We understand that adult learners have different learning styles and training needs. Our training approach involves assessing these needs and creating personalized and scalable training plans that incorporate a variety of channels. We will work with the State throughout the implementation to create training plans that address different learner needs and provide training at an appropriate frequency to align to implementation milestones, as well as creating immersive self-service offerings that allow the State of Maine's diverse stakeholders to improve their experience.

Provided below is an example of a high-level training plan by stakeholder group for an Ariba implementation. This training program includes a combination of in-person and virtual instructor led training.

FileHomeInsertDrawPage LayoutFormulasDataReviewViewEY SupportHelpPower PivotPDF-XChangeSearchShareComments						
G2						
	A	B	C	D	E	F
	Course Number	Title	Duration (Days)	User Group	Venue	Description
1	AR110	Event management (RFP START TO FINISH)	1	Sourcing Professional	Classroom or Virtual Classroom (eLearning no longer available)	This course introduces you to the basic functionality of SAP Ariba Sourcing. Through a combination of lecture, demonstrations, and lab exercises, students learn about the various types of sourcing events. This one day course covers template selection, setting event rules, monitoring supplier activity, and making manual award proposals within the system. Students perform hands-on lab exercises that include creating, publishing, monitoring, and completing a sourcing event.
2	AR111	Project management / event management	2	Sourcing Professional	Classroom or Virtual Classroom (eLearning no longer available)	In this course, students learn about the SAP Ariba Sourcing solution through a combination of lecture, demonstration, and lab exercises. Students will see how SAP Ariba Sourcing is designed to make sourcing project management faster and easier through the use of many features, including best practice templates and automated task reminders. Students also learn how to create a sourcing event as well as publish, monitor, and award the event.
3	AR211	Contract management (CLM)	2	Sourcing Professional	Classroom or Virtual Classroom	In this two day course, contract authors learn how to use the SAP Ariba Contracts solution to create and manage contract agreements. Through a combination of lecture, demonstration, and lab exercises, the course covers all processes of a typical contract agreement, including creating, processing, negotiating, approving, amending and closing the contract agreement. Students learn how the clause library and project templates expedite the contract creation process while simultaneously insures conformance to their organization's business processes. Other topics include how to search the SAP Ariba Contracts repository, as well as how to run prepackaged contract workspace reports. Lab exercises are highly emphasized to provide significant hands-on experience in the classroom.
4	AR231	Contract authoring	1	Sourcing Professional	Classroom or Virtual Classroom	This course explains how to prepare master agreement templates in SAP Ariba Contracts with Enhanced Contract Authoring. Through hands on labs and exercises, students learn how to create, use and manage the clause library in SAP Ariba Contracts. The course also covers best practices for identifying common clauses to include in the library, how to structure the library for ease of use, and how changes to the clause library affect templates.
5	AR330	Supplier lifecycle	2	Sourcing Professional	Classroom or Virtual Classroom	Students learn how to use SAP Ariba Supplier Lifecycle and Performance to enhance their organization's supplier management. This course is intended for business users who will be creating and managing suppliers for their organization, and for administrators who will be managing their organization's supplier project templates. Through a combination of lecture, demonstration, and lab exercises, students learn how to create and manage several types of supplier projects and their corresponding templates.
6	AR340	Supplier risk	N/A	N/A	N/A	N/A
7	AR510	Buying (REQ TO PO) (I think - it might cover invoice at a super high level)	2	Requisitioner & Sourcing Professional	Classroom or Virtual Classroom (eLearning no longer available)	This course covers all of the functions of SAP Ariba Buying related to the creation of requisitions, the issuing of purchase orders, and receiving against purchase orders. The training material discusses the business processes automated by SAP Ariba Buying, and explains how to use each feature. A mix of lecture, demonstrations, and lab exercises facilitate the learning process.
8	High-Level Training Plan					

Figure 109. Training Plan Summary

Ongoing performance tracking and monitoring will be deployed, as this will help identify where interventions are needed to address customer service quality, re-training needs, and identify scenarios that require more hands-on training opportunities, such as job-shadowing, scenario-based training, and simulations.

Develop

Training materials are developed with fit for purpose, agility, and longevity in mind, with an emphasis on building proficiency in critical processes. Our past Ariba implementation experience will enable us to leverage highly effective Ariba related material as we develop tailored and comprehensive training content for the State of Maine. We will also incorporate industry leading, innovative tools to develop content in newer, digitally-enabled formats – which will provide a blended learning model that enhances variety for your audiences and meets the needs of different learner types. These formats and tools could include but are not limited to the following:

- Instructor Led Training (In-person & virtual) – Interactive training content developed to be delivered by a live trainer.
- On-Demand Training – Recorded training webinars designed to be delivered through a self-guided learning approach.
- Micro Learnings – Content that's delivered to users in small, very specific bursts with tools such as SnagIt Videos, among other highly visual formats.
- Community Forums – Organic, self-powered community where users can answer questions, help solve problems, and generally make life more “secure” for each other (leveraging tools such as Teams, which can be accessed on smartphones, tablets and PCs can be leveraged to share ideas across diverse stakeholder groups).
- Gamification – A powerful tool when building and delivering successful, high-impact trainings and assessing results, focused on interactivity and active learning (including word puzzles, quizzes or other creative formats).
- Digital Quick Reference Guides – Tools leveraged when building and delivering successful, high-impact trainings, focused on active learning (including interactive PDF self-paced

trainings and quick reference guides).

Implement (Deliver)

Our implementation approach will involve the deployment of interactive and web-based courses, coordinating instructor-led training (ILT), as well as delivering a train-the-trainer program. This phase will include the following steps:

- Identify and train instructors via a train-the-trainer session (if applicable)
- Edit / finalize training content
- Pilot test training materials (as denoted above)
- Finalize and prepare detailed logistics
- Deploy and ensure delivery of training to all impacted audiences utilizing the TTT approach
- Capture feedback on relevance of content and quality of training delivery format as applicable

Train-the-Trainer (TTT): Live and virtual training delivery will be supported through a train-the-trainer approach that includes using highly skilled, multi-jurisdictional State of Maine resources, supported by project team members with in-depth knowledge of the system and subject matter experts from the Ariba team. Together with project resources, these individuals will train the over 25% of the end users of the State of Maine that must be upskilled in approximately six months.

Our goal with train-the-trainer (TTT) is to prepare the State of Maine trainers to deliver the courses to end users, as well as support refresher training and post-go-live activities. Our TTT materials bring together the training content developed as part of each functional tower into a cohesive and consistent course structure. We deliver TTT sessions to provide the identified training developers, trainers, and training support resources the skills and knowledge required to deploy effective training. Our TTT program and materials will help drive the effectiveness of your trainers, build skills, and capabilities within your workforce, and enable trainers to thrive as subject-matter resources when they transition from the project back to the agency.

Evaluate

The quality of materials and execution of training delivery cannot be confirmed without an appropriate evaluation of the training program. We will collaborate with the State to develop a training feedback survey, analyze the data collected, and update training materials and delivery approaches going forward based on input provided.

Post Implementation and Transition Plan

Based on our Public Sector expertise, we know that a key element in planning and delivering a successful transformation is transitioning knowledge and technical capabilities to the end-user on a just-in-time basis. A robust knowledge transition strategy contributes to a positive change experience, strengthens the partnership between the program and end-users, and accelerates benefit realization.

However, knowledge transition is not something that happens only at the end of the project. We will educate key Ariba stakeholders on information such as major design issues, new business processes, and technical aspects of the system through each phase of the transformation. Our organizational change strategies and tools are vital inputs to our knowledge transition plan, helping us identify super users, understand where pain-points exist, and tailor our training strategy. The knowledge transition workstream will use the State of Maine's project team, Subject Matter Experts (SME), and Ariba workstream leads to build the skills and capabilities needed to support and sustain change.

Early in the project timeline, we will develop a tactical knowledge transition plan, relying on our change strategy to guide its development and determine the most optimal tool to record the critical conceptual and procedural knowledge of super users to preserve organizational knowledge for future users and

phases. This plan will be adaptable to different learning styles, accounting for visual learners (seeing), tactile learners (doing), and auditory learners (hearing). We will bridge the current-state and the future-state by creating journey maps for different learner groups, adjusting along the way to ensure that stakeholders are consistently engaged throughout the transformation.

The overall objective is to provide the State of Maine with the transition plan, the tools, formal technical documentation, and training materials needed to operate independently and minimize the impact loss of system knowledge if stakeholders leave the business post-transformation. Our suggested approach:

- Determine the scope of the necessary project knowledge based on the State of Maine's operational future-state vision. Include project leads and agency group leaders for input as necessary. Identify knowledge objects, determining what is required for transfer from project team to stakeholders. It's important to understand that not all documents are required to be part of the capture and transition process.
- Identify knowledge owners, selecting agency stakeholders to own each of the knowledge objects. Determine who from the agency will own the objects identified for transition. This is where we will leverage our knowledge of the State of Maine's organization, Subject Matter Experts (SME), and project leadership to ensure appropriate owners are identified.
- Select enablers, using our digital learning tools and Knowledge Capture platform to transition knowledge. Select the enablers, establish a joint team including State of Maine personnel and project team members to coach stakeholders, identify SMEs and train the trainers, and focus on on-the-job training.
- Identify metrics, creating sustained momentum to measure the success of our collective efforts. We will work with State of Maine leaders to ground the metrics around the future-state vision. We will also use metrics to determine timing for when specific knowledge should be transitioned.
- Measure and signoff, ensuring the right amount of knowledge transfer occurred and course-correcting where necessary. We will work with State of Maine project leadership to determine appropriate knowledge adoption and develop a formal knowledge transition signoff agreement to confirm that we have achieved our knowledge transition goals.

The outcome of the knowledge transfer and transition process will be a smooth, seamless transition from a project mindset to business as usual.

1.2.5.8 *Help Desk Services*

IPS has partnered with Allied Digital IT Services LLC (ADSL) to provide Help Desk Services for the State of Maine. Under this agreement ADSL will function as a sub-contractor under the IPS consortium umbrella with IPS providing the governance and vendor management function. With more than three decades of experience in providing the managed infrastructure services to customers, our partner ADSL has mastered the art of customer service with their matured systems and processes (ITIL/ITSM) for high quality customer service. Today ADSL is a partner for many large geographically distributed organizations for total outsourcing of IT support services.

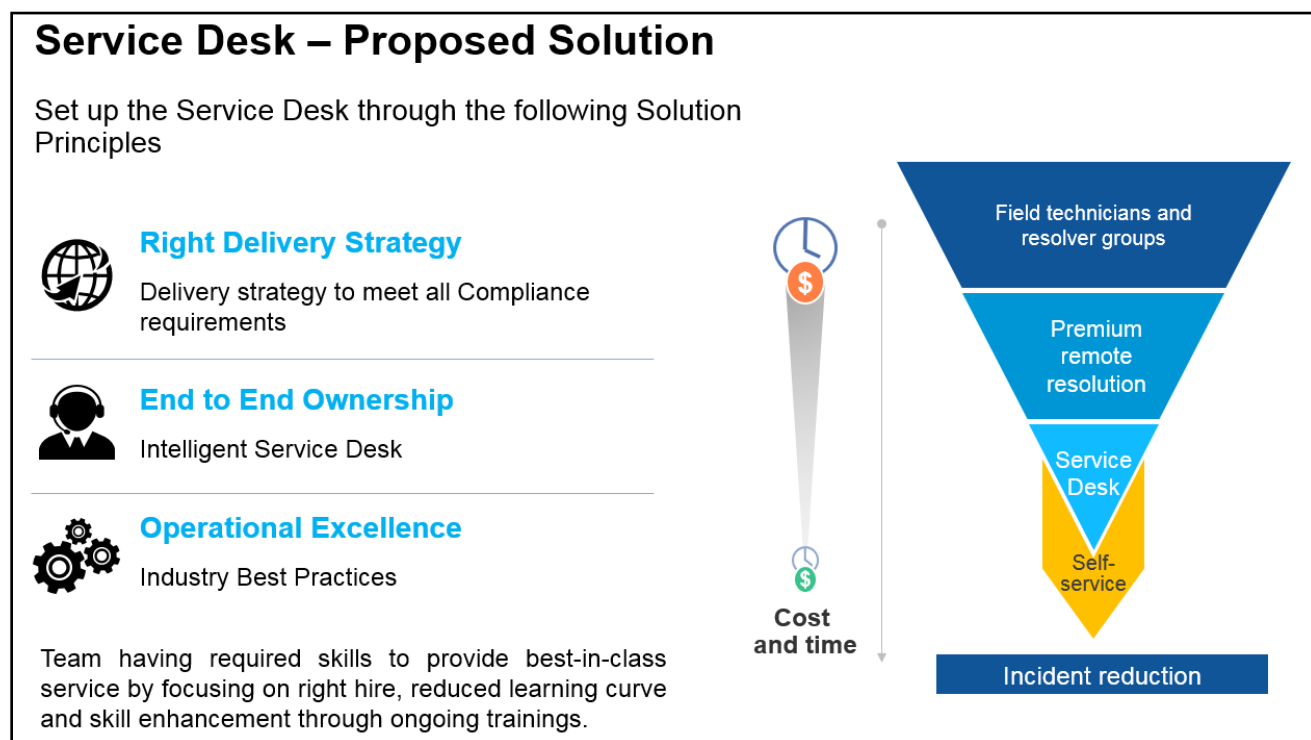


Figure 110. Service Desk Proposed Solution

ADSL's Value Proposition:

Deep knowledge in providing end user services to their customers. ADSL currently handles over 2.5 million contacts per year for end user support globally. This activity has given us sufficient experience which enables us to deliver high quality services to our clients. We will be happy to provide you with references of our delighted customers.

Highly customized, Process Driven Service Delivery:

Allied Digital's Service Delivery processes are ISO 20000 certified, and they also have all of their service delivery managers ITIL certified. Over the past years, they have matured their processes to ensure customer satisfaction with 99.9% SLA adherence. The ADSL GSD will field and accept ownership of information technology issues, inquiries and requests submitted by client's internal technology users via the telephone, email, or web (when implemented).

Service Delivery Parameters & Operating Procedures

Table 59. Service Delivery Parameters

Service Desk	
Service Description	Provide a single point of contact for the acceptance and ownership of information technology issues routed to the Global Service Desk.
Number of Users supported	5,000 - 12,500
Approximate Monthly Contact Volume	1,000 – 3,500 contacts per month
Service Desk Coverage	24*7 State of Maine will define their observed Holidays
Service Desk Center Location	Allied Digital Corporate Office, Torrance CA

Service Desk	
Business Hours Team	On-Shore, Shared Team located in US
Caller Entitlement	Caller Entitlement will be verified by an approved process
Primary Language Supported	English
Email to Incident Conversion	User submitted e-mail requests will be converted into an incident
Toll-Free Phone Number	Provided by ADSL and included in pricing
Incident Management System	ServiceNow – Infosys
Remote Desktop Tool	Remote control tool approved by State of Maine

Benefits of the Service Desk

The following highlights key benefits the ADSL Global Service Desk:

- Enhanced and effective First Call Resolution methodology
- Accurate and appropriate escalation
- Highly trained and certified agents
- SLA-driven operating model which guarantees consistent and predictable services
- Root Cause Analysis / Knowledgebase eliminates redundant issues
- Standard operating procedures based upon Industry best practices
- Real-time reporting
- Formal engagement with ADSL Project Management Office (PMO)
- HDI and ITIL framework methodologies provide “best in breed” services

Functionality and Value

- Emphasis on First Call Resolution
 - Reduction in workload of upper support tiers
 - Decreased resolution time
- Utilization of Remote-Control tool to assist in resolving problems quickly
 - Reduce escalations and end user disruption
- Detailed reporting of incident activity and service performance
 - Comprehensive, real-time view into enterprise support demand and service performance
- Transparent resolution ownership and status management
 - Improved customer experience, reduced resolution time and resolving group accountability
- Develop / maintain Standard Operating Procedures for supported technologies
 - Consistently provide predictable, repeatable support services
- Employ a Quality Assurance program including call monitoring and incident review
 - Ensure quality support to Clients end users
- Leverage Cisco Call Manager (ACD) to receive and route calls
 - Measure and monitor phone metrics such as Average Speed to Answer (ASA), Abandon Rate and Talk Time

Experience supporting eProcurement solutions.

IPS has extensive experience running the eProcurement Service Desk for Government of Canada (GC)– Public Services and Procurement Canada entity. Our service desk based out of Ottawa, Ontario, Canada went live in March 2020, and has been supporting 8000 PSPC buying officers and 4500 suppliers as of June 2021. As the Government of Canada ramps up the usage of the system, the Service Desk will ultimately support 30,000 suppliers. The IPS Service Desk has extensive experience in supporting the federal procurement solution including managing catalogues, support RFIs and RFX events, assisting suppliers with registration and bidding related questions and issues, working with buying officers to assist them with workspace and PR (Purchase Requisition) related issues to name a few.

Running procurement operations also involves working with SAP Ariba and Fieldglass in getting incidents resolved; managing releases and ensuring the application is stable and performs as per expectations. IPS has built a large library of procurement related KB articles and has a pool of Ariba certified specialists on the Tier 2 team. The Tier 1 team is well versed in handling generic procurement related questions and very efficiently performs the role of “Catch and Dispatch” regarding functional escalation of incidents. In addition to comprehensive Service Management reports, the IPS Service Desk offers detailed procurement related reporting on a monthly basis across 27 different procurement KPIs to GC. IPS will work very closely with our partner ADSL in sharing this experience/ expertise in establishing the procurement desk for the State of Maine.

Support/Management Plan that addresses:

Help Desk location and staffing

ADSL’s team selection process is one of the ways the partner has been able to retain employees and maintain a low annual attrition rate. ADSL knows that service desk is a very volatile industry. In fact, many see it as a steppingstone into IT. To combat this, ADSL has created many internal programs and incentives to retain their staff. Their hiring process starts off with a test sent to potential candidates that they need to complete before the interview. During the interview, the first question ADSL interviews ask is “walk me through the steps of making an omelet.” ADSL interviewers get many diverse types of answers and reactions. The interviewers look for attitude towards the questions, level of depth and description, and presence /confidence. ADSL’s belief is that if the candidate can walk the interviewer through the steps of making an omelet in a controlled and descriptive manner then you can for example, walk a user through resetting their own password.

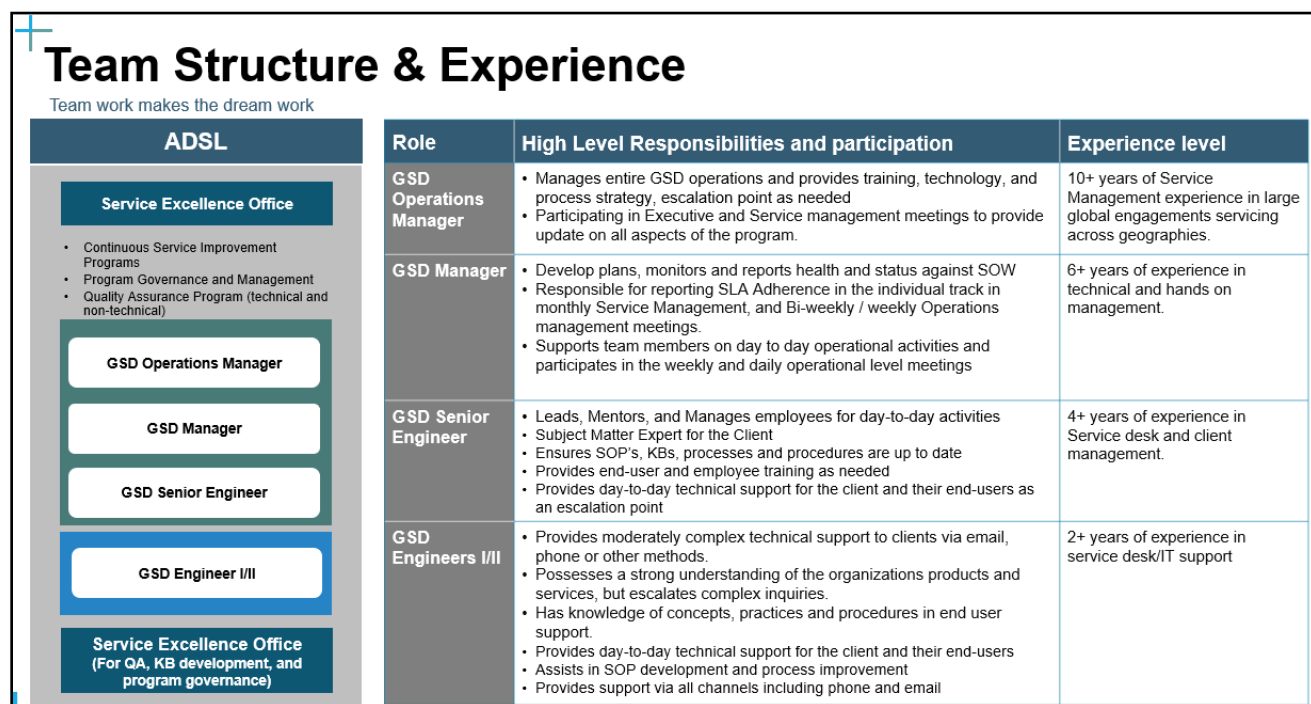


Figure 111.ADSL team Structure and Experience

ADSL leverages a creative approach to hire and nurture our talented workforce. The employee advancement, improvement, and recognition programs include the following:

- Extensive interview process including both management and peer review.
- Background and reference checks.
- Nurture talent by strongly promoting an environment of internal advancement, earning additional responsibilities and promotion.
- Career ladder for each employee
 - Entire service desk management team was promoted from within.
- Funding for all relevant professional certifications
 - ADSL pays for all certifications
- Quarterly Blue Star Award that provides recognition and financial reward, reinforcing the appreciation ADSL values in their team.
- Quality Assurance Team which reviews agent calls scores the calls against a 27-point evaluation guide and produces a performance evaluation grade (PEG) for each call reviewed.
- Sponsor a weekly team lunch for all service desk staff.
- Weekly award of gift cards for agents achieving the highest performance evaluation grades.

Service Desk Certifications

ADSL is highly committed to retaining and nurturing the top talent this industry has to offer. This effort has resulted in the following:

- Staff regular appearance in the Help Desk Institute (HDI) Analyst of the Year contest
- One of the lowest voluntary attrition rates in the industry
- Agents who possess multiple Industry certifications and training credentials

ADSL's partnerships with quality staffing agencies and local colleges in the Los Angeles area have created a pipeline of qualified candidates. ADSL also incentivizes their employee with internal referral

programs. They also require all engineers that are hired possess at minimum 3 IT related certifications. Typically, these certificates are an A+, N+, and a Microsoft related certificate. Most of ADSL's engineers take advantage of their certification program (as seen in the list below). As an added incentive, ADSL pays for certification costs.

- A+ (Hardware & Software)
- N+ (Network +)
- HDI (Helpdesk Institute)
- MCSA (Microsoft Certified Solutions Associate)
- MCSE (Microsoft Certified Solutions Expert)
- CCNE (Cisco Certified Network Engineer)
- CCNA (Cisco Certified Network Associate)

Participating Entity responsibilities and staffing recommendations

Table 60. Operations Services RACI Matrix

Service/Task	Responsible Party	
	State of Maine	Infosys
Incident Management		
Tier 1 Business Hours Support	C	A,R
Tier 1 After Business Hours Support	C	A,R
Tier 2/3	C	A,R
Known error documentation	I	A,R
Knowledgebase updating	I	A,R
Incident reporting (daily, monthly, annually)	I	A,R
Knowledgebase audit (annually)	I	A,R
Service Request Management		
Service request submission	A,R	C
Service request assessment and approval	C	A,R
Service request fulfillment	A,C	R
eProcurement Application Maintenance		
Application patches and regular updates	I	A,R
New business capability releases and platform changes	A,C	R

Systems and tools utilized to provide services including phone, chat and ticketing systems.

ADSL will provide Cisco Finesse and Nice inContact CXone for audio recording. For Chat, IPS will leverage Amazon Connect Chat for chat support and ServiceNow for ticketing.

ServiceNow

For the State of Maine, the proposed ESM Café solution is a gold image of ServiceNow solution. It is designed on top of ServiceNow and has ready to deploy work packages for base ITSM applications. We propose to implement ESM Café to enable the State of the Maine's service desk.

We will leverage several ServiceNow tools and accelerators based on experience from similar engagements and best practices which will be utilized at GC for this engagement. A few of the delivery accelerators are:

- ServiceNow Integration Factory to streamline integration efforts
- iPRISE: Integrated process repository and Express ITIL solution to reduce time for process definition and business requirements gathering
- Persona based Service Portal: Endorsed by ServiceNow as a “Game Changer” for our client's business, Infosys has designed a custom persona-based Service portal to enhance end user experience. In their simplest form, personas group end users by a set of common characteristics, such as:
 - Role and function
 - Security access
 - Level of responsibility
 - Approved devices and applications
 - Support level required

Welcome to your Esm Cafe!
To service you better, please answer the four questions below.

1. WORK SETTING	2. WORK STYLE	3. TECHNICAL KNOW-HOW	4. COLLABORATION NEEDS
Where do you most often work?	When do you need to be connected?	How much help do you need with new technology?	How often during the day are you working with others?
Office	Business Hours	Not Much	Rarely
Mixed	Always On	Occasionally	Sometimes
Always Remote		A Lot	Always

Submit Answers

Figure 112.ESM Café Entry

ServiceNow Partnership, Center of Excellence and Managed Service platform

We have an extraordinarily strong partnership with ServiceNow and our partnership with ServiceNow brings in value in multi dimensions including:

- ServiceNow Center of Excellence: Has established “ServiceNow Center of Excellence (CoE)”. The key areas that the CoE focuses on are, managing and building Proof of Concepts for our customers, integration with third-party technologies, training and providing value added services to our clients, recommendations on development best practices, reusable work packets.
- Infosys has set up demo labs for training and development purposes. Some of the key benefits are:
 - Reduced time to implement by utilizing the preconfigured process built on the OOB functionalities of ServiceNow.
 - Standardization and alignment to Best practices: The iMSP solution is built on ITIL best practices keeping in alignment to best practices to the OOB functionalities.
 - Cost Optimization: Provides considerable cost benefits by bundling License, implementation and support cost.

- Solutions and Accelerators: We have 75+ solution accelerators for ServiceNow implementations. These accelerators are designed based on our experience in executing ServiceNow programs, leveraging our ServiceNow partnership and industry best practices. Have successfully used and demonstrated these solutions and accelerators in our recent engagements.
- NextGen Integrated App Store: Enterprise Café designed and developed internally on ServiceNow as the gold image that can be leveraged for our customer's ServiceNow implementations for reducing time to market. It has all the base ITSM process applications and integrations designed to be deployed rapidly.
- Solution Designing and blueprinting: We have worked with ServiceNow Professional Services to design future solutions and blueprints for our large clients.



Figure 113. Service Now ESM Café Model

Performance metrics tracking and reporting.

Reporting is a critical tool in understanding the volume, nature and effectiveness of resolving end-user issues. ADSL is proud of the robust reporting that our solution offers. Reports are focused on specific key areas; each providing the right combination of measurement and history to demonstrate performance and identify trends. The following standard reports are provided by the 15th calendar day of the following month that ADSL can provide the reporting portals. Below is a sample of the ACD report and on the following page is a table listing some of the Standard GSD reports.

Cisco ACD Phone Statistics Report:

- Total Presented/ Offered Calls
- ASA SLA Target (%)
- Total Handled Calls
- Abandon Rate (%)
- Total Abandoned Calls
- Abandon Rate SLA Target (%)
- Total Dequeued/ Flow Out Calls
- Average Handle Time

- Average Speed of Answer (ASA)

Incident Statistics (system-dependent):

- Tickets Created and Resolved
- Ticket Origin (Call, Web, etc.)
- First Contact Resolution (FCR) (%)
- Top 10 Tickets
- Aging Tickets by Assigned Group and Assignee Survey Data Reports
- Survey score average, responses, sent, and %



(*) Reporting is reliant on leveraging your ITSM to provide these reports. If it cannot provide metrics or reports, then the SLA against the metric will not be applicable as we are unable to track and report against it. Our business analyst team will create dashboards and our Management team will present their findings to customer, at the minimum, monthly.

Figure 114. Performance Metrics Dashboard

Issue analysis, tracking, and reporting.

As shown in the call flow diagram below, calls routed to the ADSL Service Desk will be “triaged”, resolved when possible, and if they cannot be resolved escalated to resolving groups.

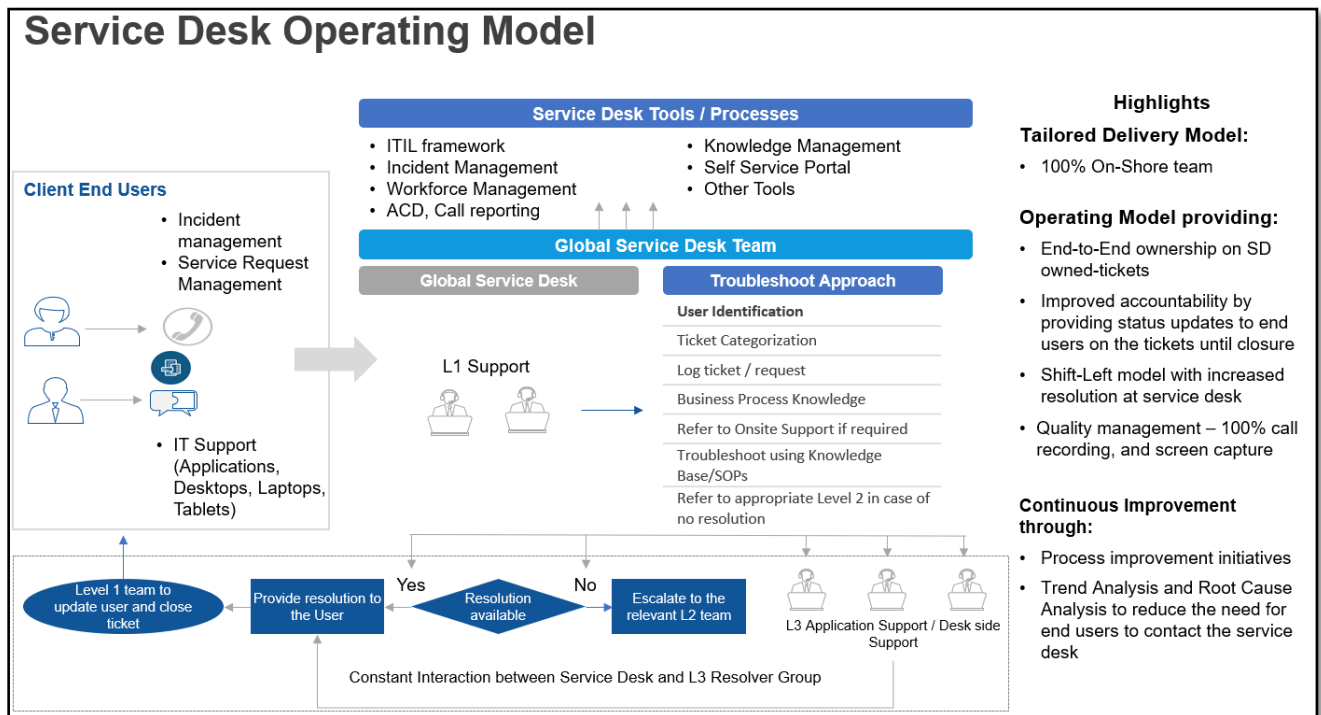


Figure 115. Service Desk Operating Model

- Receiving the Call** – The client end-user may contact the Service Desk by e-mail or by telephone. The client can also route support calls to the Service Desk through a dedicated telephone support line.
- Answering the Call** – Service Desk Agents are fluent in U.S. dialect English and will answer calls in a professional and courteous manner. ADSL's staff is locally based. Their Cisco Automated Distribution System will route calls based on skillset and priority levels in the Cisco queue. When answering a call, the Agent will use a client-branded greeting. All agents are trained on Customer Service and calls can be recorded for auditing purposes which are conducted daily. Agents conduct one-on-one training with the head of ADSL's QA department for the "customer-service experience." This training is 100% non-technical and is focused and dedicated to the customer experience. Training includes reviewing calls to monitor dead-air, tone, greetings, scripts, and a review of our 25-point QA checklist.
- Logging / Triaging the Call** – The end user will be asked for an existing Incident Reference Number or, if reporting a new issue, will be asked to provide their name, Client site location and to indicate the main problem or the reason for the call. The call will be immediately triaged using the priority scale and logged into the ITSM system. The agent will attempt to triage and leverage appropriate tools to support the user. The developed knowledge-base articles will illustrate how to resolve, remediate, or escalate any tickets as needed. The end-user will be given the unique Incident Number for cross reference. Client end users who contact the GSD for call status or questions are requested to provide the Incident Number to aid in locating the incident record.
- Incident Support or Escalation** – ADSL GSD will attempt to solve problems as defined by the Client. If the issue cannot be resolved and it is determined to be of low severity, the issue will be escalated per the appropriate escalation script. If an issue is determined through triage to be a high severity issue, the issue will be handled in accordance with the standard operating procedures defined by the client.
- Incident Closure** – The GSD agent will verify with the client employee that the problem has

been resolved. They will then update the incident and set the status to “closed” in the Incident Management System. Upon closure of the incident the client employee will be notified.

6. **Incident Resolution Documentation** – Closed incidents will be reviewed, and resolution data will be used to update existing GSD procedures, support scripts and knowledgebase.

Call Routing and Staffing Model

ADSL’s industry-unique support model, or “hybrid model,” is based on the combination of having primary and secondary engineers as resources. The hybrid model is comprised of several different factors including:

- Our Automated Call Distributed System:
 - Cisco Call Manager routes calls based on agent priority in the pre-defined cisco queue.
- Skill-Based Routing:
 - During transition, ADSL determines agent priority based on industry experience, technical knowledge, and soft skills. The more qualified agents will serve as primary agents who will over time become Subject Matter Experts for your environment. In addition, their secondary support agents will act as secondary resources when we need to scale-up for volume due a spike in calls. These shared agents will have the exact training, knowledge, soft-skills, and technical experience that our primary agents must support your end-users.
- Cost-Effective Resource Model:
 - Both primary and secondary resources will be able to support all your end-users. The main difference between the two is that the secondary resources will support 3-5 additional clients and are on a lower priority in our Cisco Call Manager system. The lower the engineer priority (1-5), the less calls they may receive compared to the dedicated agents who are higher priority (5-10).
- Customer satisfaction tracking and reporting; and

In the past ADSL has implemented similar programs for promotion of Customer Satisfaction (CSAT) surveys so that end-users may become excited and provide feedback. A proposed sample plan is shown below, the promotion team may send newsletters, monthly email blasts, and other collateral to get end-users excited by:

- Ensure that CSAT survey is easy to use and quick. For example, push notifications with an interface on desktops are an easy and quick way to receive feedback.
- Educate end-users on the benefits of using the feedback and CSAT surveys. Some end-users may not be aware of what it can do to the IT department and team morale. Education may include how to leave feedback and what we do with that feedback. Better knowledge and education on the benefits provides greater value to end users.
- Create marketing collateral such as infographics to explain how the voice of the end user matters and what we do to ensure they’re heard.
- The promotion team, with approval from our clients, as we’ve done in the past with other customers provides incentives or rewards such as a monthly \$100 gift card. Providing incentives or rewards to end-users who leave feedback will encourage others to do it as well.
 - Option/approach to transition to a Participating Entity Help Desk operation including training of Participating Entities Help Desk resources.

Upon expiration or termination of this Amendment, ADSL will cooperate with the State of Maine to assist in the orderly transition of the Services provided under this Amendment. ADSL will notify the Client in advance if any charges are associated with such assistance, and in such case will provide the assistance only upon Client’s approval of the charges. The parties agree to use the Change

Control process to initiate, review, and approve any request for Services transfer and termination assistance.

ADSL shall provide Services transfer assistance ("Termination Assistance") until the expiration or termination of this Amendment. As required for an orderly transition of other ADSL services, ADSL shall provide Termination Assistance for related services for up to one hundred eighty (180) additional days after the effective date of expiration or termination of this Amendment or as otherwise mutually agreed by the parties.

If such Termination Assistance requires ADSL to incur expenses in addition to the expenses that ADSL would otherwise incur in the performance of this Amendment ("Additional Termination Services"), then: 1) ADSL shall notify Client of any additional expenses associated with the performance of such Additional Termination Services pursuant to this section prior to performing such Additional Termination Services; 2) upon Client's authorization, ADSL shall perform the Additional Termination Services and invoice Client for such Additional Termination Services; and 3) Client shall pay ADSL for such additional expenses incurred to provide the Additional Termination Services under the normal payment terms and conditions of the Agreement.

Termination Assistance shall begin upon ADSL's receipt of 1) Client's notice of the termination for convenience; 2) either Party's notice of the termination for cause; or 3) notice by Client of its intention not to renew. Except as provided above, there is no additional charge for the Termination Assistance listed below except if termination is for default caused by a breach by Client.

Termination Assistance will include the following:

1. Pre-migration Services
 - a. Freeze all non-critical software changes.
 - b. Provide a transition plan for personnel who support Client.
 - c. Explain the operations manual to new operations staff.
 - d. Provide knowledge transfer to new operations staff if Client is assuming responsibility for the services, and assist with training if a third party is assuming responsibility.
 - e. Submit a schedule for termination activities.
2. Migration Services
 - a. Assist in the execution of a parallel operation, until the effective date of expiration or termination of this Amendment, including delivery to Client of the then current procedures manual.
 - b. Provide a listing of all ADSL employees who have (or had) access to the Client system, devices, or other technology artifacts, including the type of access by name (or ID number), level of access, and function that the resource conducted. This will be used to remove all ADSL access at the time of termination.
3. Post-migration Services
 - a. Answer questions regarding this Amendment on an "as needed" basis.
 - b. Turnover any remaining Client-owned reports and documentation still in ADSL's possession.

1.2.5.9 *On-Site System Stabilization Support*

Infosys proposes a comprehensive Hypercare support plan (Stabilization period) for post go-live. The processes, methods and tools are well aligned to State of Maine's requirements.

- In accordance with the State of Maine's requirements, Hypercare support will be provided for 3 months, wherein the project team closely monitors and resolves the issues faced by the end

users.

- Users will call the Helpdesk number and Helpdesk team will remediate L1 [Level-1] requests. The help desk will log the calls in Service Now.
- A war room will be set up which will answer the end user queries and provide the functional guidance for the issues faced. The war room will be managed by Support Stabilization Command Center Team comprising of State of Maine Business Leads, IT, SME and Infosys project team members. The war room will be primarily managed by Infosys. The team will help users in resolving L2 [Level-2 support] issues or assign the incident to Technical Team for further analysis
- A daily defect triage meeting will be conducted to review and manage the open defects in Service Now.
- The Command Center team prioritizes the issues by severity. Issues will be redirected to technical team [Infosys / PeopleSoft] in Service Now, if the incident needs a fix (L3: Level-3) or further analysis is needed.
- The Technical team will analyze and provide fix as needed. Product issues will be reported to SAP Ariba for resolution.
- During the Hypercare, Infosys Onsite and Offshore consultants who have been part of the core implementation team will be available for post Go-Live support activities and the key staff shall be retained in the team for this period. They will closely work with the key stake holders and the end-users to quickly resolve any production issues noticed during the Hypercare/Stabilization period.
- After the three months of Hypercare support, the team will transition to Managed Services team.
- The Managed Services team will be comprised of a portion of the project team and the Managed Services team so that knowledge is retained and the transition is smooth.

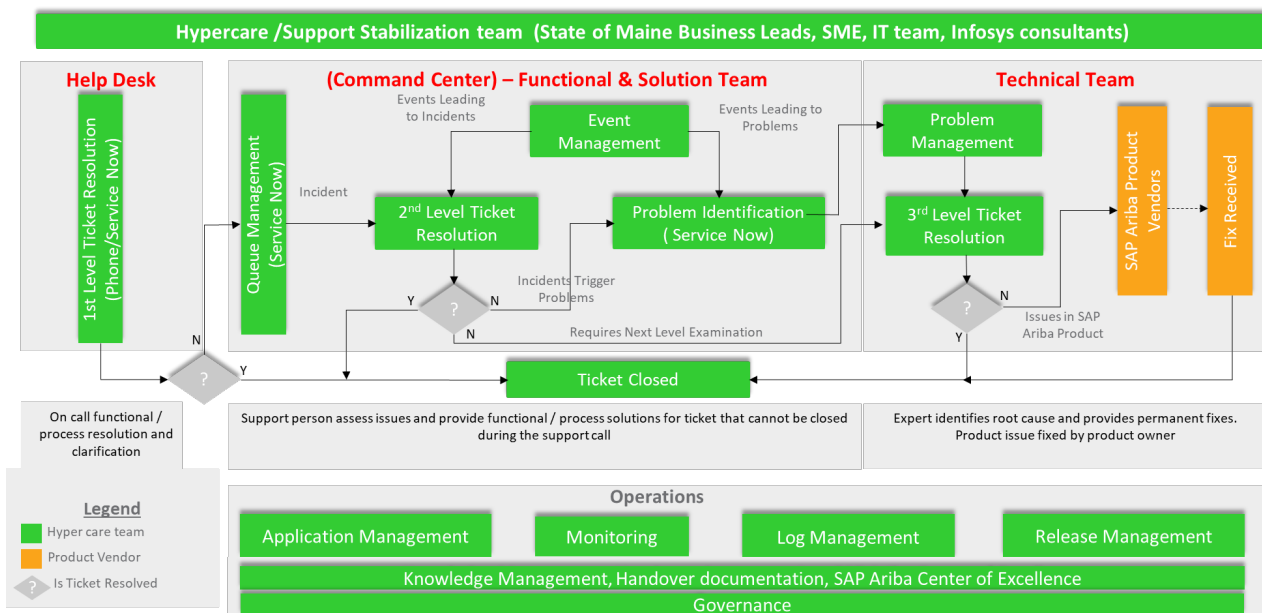


Figure 116. Onsite System Stabilization Support Plan

Infosys believes that preparations for an effective knowledge transfer will need to start very early on during the course of the project.

Preparing from Day 1

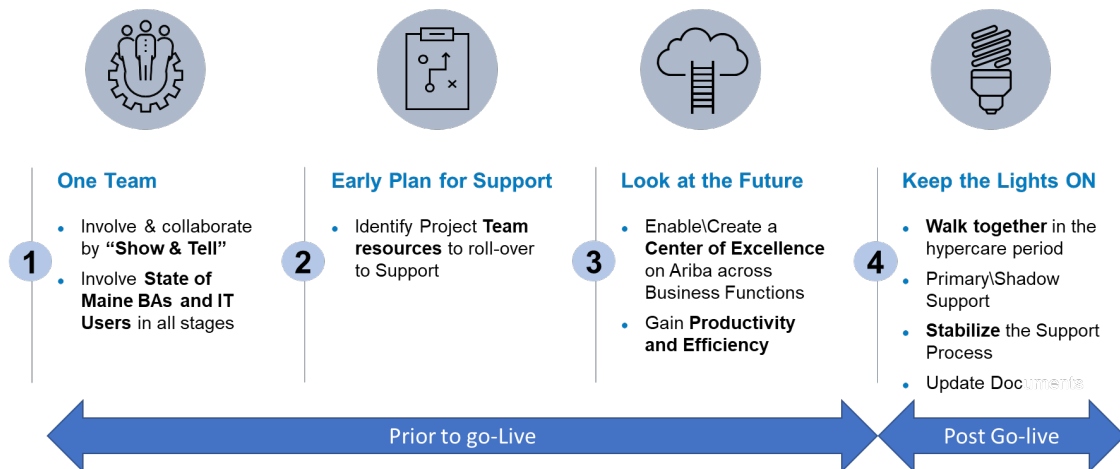


Figure 117. Knowledge Transfer-Preparing from Day-1

Some of the noteworthy aspects of our approach are:

- **One Team:** Close coordination between the State of Maine's Teams, Infosys project teams as well as any external system SME (State of Maine PeopleSoft team). We believe that by using this 'One Team' approach right from the beginning of the engagement, we will be able to achieve a great degree of synchronization of thoughts and ideas right from the start of the project and we will be able to sustain this synchrony throughout all phases of the project.
- **Early Plan for Support:** Early identification of project team members who will be rolled over to the support teams. This will enable the identified resources to be 'Support-Ready' whereby they will be well versed with the systems, processes and methodologies involved during the implementation phase and will be able to apply these learnings better during the support phase. Being part of the project from the early phases, the support team will be fully on-boarded with the details of the documentation and technical solution. They will have ample opportunities to share their inputs in the early phase of the project keeping the support perspective in mind. This is an added advantage of early onboarding of few identified support team resources.
- **Look at the Future (Ariba CoE):** Once the pool of key project team members, State of Maine SMEs and managed services resources are identified, we will encourage close collaboration and learning by way of a Center of Excellence wherein team members sustain the process of knowledge gain by means of 'learning from each other' thereby 'learning with each other'. This will enable the team to quickly and effectively realize the improvements in processes, productivity and become more efficient in their transformation journey.
- **Keep the lights ON:** All of the effort and learning from the previous phases will culminate towards the most important phase of the knowledge transfer journey in what we call 'Keeping the lights ON'. During this phase, Infosys will develop a structured approach whereby we will transfer knowledge of the 'What', 'Why' and the 'How' of the changes resulting from the implementation to the identified Managed Services (i.e. support) team members. We have designed this phase to coincide with the 'Hypercare' phase.

Infosys will follow a gating process within the transition phase in order to ensure seamless transfer of knowledge between Infosys teams and the future Managed Services teams. The diagram below provides a high-level overview of the process that we will follow:

Important Note:

- The timelines of the KT phase will coincide with the Hypercare period.

- Duration of each phase will be mutually agreed among Infosys and the State of Maine.
- Each phase will have a defined Entry Criteria and Exit Criteria.

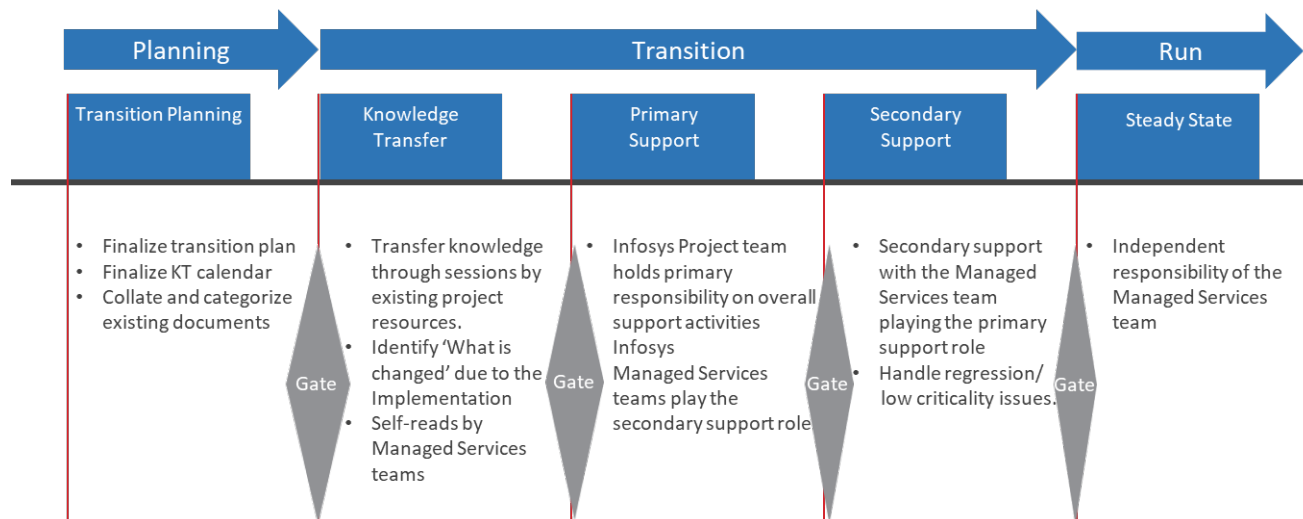


Figure 118. Transition Plan with Gating process

1.2.6 Managed Services Requirements

1.2.6.1 *Solution Support*

Infosys is well known in the U.S. and throughout the globe for our excellence in managing applications, systems, and services for clients. We are pleased to see that the State of Maine has recognized many of the key features of efficiently managed, high profile business systems.

Our commitment to 10+ years of support for the State of Maine starts on Day 1 of the project and continues through Go Live and into steady state operations. We have gained hard earned experience in transitioning new and existing applications to a managed service environment. Part of our success in this area comes from rigorous planning and risk management, the other part is our people, some of the finest professionals in the industry in managed services.

Infosys has proven methodologies and processes for effectively managing complex business applications and systems. We are specialists in identifying and managing risks associated with third-party COTS and Cloud-based systems. Our Managed Services Team goes above and beyond in planning future releases and feature expansions, as well as managing emergency releases and hot fixes when needed.

The team consists of highly experienced, cross-functional personnel to support State of Maine in meeting its needs. Every team member has many years of experience and certifications in their respective areas of knowledge.

Infosys is a very good cultural fit because we understand public sector entities and their unique requirements. We employ a collaborative and flexible workstyle to meet current and emerging unique situations.

1. Solution Support

Maintain the performance, availability and stability of the Solution. The Contractor must schedule its implementation of changes so as not to unreasonably interrupt State business operations.

Make no changes that would materially alter the functionality of the systems used to provide the Services or materially degrade the performance or SLAs as established of the Services, without first obtaining State approval. In the case of an emergency, and in keeping with State security policies in effect, the Contractor may make temporary changes at any time and without State approval, to the extent such changes are necessary, in the Contractor's judgment, (i) to maintain the continuity of the Services, (ii) to correct an event or occurrence that would substantially prevent, hinder or delay the operation of State critical business functions; and (iii) to prevent damage to the Contractor's network. The Contractor will promptly notify the State of all such temporary changes. At the conclusion of the emergency the Contractor will restore any changes to the pre-emergency state, and if the change is deemed necessary for normal operation of the system, a corresponding change request must be initiated for State review and approval. The Contractor must review and perform a root-cause analysis of any deviation from any scheduled or failed changes.

Perform technical activities including but not limited to: system code/object migrations, patch implementations, testing, performance tuning, log administration, data copies and exports, integrations and scheduled reporting/ETLs, and responsibility for issue resolution such that migrations into production will be executed at agreed periodic intervals and other production changes will be scheduled during the maintenance window. The Contractor must follow a mutually agreed, formalized and published methodology for migrations into production.

Support Model



Figure 119. Support as the Final Step

The Release Plan is the guide to successfully transitioning each release to production. Infosys has adopted ITIL V4 practices as the foundation operating model for operations support. Our Operations Support methodology is focused on service excellence, proactive behavior, and end-to-end accountability of support services.

The post go-live support and transition process contains four components:

- **Knowledge Transition:** Project team members develop knowledge transfer agreements that outline the specific skills and capabilities to be transferred and the activities required to close the knowledge gap.
- **Shadow Support:** During the hyper-care period post go-live, Project/Development teams are responsible for support and application/infrastructure management during the transition to steady-state support.
- **Primary Support:** Operational (application/infrastructure) Support and Help Desk teams start taking over Production incidents and at a pre-defined trigger point they will completely take over the handling of incidents from the Development teams.
- **Steady-State Support:** At this stage Development teams will be released from the support organization and Operational Support teams will be completely responsible for all Production incidents, ongoing maintenance and enhancement activities, and Incident Management and Resolution.

Team Infosys will offer targeted support to key user groups, including:

- **Procurement Community:** Supporting sourcing, contract management and catalogue

management users.

- State of Maine Buyer Community: Providing support as needed for users making purchases on a sporadic basis.
- Supplier Community: Providing support to both existing and potential future suppliers.
- General Public: Support the public who may wish to know about a publicly posted tender or other open data.

Operations Capacity

One of the key focus areas for the State of Maine is to deliver seamless and uninterrupted services to users. To achieve this, it is critical to optimally staff the Operations team, and set up a system and processes to address various issues that will arise on a day-to-day basis.

The Infosys team will onboard the Operational staff needed and recommend the necessary infrastructure changes based on the current and future enrollment statistics captured in the Transition-In Plan.

The Infosys Operations team will monitor the performance statistics of the production servers and will recommend any capacity resizing based on the load.

Operations Compliance and Audit

As a part of the Operations phase the Infosys team will ensure that the necessary audit controls are in place. Team Infosys will provide a secure email facility that will be used to communicate with the State of Maine.

Approach to Managing Ongoing Change

For a major transformation program such as eProcurement, changes are expected to occur throughout the lifecycle of the program. The following process will be adopted to proactively manage these changes to ensure proper operation of the offered services.

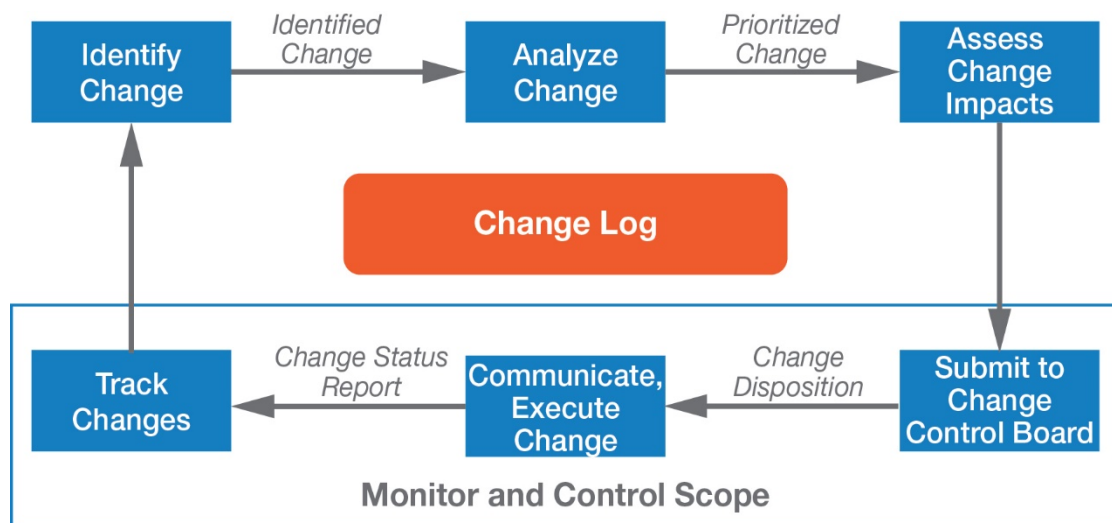


Figure 120. Approach to Managing Ongoing Change

Change Management Lifecycle

Given the requirement for ongoing releases and changes within the eProcurement program, it becomes crucial to maintain proper control over scope items, to ensure that changes are not enacted without approval, and to ensure that approved changes are executed comprehensively and proactively as per proper process control. The Change Management Lifecycle is further detailed below.

- Identify and analyze change — when potential changes have been identified or requested, the

Initiator first logs a change request in the change log. The change is decomposed into its basic elements, such as change requested, reasons and justifications, and options considered.

- **Assess change impact** — The initiator/change request owner works with various stakeholders to assess respective impacts to the overall program. Recommendation for change resolution will be incorporated into the change log to be submitted to eProcurement Change Control Board.
- **Submit to Change Control Board** — The eProcurement Change Control Board (CCB) is composed of the eProcurement leadership team, business and IT solution architects and stakeholders, as well as SMEs in various functions. Change requests that have significant impacts to the eProcurement program are submitted to the CCB during routine or special CCB sessions for review and for decision making. The CCB makes a go/no-go disposition of the change request and provides directions for the next steps. The resulting action items are recorded against the change request in a central repository.
- **Communicate and execute change** — Change action Items are assigned to an owner and worked on to resolution. The Change request owner is responsible for closing resolution and reporting to the CCB of the outcome of the changes.
- **Track changes** — All change requests will be logged in the Change Management system and tracked by the eProcurement PMO to ensure prompt execution and closure

Prior to using any software or equipment to provide the Services perform all necessary testing to verify that the item has been properly installed, is operating substantially in conformance to its specifications, and is performing its intended functions in a reliable manner in keeping with the defined Service Levels in effect at the time of the change.

Reasonably accommodate the Participating Entity testing, review and approval processes prior to promoting these Solution components in the Production environment.

Monitor all third-party software vendors and vendor services for proactive notification of all applicable patches and updates. When new eProcurement impacting items are released, they must be tested by the Contractor in its protected test environments, and jointly scheduled with the Participating Entity for installation during the next scheduled maintenance window. A priority update window may be required in advance of schedule if a patch or fix is deemed to be critical or security related.

Description of the User Acceptance Testing Process

User Acceptance Testing (UAT) is the final stage of eProcurement system validation, performed by the State of Maine business owners with assistance from our team. The design and functionality must meet the business requirements. UAT is the final quality control procedure to determine whether the application is performing as expected and ready for deployment into Production.

The steps in the UAT process are highlighted in the figure below. Team Infosys will be leveraging our best-in-class Panaya CloudQualitySuite testing tool to set up and execute UAT to accelerate the testing process, enable collaboration, and achieve high quality results in the UAT process.

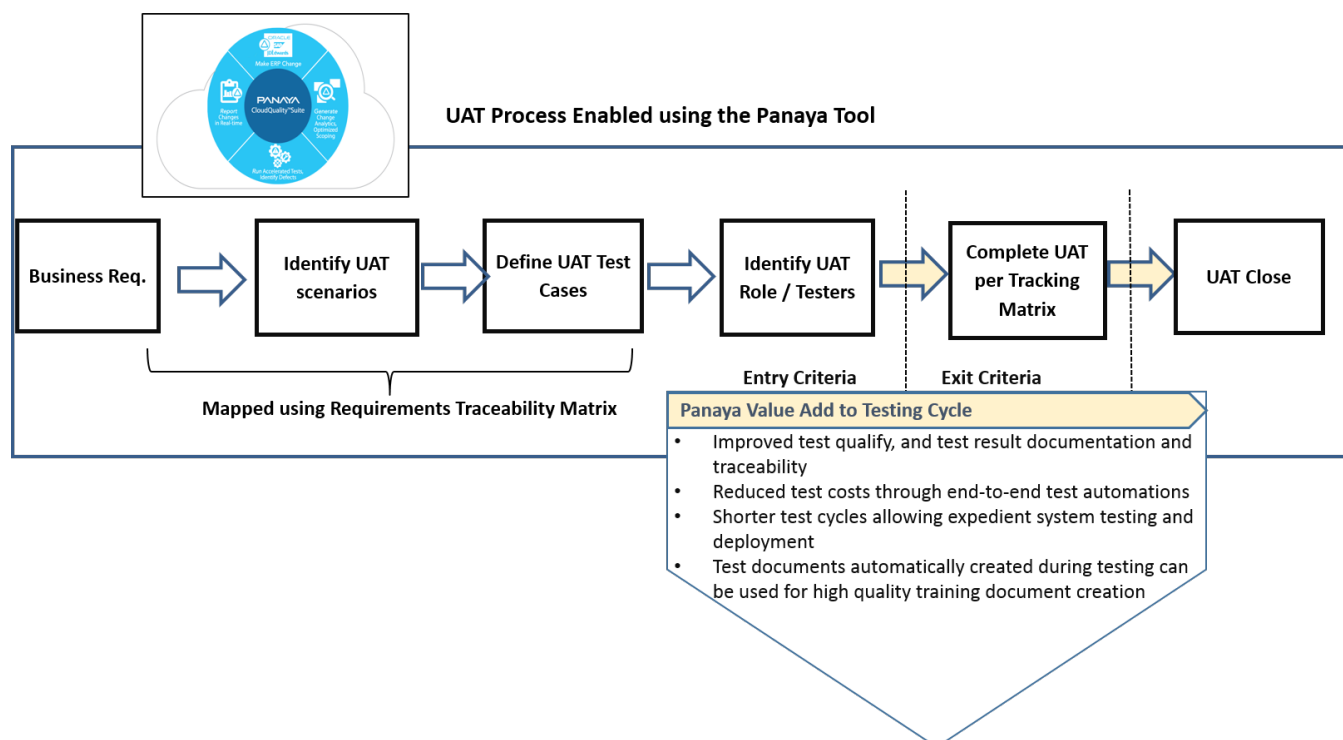


Figure 121. Panaya Enabled UAT Process

UAT Process (Value Add) driven by Panaya CloudQualitySuite Tool

The UAT process begins by using functional and process requirements to identify UAT business scenarios to be tested in the UAT phase of each release milestone. Each UAT scenario is then broken down into one or more test cases, each of which will test one or more requirements. UAT test cases are geared toward simulating real-life business scenarios where multiple test cases can cover each end-to-end business scenario.

The mapping of process and functional requirements to UAT scenarios is done by using the Requirements Traceability Matrix (RTM), to ensure that all requirements are tested using one or more UAT.

Table 61. eProcurement UAT Entry/Exit Criteria

UAT Entry/Exit Criteria	
Entry Criteria	Exit Criteria
- Test environment set up completed - All test scenarios for the test phase identified and agreed by relevant stakeholders and execution plan documented - Planned Test cases for a minimum of two (2) weeks of execution are prepared - Master data set up (Manual) in the test environment completed for a minimum of two (2) weeks of planned test cases - Security role build completed and USERIDs set up with appropriate business roles	- All planned test cases are executed, and test results review completed - No Severity 1 (critical impact / system down) and Severity 2 (significant impact / application usable but severely limited) defects are open - Defect Resolution Plan has been prepared for all Open Defects - All Severity 3 and 4 issues have been reviewed with the process owner, individual and cumulative impact has

UAT Entry/Exit Criteria

• Access to the test environment provided to the testers • All Exit criteria for the previous test phases are met • Test Phase Entry validated by the Local Team and approved by the Core Team	• been assessed and not deemed to be critical • Workarounds identified and documented for all open defects if required. • Exit report validated by the Local Team and approved by the Core Team

During the execution of the testing, every test case will be recorded along with test results in the Panaya CloudQualitySuite tool. In case the functionality is not working as expected, defects will be raised by testers and assigned to a team for issue resolution. The team resolves the issues and notifies the tester to retest.. After the UAT is completed and issues logged are resolved with approval and sign off from the project authority, exit criteria need to be checked and validated from the exit criteria table above before the UAT can be closed.

For all Production and Non-Production environments (including environments that support systems development, testing, training, demo, QA and otherwise) monitor those environments, apply patches, and administer the system logs.

Upon the creation of any environment for Participating Entity use, (unless excused in writing by the State) include these environments in regularly scheduled backup, maintenance, update/upgrade, patching, monitoring/reporting functions prior to productive use by the Participating Entity and until the use of this environment is no longer required by the Participating Entity.

Application and system software/hardware upgrades for in-scope services must not impair the Contractor's ability to meet the Service Levels.

Approach to Service Continuity

The IT Service Continuity Management plan supports the overall Business Continuity Management (BCM) process by ensuring that the required IT resources can be recovered within business related agreed upon time frames and provide pre-determined levels of service under exceptional conditions which includes the following common responsibilities:

- Risk management
- Selection of options based on business requirements
- Definition of roles and responsibilities
- Alignment of IT recovery plans and BCM exercising (testing)
- IT focus

Resources include hardware, software, staff, and physical environments for the technical and operational aspects of the total Business Continuity Plan. Key points for consideration and proposing IT Service Continuity Management (ITSCM) plan includes:

- ITSCM must be aligned to the Business Continuity Lifecycle. Business Continuity Management (BCM) is concerned with managing risks to always ensure that an organization can continue operating to, at least, a predetermined minimum level and BCM process involving following:

- Reducing risk to an acceptable level
- Planning for the recovery of business processes should a risk materialize and a disruption to the business occur
- ITSCM must be a part of the overall Business Continuity Plan and not dealt with in isolation as ITSCM is the “technical component” of BCM.

As eProcurement is a Cloud-based procurement solution, vendors for Cloud software, including SAP and ServiceNow, have the primary responsibility to ensure that there are no service disruptions for their Cloud applications. With multiple redundant data centers and real-time data synchronizations and backups, it is highly unlikely that the system would become unavailable to end users for any extended period.

Our proposed approach to develop IT Service Continuity Plan is based on the initial steps for Business Impact Analysis and subsequently following the steps as shown below for implementation.

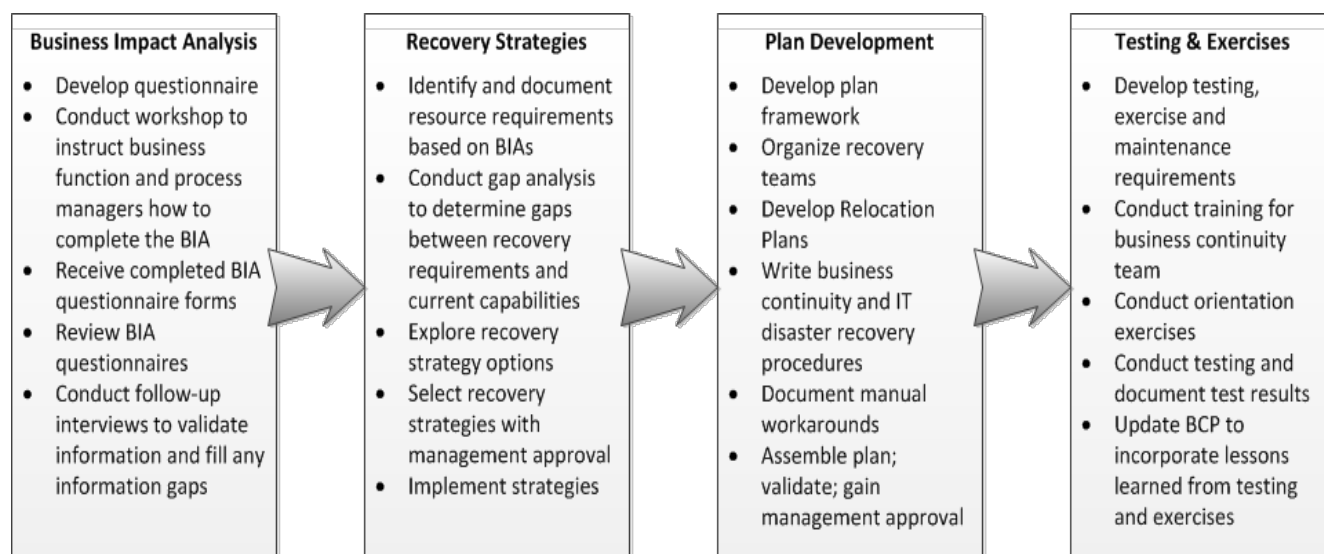


Figure 122.IT Service Continuity Plan Development Approach

Proposed Approach to Developing an IT Service Continuity Plan

Below is the summary list of key component details for IT Service Continuity Management (ITSCM) Plan and alignment to ITIL and Other Processes:

Table 62. Proposed IT Service Continuity Management (ITSCM) Plan aligned to ITIL Processes

Our Proposed IT Service Continuity Management (ITSCM) Plan aligned to ITIL and Other Processes	
Service Level Management (SLM)	• ITSCM is IT Service-oriented and SLM provides a key interface as it defines what are the IT Services within a Service Catalog and at what Service Levels they must be maintained.
Configuration Management (CM)	• During an Incident response, the CM provides the impact assessment information necessary to determine if the Incident is severe enough to require ITSCM invocation.
Availability Management	• Availability Management’s perspective is to improve high availability through the elimination of single points of failure from components and systems.

Our Proposed IT Service Continuity Management (ITSCM) Plan aligned to ITIL and Other Processes	
	ITSCM's perspective is to cover fail-over/fail-back concerns, any remote replication and remote system mirroring, backup operations, and provide guidance when no automated technological solution is available.
Incident Management	- The Incident Manager must decide if ITSCM contingencies/capabilities should be used, and when the trigger should be pulled (based on senior management decisions). - ITSCM is accountable for ensuring all knowledge, information, and documentation is available to the Incident Manager for making informed recovery invocation decisions
Change Management	- ITSCM involves many technical components, in separate locations, that must be kept in sync. - A Change Management process that does not provide notification when an impending change has an impact on "recovery" or "failover" components will mean failure for ITSCM.

Our Proposed IT Service Continuity Management Plan meets the following eProcurement solution and support Objectives:

- Maintain service continuity plans (including IT) that support the organization's overall BCP plans
- Complete regular Business Impact Analysis (BIA) exercises
- Ensure plans are maintained in line with changing business impacts and requirements
- Conduct regular Risk Analysis and Management exercises
- Business participates (Involvement from eProcurement Solution)
- Provide guidance to other areas of the business and IT on continuity and recovery related issues
- Ensure appropriate continuity and recover mechanisms are in place
- Meet or exceed agreed to business continuity targets
- Manual "work-arounds" are proposed and in-place.
- Assess the impact of changes on ITSCM
- Ensure proactive measures to improve the availability of services are implemented

Based on our overall analysis of the eProcurement requirements and details, one of the key focus areas is to deliver seamless IT services which are highlighted above. To ensure seamless delivery, we will use our proven Integrated IT Service Delivery Management Model for all day-to-day operations. The application operations and support team will work with the development teams, hosting vendors/partners and other support partners, as necessary, to drive enhancements or fixes/resolutions to any issues to provide IT-Service Continuity. The Integrated Service Delivery Model is based on ITIL Service Management Framework and has been built on the best practices derived from our experience of running application and infrastructure operations for global corporations. The Integrated Service Delivery Model will not only help integrate various service operations across people, process and technology, but also eliminate redundant handoffs and streamline, simplify the Issue-to-Resolution cycle.

Based on the principles above, objectives and ITIL best practices, the diagram below depicts the integrated delivery structure and the collaboration model:

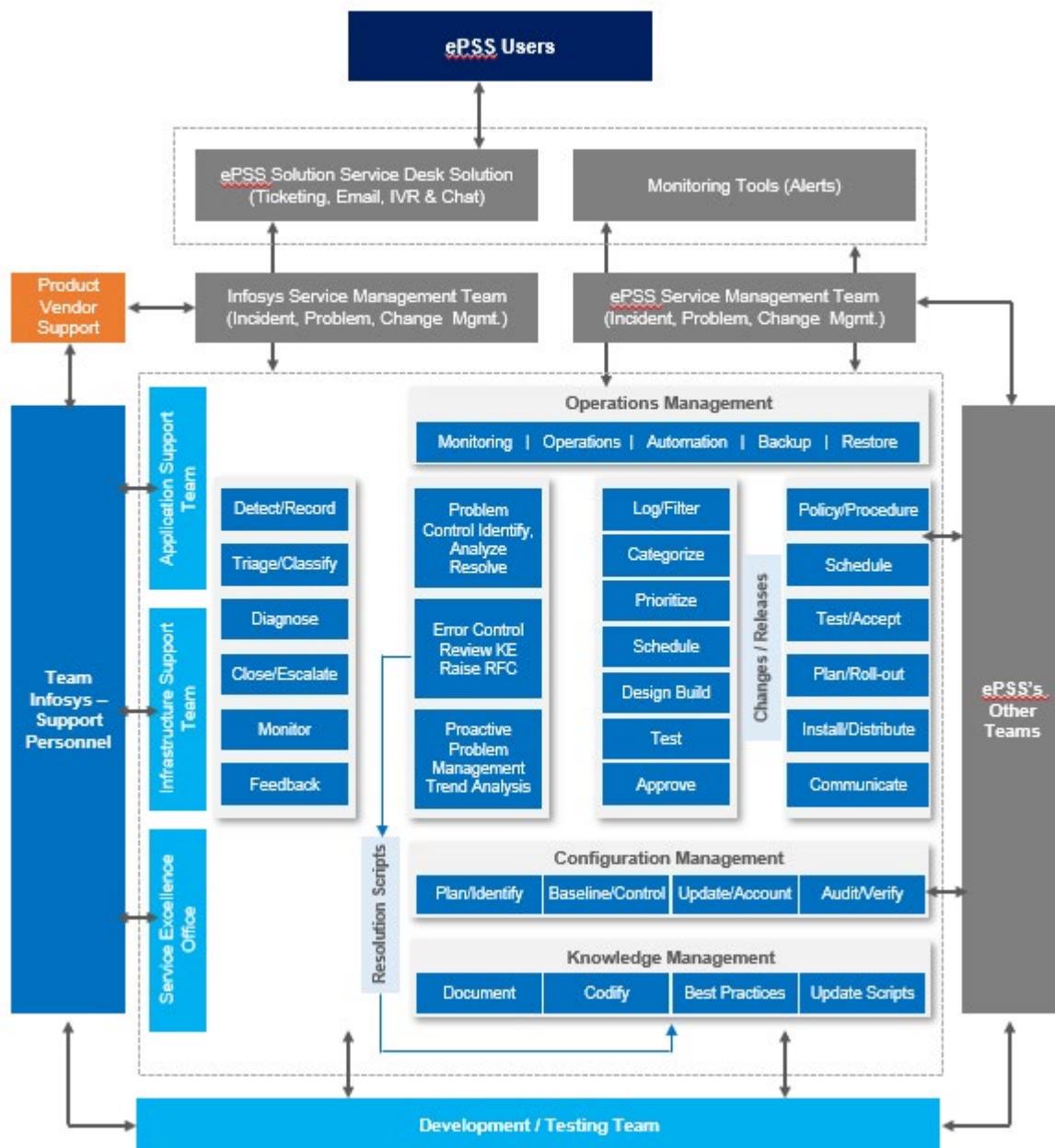


Figure 123. ITIL Best Practice Model

ITSCM Integrated Service Delivery Model

The importance of this model lies in its ability to bring together the various groups responsible for different services. Though each of these groups is aligned to a focus area, they follow standardized processes, methodology and tools to deliver end-to-end services to the end user. This will ensure a seamless resolution of issues irrespective of the type of problems and will provide rich customer experience to eProcurement.

SAP Ariba's Approach to Service Continuity

From an eProcurement Cloud Service vendor perspective, the infrastructure that SAP Ariba is hosted on is fully redundant and our disaster recovery plan provides detailed guidelines for backup, hardware repair, and data restoration. In addition, the application can be completely rebuilt at a number of other locations in the event of a major disaster. SAP Ariba offers two world class redundant sites in the U.S. The primary datacenter is Equinix, located in San Jose, California. SAP Ariba's secondary datacenter

is located in Pittsburgh, Pennsylvania. Over-the-wire backup guarantees data is secure and no more than three hours old.

SAP Ariba breaks its disaster recovery plan down into three tests. The first test validates backup and restore, which happens monthly. The second test validates how the plan aligns with the current processes in the day to day operations; this is done with a walk through. The final test performs a full execution. It is executed after a successful walkthrough. Our disaster recovery plan is tested annually. In the event of a disaster or significant disruption, SAP Ariba has documented plans for business continuity and IT disaster recovery.

Team Infosys recognizes that the State of Maine needs the highest-possible availability and reliability. To that end, SAP Ariba infrastructure is scalable and redundant at all tiers. To provide high availability and reliability, Ariba has extensive error handling and fail-over capabilities. This section describes the main features of SAP Ariba's failover and recovery plans. In order to ensure the highest availability of SAP Ariba, SAP Ariba uses such best practices as:

- Frequent systems backup and maintenance
- Redundant systems
- Proactive customer notification of unplanned down-time
- International support coverage

SAP Ariba Redundancy

SAP Ariba runs redundant copies of all critical software subsystems including application services, enabling automatic fail-over in the event of an error so that there is no disruption of service. SAP Ariba hardware infrastructure is also implemented with automatic fail-over mechanisms. For further redundancy, SAP Ariba is connected to the Internet with two different ISPs running through physically separate conduits to the upstream provider.

In the event of any hardware failure, SAP Ariba Operations will be automatically notified so that the failed equipment can be analyzed and repaired, and the problem prevented in the future. Even if, for some reason, automatic hardware fail-over does not work, the data integrity will still be intact.

In addition to redundant hardware and software, SAP Ariba benefits from the triple-redundant power systems provided by our datacenters. These include redundant connections to power utilities, backup power supplies, and diesel generators that can run for days without refueling, if needed. Inert gas and dry pipe sprinkler systems protect the equipment from fire and inadvertent water damage.

SAP Ariba performs periodic preventive maintenance. This preventive maintenance is scheduled for low-use times, such as weekends. All data in the system is maintained and will wait while maintenance is being performed and resume processing when maintenance is finished.

Ariba uses replication technologies to copy data between data centers within region. Application of these technologies protects against data loss from a disaster effecting a single site. Ariba makes several backup copies of customer data to ensure no data loss happens.

ServiceNow Availability Solution – Advanced High Availability (AHA) Architecture

ServiceNow Advanced High Availability (AHA) architecture is a key element in delivering a true enterprise Cloud. Advanced High Availability meets and exceeds stringent requirements surrounding data sovereignty, availability and performance.

ServiceNow's data centers are arranged in pairs. All customer production data is stored in both data centers and kept in sync using asynchronous database replication. Both data centers are active at all times, each with the ability to support the combined production load of the pair. A production instance from one customer may be operating out of one data center in the pair and a production instance of another customer from the other.

ServiceNow maintains continuous, asynchronous replication from the database in the current primary data center (read-write) to the secondary data center (read-only). To transfer a customer instance from a primary data center to a secondary, ServiceNow designates the secondary to be the primary and the primary to be the secondary if it still exists.

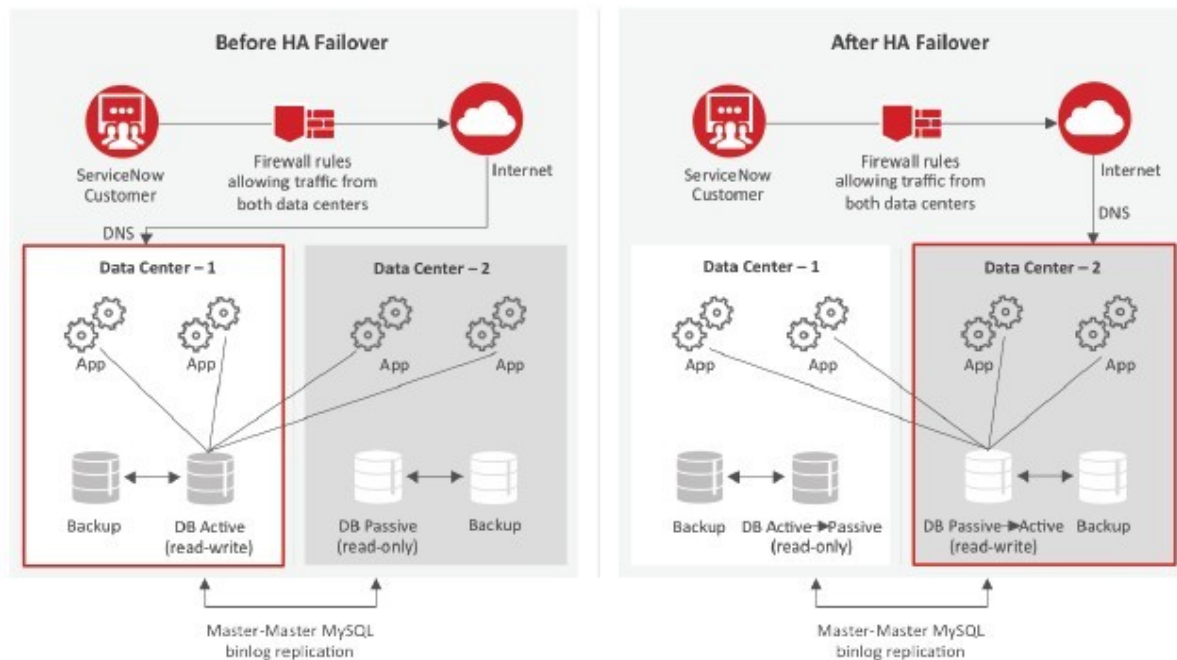


Figure 124. ServiceNow High Availability Overview

ServiceNow High Availability Architecture

ServiceNow's data centers and Cloud-based infrastructure have been designed to be highly available. All servers and network devices have redundant components and multiple diverse network paths to avoid single points of failure.

Identify to the Participating Entity any issues that may adversely impact the Participating Entity in-scope environment and operational requirements and that require analysis of the technical components of the system, including the applications, databases, ancillary and systems software and hardware.

Approach to Risk Management

Our approach to risk management will strategically address key risks throughout the life cycle of the transformation. Team Infosys will leverage our significant past experience from eProcurement implementation, operations and transformation, and our risk management process to effectively manage risks for successful delivery of the eProcurement. In addition, our risk management approach will include an independent risk management assessment at each stage of implementation of the eProcurement. This will support effective program-wide risk management and alignment to benefit objectives from the transformation.

Risk Management Best Practice

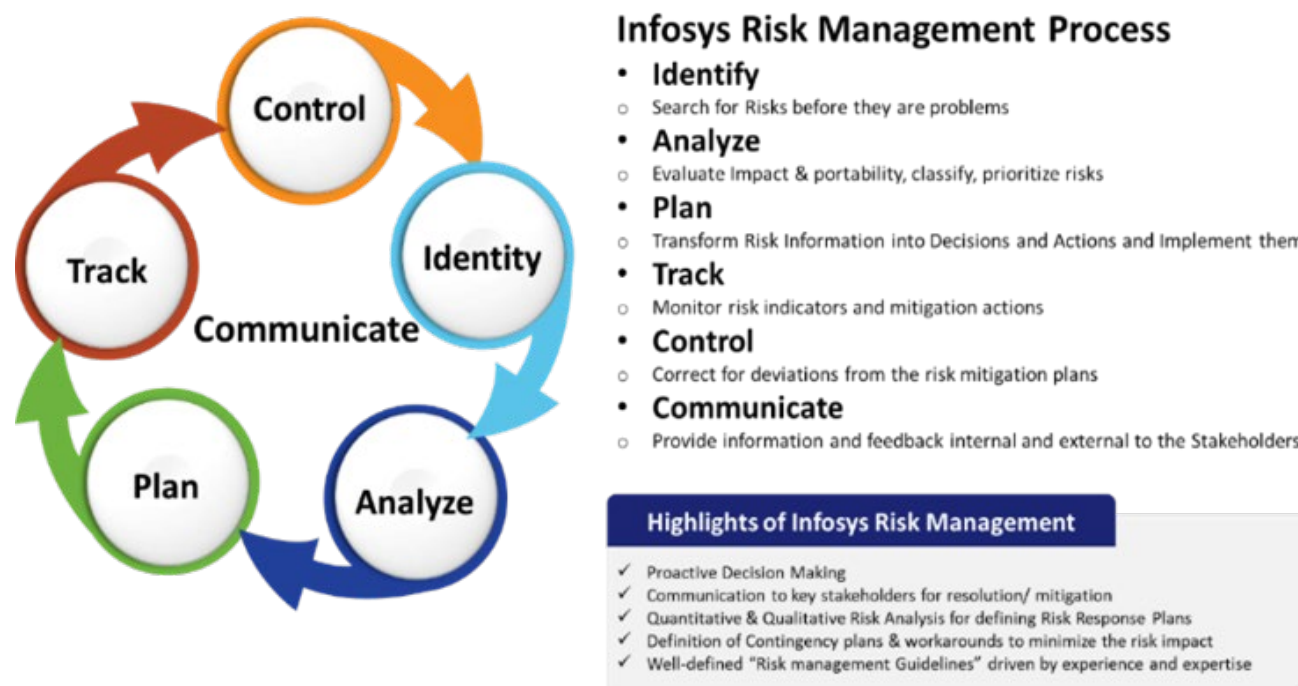


Figure 125. Infosys Risk Management Process

A proactive and robust risk management process at the operational level is a key requirement for reducing uncertainty which identifies conditions and occurrence that are uncertain and result in an unfavorable outcome as risk. The risk assessment and control processes help to identify the various risks, Impact, probability of occurrence and mitigation plan.

These details are captured in a detailed Risk Management Plan and are tracked throughout the project. The Risk Management Plan is continually modified to reflect the changing realities of the project. The risks that have been identified with high probability and high impact are reviewed in the regular status meeting and mitigation plans are modified to meet them.

Risk Management Methodology

Infosys follows a structured approach for risk assessment and risk control which is summarized in table below:

Table 63. Risk Management and Control

Risk Assessment	Risk Control
• A formal risk management plan will be used to log risks • The project manager will identify risks and issues at a project level and log them into the project level risk management plan • Brainstorming and surveying techniques will be used for risk identification • Each risk will be assessed for its probability of occurrence and assigned a value of Low, Medium or High • Each risk will be assessed for its Impact and assigned a value of Low, Medium or High	• A risk mitigation plan will be determined for identified risks • At predefined milestones during the project, status of the existing risks will be re-evaluated • Additional risks, if any, are also identified and risk mitigation steps are executed • All risks with High Probability and High Impact will be constantly monitored

Risk Management for the eProcurement Program

At the start of the project, risks to the eProcurement program will be identified and communicated to the State of Maine stakeholders and Infosys stakeholders, and mitigation strategies will be collaboratively developed as applicable. Risks will be tracked regularly (weekly/bi-weekly) and mitigation plans will be drawn up. Risks will also be retired as appropriate (but logged for audit purposes), and new risks will be added to the list as they are discovered. Infosys will use an eProcurement Risk database or the State of Maine's risk management tool for risk tracking. Refer to the figure below for the detailed risk process eProcurement program will employ.

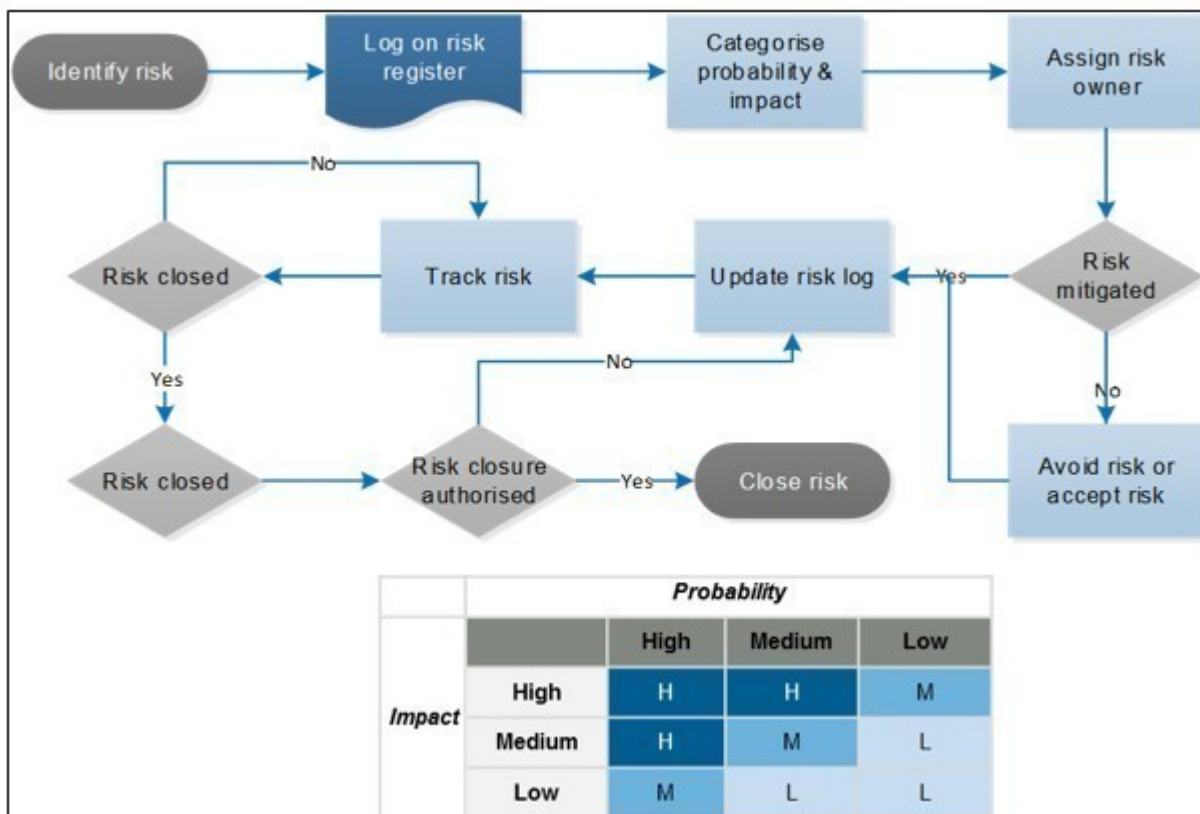


Figure 126. Risk Management Process

eProcurement Risk Management Process

Leveraging Past Experience to Identify Potential Risks

Based upon our extensive Ariba implementation experience with clients such as AstraZeneca, Novartis, United Health and the Government of Canada, we have identified a number of critical risks that have surfaced throughout the implementation programs. The major risk areas for eProcurement implementation are:

- **Program Management** – includes risks related to project schedule, resourcing, scope, benefits management and cost management
- **Business Readiness** – includes risks related to buy-in for the solution, sufficient and adequate training, communication effectiveness
- **Technology Readiness** – includes risks related to the solution build, Cloud/SaaS technology, security and master data (migration of legacy data, management of data quality, etc.)

- **Operations** – risks related to ongoing service delivery after eProcurement go-live (applicable to each major release)

Summary of Risk Management

This section provides a summary of our risk management process as it relates to:

a.) an ability to identify, understand, and minimize or eliminate risk to the State of Maine

Our robust risk management process is preventive and identifies and assesses the impact of risks to the project. The process is designed to uncover risks before they occur. Though not all risks will be identified before the Risk mitigation will be determined for identified risks and evaluated throughout the project at a predefined interval, or for high risks, those will be continually monitored.

b.) how it will lead to a successful implementation of the eProcurement program.

Risk management by itself is not the only factor for a successful implementation. There are many other factors that can derail a program, regardless of how well the risk management process is implemented.

Risk management is a major component for the implementation of a successful program. It will provide a vehicle to address some major areas that can cause a program to fail. The following are examples of concerns:

- Scope management
- Overrun of tasks
- Requirements not properly captured
- Functional design does not meet the requirements
- Technical design does not translate the functional requirements correctly
- Testing does not test all conditions
- Testing environments not setup correctly

c.) thorough analysis of risks that may cause the project to not be completed on - time or within budget.

In general, all risks identified throughout the lifecycle of the engagement will be logged and managed at set intervals based on the severity of the risk. The higher the risk the more frequently the risk will be monitored. There will be a risk management team established with participants from both from Infosys and the State of Maine who will have the authority and accountability to take the necessary actions to resolution. This team's responsibility will vary depending on the severity of the risk and may require project executives to be fully engaged to the effort.

Conduct reviews with the Participating Entity for corrections to performance, functional, integration or technical issues with in-scope environments or operations and incorporate resulting changes into ongoing continuous improvement initiatives.

Provide reviews of Participating Entity use of the Solution to make recommendations/suggestions on how the Entity could make more effective use of the Solution.

Clear Channels for Relationship Management

Communication is an integral factor of successful program management. The Communications Management Plan sets the framework for PMO communication routines and standards that will be applied throughout the eProcurement program. For the proposed communication flow for overall program management and specifically issue resolution, refer to the figure below which includes the processes required to ensure timely and appropriate disposition of project information and prompt resolution of issues. Project managers spend most of their time communicating with team members and other eProcurement project stakeholders, whether they are internal or external to the State of Maine. Effective communications will bridge the eProcurement workstreams which may have different cultural or organizational backgrounds, different levels of expertise, and different perspectives and interests, which may impact or influence the overall project outcome.

During eProcurement Program execution, communication with the State of Maine organizations is a critical component to ensuring the organization is prepared for the impending solution. This is accomplished through the careful planning and execution of the organization change strategy, plan and end user training. Refer to Organization Change Management (OCM) Services and Training Services for specific details. Team Infosys will establish a disciplined and rigorous communications protocol between ourselves and the State of Maine key stakeholders and the leadership team to ensure that there are clear and effective communication channels at multiple levels of the program, and issues and inquiries are brought to the State of Maine's attention at the right time and at the proper level to ensure timely resolutions. With the proposed communication protocol, we will also make sure that the State of Maine stakeholders have an open channel to provide guidance and directions as required. A similar approach has been taken with other clients and many large transformational programs including the Ariba programs at AstraZeneca and Novartis.

Planning project communications is important to the ultimate success of the eProcurement Project. Inadequate communications planning may lead to problems such as delays in message delivery, communication of information to the wrong audience, or insufficient communication to the stakeholders and misunderstanding or misinterpretation of the message communicated. A Communication Matrix will outline various stakeholders against respective communication methods to follow.

Team Infosys also proposes performance dashboard driven metrics to effectively gauge, analyze and report relationship management reporting across the eProcurement program involving all stakeholders, which will capture and reflect the flow of communication and the information that needs to be transparent to all levels of the eProcurement program structure. In addition, ITIL audits and CMMi Level 5 audits will be utilized to identify areas of non-compliance and for improvement suggestions.

Proposed Communication Process for Issues Resolution

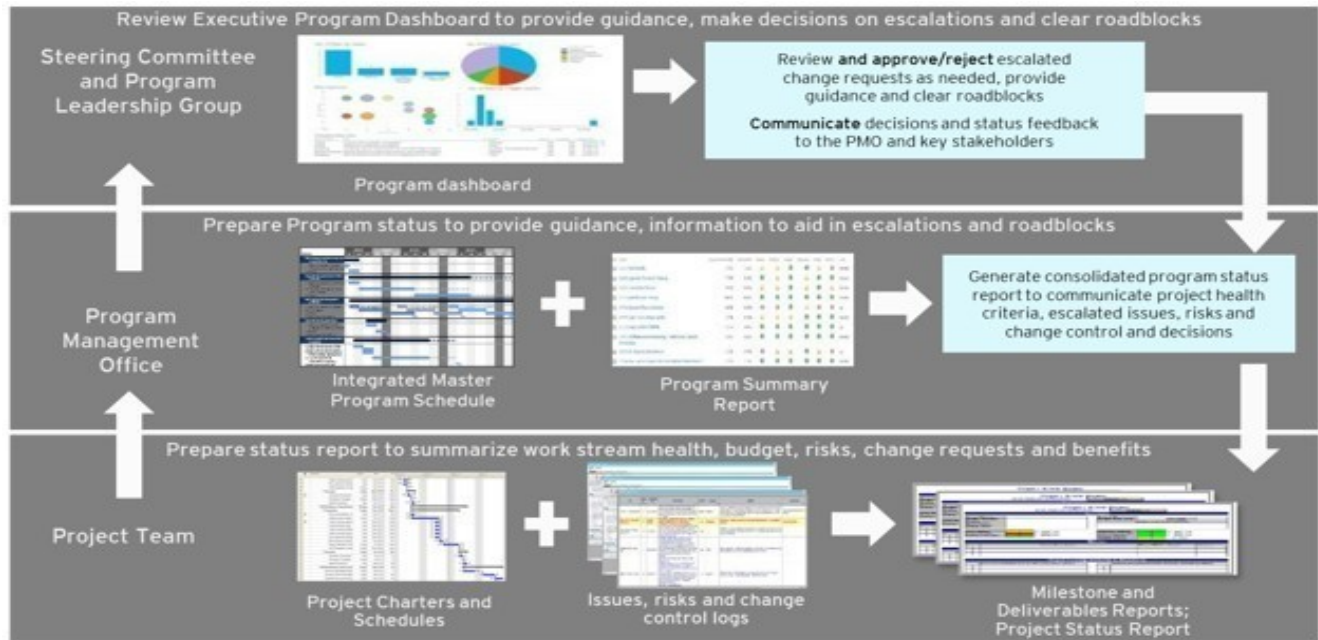


Figure 127. Issue Resolution Communication Process

Proposed Communication Process for Issues Resolution

One of the critical outcomes of effective communication are clear lines of accountability. Below is the eProcurement program communication and meeting approach and plan which we have leveraged before for other large public sector implementation/transformation engagements, to bring Operations and Managed Services efficiencies and effectiveness in delivery for projects of similar complexity, size and transformation objectives as eProcurement.

Communications Meeting Management Matrix

The Communications Meeting Matrix can be referenced and leveraged by the State of Maine as in the figure “eProcurement Program Governance Reoccurring Meetings” below which consists of the Communication Meeting name, the owner responsible for sending out invites, driving participation, and sending out notes within 24 hours using the standard agreed upon format.

Status Meetings and Reporting

Infosys will ensure effective meeting hygiene is adhered to consistently and will include following:

- The eProcurement PMO will distribute a meeting agenda at least two days prior to any scheduled meetings.
- All participants are expected to review the agenda prior to the meeting.
- During all meetings, a timekeeper will ensure that the group adheres to the times stated in the agenda.
- A meeting recorder will take all notes for distribution to the attendees upon completion of the meeting.
- It is imperative that all participants arrive to each meeting on time and cellphones should be turned off or set to vibrate mode in order to minimize distractions.
- Meeting minutes will be distributed no later than 24 hours after each meeting is completed.

Meeting Management Plan

The Meeting Management Plan (separate document) and log will further define a process and schedules to review high-level reporting.

While online collaboration is a basic requirement for project team members, time also needs to be set aside to share information face to face. Infosys incorporates a structured meeting schedule that encourages information sharing in a way that drives the goals of the project.

Infosys meetings are strictly managed, with agendas and time constraints adhered to. Each meeting invite is sent out at least 48 hours in advance, along with a detailed agenda.

There are two types of meetings on projects: Ad hoc and Recurring. Ad hoc meetings typically consist of breakout discussions resulting from a discussion in a recurring meeting that was too long to resolve.

Infosys will provide the following reports to the State of Maine to facilitate the cadence of reoccurring governance meetings adhering to our governance framework:

- Status Reports
- Issue Logs including Resolution Reporting
- Risk Register
- Process Improvement Recommendations – including steps and any additional costs required to achieve
- Change Request / Management Report

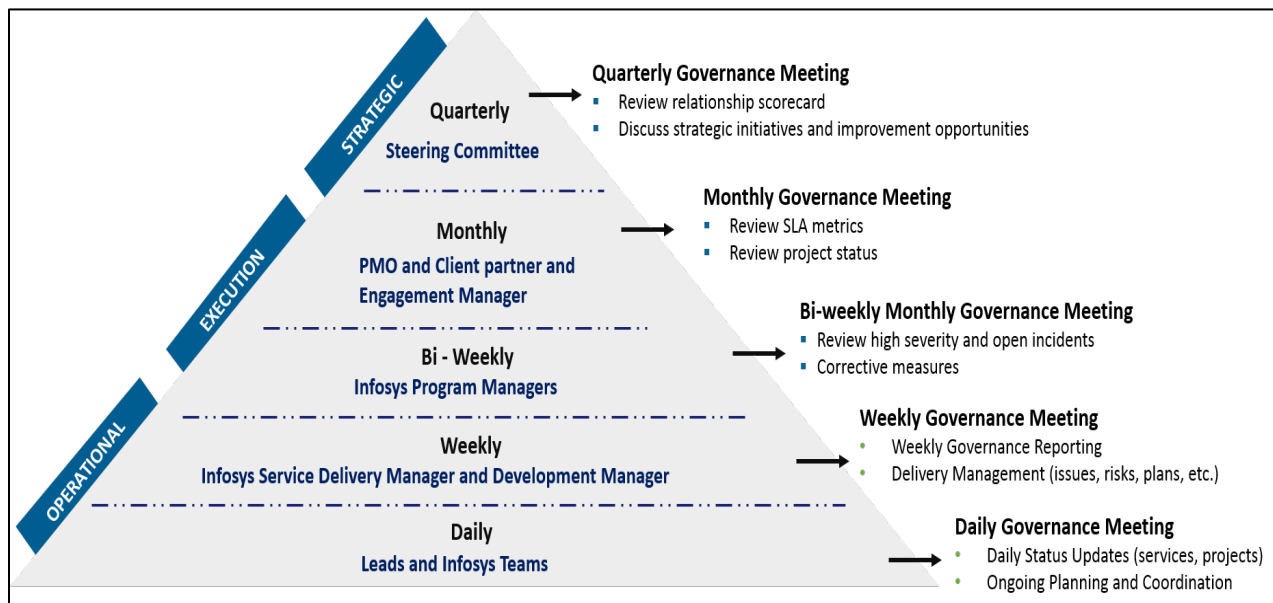


Figure 128. Meeting Management Plan

eProcurement Program Governance Reoccurring Meetings

Communications Methods and Technologies

A folder structure for the entire program will be created within the first 30 days of the eProcurement program initiation. All documents will be stored in SharePoint or a similar repository, including historical artifacts, discovery documents, and source documents, signed off deliverables, all status reports, and important communications. These program documents can be accessed by the entire program team at any time throughout the program execution.

Project and Program Reporting

Infosys' project and program reporting is focused on measurements and metrics providing a clear view of how the eProcurement program is progressing, key decisions and issues that need to be addressed, and what needs to be done to keep the project on time and schedule. Defining and establishing agreed upon program standards for status reporting supports consistent status reporting routines at a program level to provide consistency of communicating status across the platform, from top down.

Status Reports help measure and track work performance, promote continuous improvement, enhance team communication, and provide metrics that monitor quality, efficiency, and timeliness of deliveries. Key project performance indicators will include quantitative and qualitative measurements for overview during Weekly Project Status Reports balance a well-rounded assessment for determining project health. The KPIs for various reports will include measurements for the required reporting criteria and categories.

Resolving Disagreements

Infosys will provide the State of Maine with transparent information regarding the state of the eProcurement program. All involved executive sponsors, project members and the State of Maine Stakeholders will have a clear understanding of who is responsible for which deliverable or artifact, who is the contact person for each work stream, and who is making the decisions.

In the event that a disagreement occurs, Infosys has standardized the escalation process to resolve issues quickly and to prevent any delay in project schedule as outlined in the governance structure, refer to the diagram below.

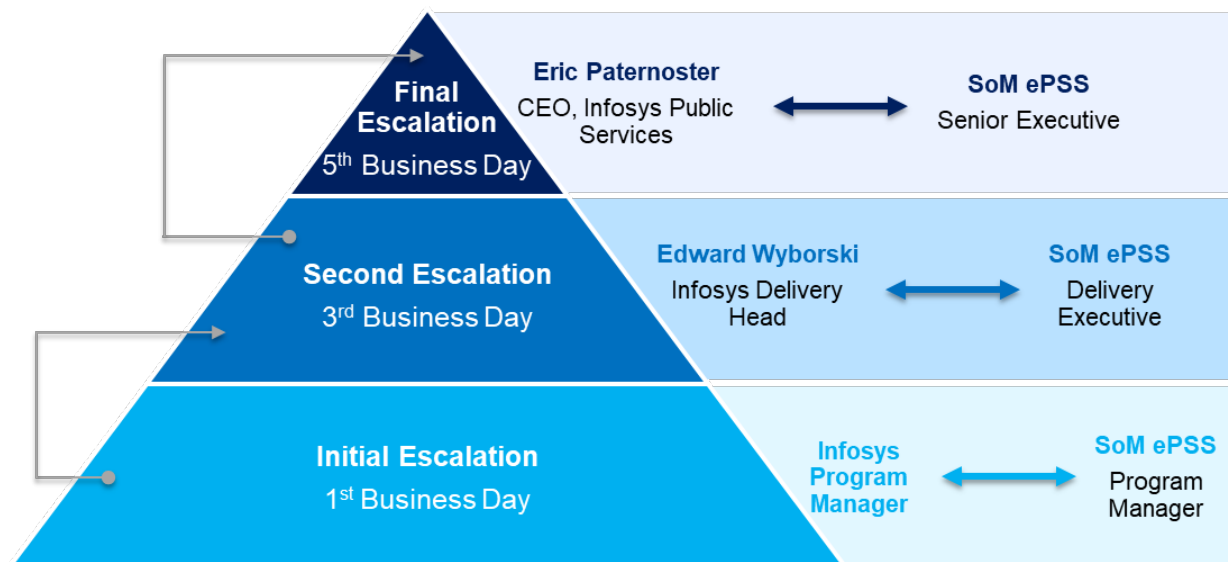


Figure 129. Escalation Process

Proposed Escalation Levels and Process for Issue resolution

Decision Making and Approvals

The eProcurement Decision Management process will be initiated when a decision cannot be made or a higher level of authority from within the eProcurement Governance Structure is required. This process can be initiated for:

- Where approvals are required for specific eProcurement deliverables based on a pre-defined approvals matrix
- An unapproved change request from the Core Solution Committee and Change Control Board

- An unresolved issue from the eProcurement Project workstreams
- A risk which requires authorization for an action plan from the Risk Management Meeting

Following investigation of options, a case will be prepared to enable presentation and communication of the issues, changes or risks, to enable effective decision making. The case will be taken to the next level of the governance structure if a decision requires a higher level of authority. Note: The issue, change or risk may be handed over to a different presenter for the communication to higher levels of the governance structure as applicable.

The overarching goal of the program is to have clear, open and transparent lines of communication across everyone involved to successfully deliver the eProcurement solution as outlined in the RFP. Team Infosys will create partnerships between the State of Maine and ourselves at every level of the governance structure to enable strong communications to take place. Issues and concerns should be raised as soon as they are uncovered or presented to any individual or team to mitigate them in the most efficient and effective manner.

Infosys believes that the success of any large implementation and managed services partnership is possible only through establishing an appropriate governance mechanism which provides optimal control and transparency to the client. Infosys is committed to providing the State of Maine with a robust governance mechanism for the eProcurement Program that is built on a framework to monitor several areas of service delivery, enabling predictable service delivery and adherence to the eProcurement contract.

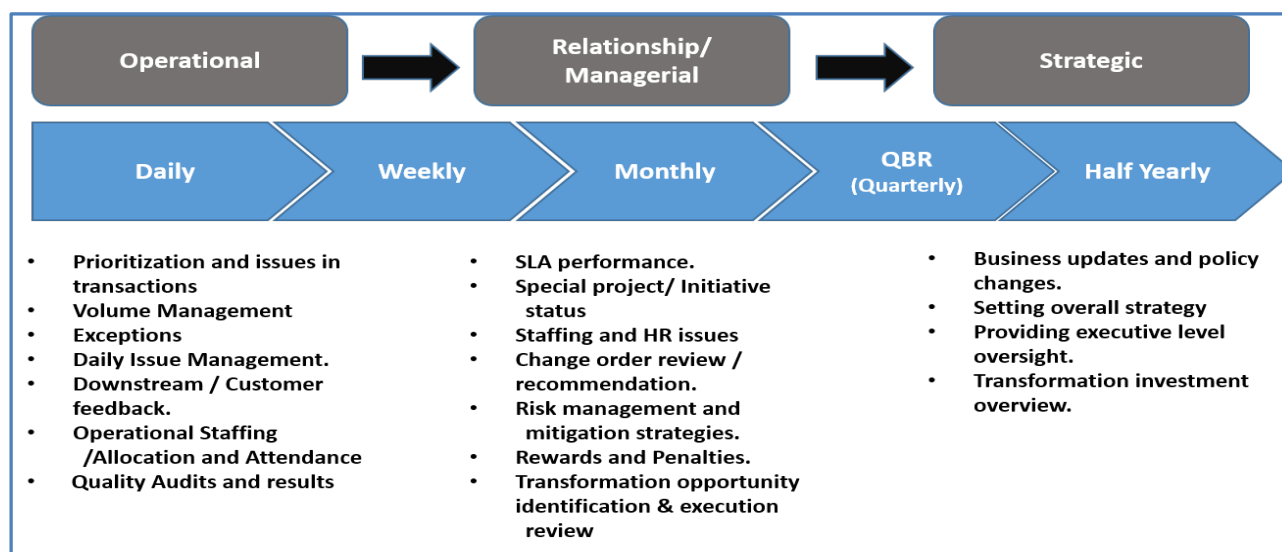


Figure 130. Decision Making Process

Communication Plan

The communication plan as outlined above, covers operational, relationship and strategic focus areas who will receive information throughout the eProcurement program execution.

The governance and communication plan proposed by Infosys is detailed in the table below. Infosys will work with eProcurement to evolve the proposed governance structure, program meeting cadence and communication plan as per requirement, as the relationship matures.

Table 64. Governance and Communication Meeting Cadence Details

Forum	Type	Charter	Frequency	Reporting
Bi-Annual Governance Board	Strategic	• Provide strategic direction • Oversee the relationship between eProcurement and Infosys • Review overall engagement performance • Seek opportunities to enhance that performance through mutually beneficial opportunities • Showcase innovation and consider and approve projects that will deliver significant benefit to eProcurement	Bi-annual	• Strategic Account Review Report • Health of Relationship Monitor • Performance Improvement Report
Quarterly Review Board	Management	• Status update on operations: key highs, lows, critical issues and corrective measures planned • Drive continuous improvement in service delivery	Quarterly	• Program Management Report

Forum	Type	Charter	Frequency	Reporting
		• Provide, direction, oversight and support for approved projects • Review and plan for major changes of scope and direction for the program		
Monthly Operations Review	Operational	• Manage day-to-day operations across all service areas • Manage the level of service delivery against commitments • Drive continuous process improvement	Monthly	• Monthly Run Report • Service Level Reports • Monthly Review Minutes and Actions
Weekly Operations Review	Operational	• Manage day-to-day operations across all service areas, with separate meetings for each area • Manage the level of service delivery against commitments	Weekly	• Weekly Review Minutes and Actions

Maintain an e-mail listing for each business and service owner of the eProcurement solution including third party Solution components. When there is an unscheduled outage or reduction in required performance of the eProcurement solution, the Contractor must promptly notify the appropriate

business and service owner contacts of an outage and restoration of service in accordance with the Run Book or other supporting documents.

Email Notification Service

To notify internal and/or external users of upcoming scheduled maintenance, unscheduled maintenance, outages, service degradations or other events or information, Infosys will implement an Email Notification Service. If the State of Maine already uses either a commercial bulk email service provider or an internal system for such notifications, Infosys proposes using the same system for eProcurement email notifications.

Alternately, Infosys will provide its own service for this purpose. Depending on the expected number of notifications and recipients, this service will incorporate either a Microsoft 365 system for lower volume distribution, or an external commercial bulk email service provider for higher volumes of emails.

Distribution lists will be created for various user and functional groups, so that targeted email notifications can be sent depending on the situation. These lists will be created from the Identity, Credential and Access Management (ICAM) system. Pre-defined templates approved by the State of Maine will be used for all email-based communications to users.

Email notifications will be sent by either the Help Desk Services or the Solution Services groups, after necessary approvals have been obtained from their respective managers and an authorized State of Maine employee. A formalized process will be created and agreed to for this purpose.

Monitor system use/capacity, forecast capacity and review the Participating Entity growth plans during quarterly service review meetings, and if requested due to an unforeseen requirement, participate in the required number of ad-hoc reviews coinciding with these new requirements and infrastructure needs to correctly plan for capacity – periodic capacity increases as well as burst requirements.

Continuous Monitoring Program Services

Many organizations, especially within public sector organizations, have discovered that while traditional security monitoring systems can help information assurance efforts, they are rarely enough to react to today's external, targeted, persistent, zero-day attacks. As a result, leading federal and state agencies and some private sector organizations are beginning to replace point-in-time audits and compliance checks with a continuous monitoring program to help them prioritize controls and provide visibility into current threats

One of the first major challenges in developing a strategy for implementing a continuous monitoring effort is defining the role of continuous monitoring to include threat analysis and risk management support as well as vulnerability monitoring. We break continuous monitoring into two primary categories:

- Proactive: Vulnerability monitoring and asset/device awareness
- Detective: Full-view, context-aware threat monitoring, analysis and alerting

Proactive technologies are aware of device and security state (through configuration and patch management, application monitoring, end point security monitoring, and so on). Such technologies are available to help organizations know everything happening across the network and not just traffic pattern and type, but complete, port-agnostic awareness of content and context of all network data.

To create situational awareness and achieve successful continuous monitoring of networks, proactive and detective monitoring actions must work together and be visible to top-level analytics. For example, an organization using proactive monitoring for devices, system state, and vulnerabilities may provide a level of foreknowledge of whether a known or emerging threat applies to its IT assets. The detective threat-monitoring system should be able to reference these data when analyzing threat information.

To combat advanced problems, such as zero-day malware, command and control traffic, and sensitive data exfiltration, continuous monitoring systems must accurately analyze all network traffic, fuse external threat intelligence, and gather log data from applications, network data and security systems in real-time. This capability includes the requirement for visibility into threats and encrypted malicious traffic hiding in approved traffic types and using approved ports and services.

While each organization's requirements are different, the continuous monitoring strategy should include the following types of both legacy and leading-edge monitoring and correlation capabilities:

- Vulnerability, configuration and asset management
- System and network log collection, correlation and reporting
- Advanced network monitoring using real-time network forensics
- Threat intelligence and business analytics that fuse data from all monitoring feeds for correlation and analysis.

To achieve continuous monitoring, the following guiding principles can be implemented to measure effective monitoring:

- Collect and analyze all network traffic in real time.
- Centralize legacy log and statistics-based data sets.
- Create actionable business analytics.
- Deliver business continuity for application system
- Delivering best in class efficiencies through continuous service and process improvement
- Adoption and implementation of ITIL best practices

Also, while selecting and proposing the eProcurement solution for the State of Maine, we ensured that all the proposed software products have industry best practices based on the SaaS Security Reference Architecture as covered in the figure below.

- SAP Ariba Cloud-based eProcurement solution
- ServiceNow Cloud-based SaaS solution for service and operations management.

All of the eProcurement solution components will be hosted by multiple Cloud provider's solutions, with each hosting area maintaining its own tools for monitoring aligned to SaaS Security Reference Architecture.

SAAS SECURITY REFERENCE ARCHITECTURE

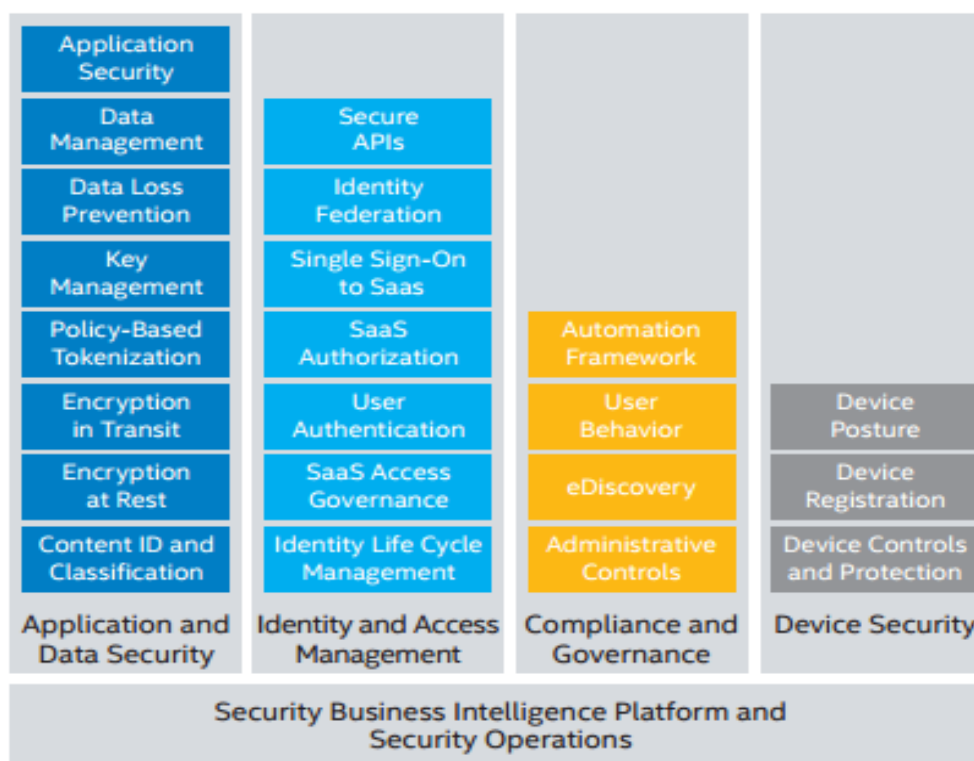


Figure 131. SaaS Security Reference Architecture

SaaS / Cloud Security Reference Architecture

The process strategy for continuous monitoring includes the following initiatives:

- Define a continuous monitoring strategy based on risk tolerance that maintains clear visibility into assets and awareness of vulnerabilities and utilizes up-to-date threat information.
- Establish measures, metrics, and status monitoring and control assessments frequencies that make known organizational security status and detect changes to information system infrastructure and environments of operation, and status of security control effectiveness in a manner that supports continued operation within acceptable risk tolerances.

Continuous Monitoring Process

- Implement a continuous monitoring program to collect the data required for the defined measures and report on findings; automate collection, analysis and reporting of data where possible.
- Analyze the data gathered and Report findings accompanied by recommendations. It may become necessary to collect additional information to clarify or supplement existing monitoring data.
- Respond to assessment findings by making decisions to either mitigate technical, management and operational vulnerabilities; or accept the risk; or transfer it to another authority.
- Review and Update the monitoring program, revising the continuous monitoring strategy and maturing measurement capabilities to increase visibility into assets and awareness of vulnerabilities; further enhance data driven control of the security of an organization's

information infrastructure; and increase organizational flexibility.

Security control assessments performed periodically validate whether stated security controls are implemented correctly, operating as intended, and meet baseline security controls. Security status reporting provides State of Maine officials with the information necessary to make risk-based decisions and provides assurance to existing customer agencies regarding the security posture of the system.

In the monitoring domain, proposed SaaS products have significant strength and capability in providing application systems monitoring services for its customers through widely accepted tools. With our broader expertise and experience in the usage of multiple monitoring tools, same tools and processes can be fine-tune for eProcurement application requirements. These continuous monitoring exercises can be categorized as:

- Proactive monitoring of applications ecosystem with regards to:
 - Application usage and performance
 - Key points of failure
 - Application availability
- Alerts, notifications, and dashboards:
 - Set up alerts for key points of failure
 - Real-time dashboards for preventive monitoring
 - Proactive forecast preparation and validation to detect anomalies before execution
- Provide inputs for batch job execution analysis from Problem Management perspective:
 - Batch job failure trends
 - Batch job delay trends
- Revise SOPs (Standard Operating Procedure) regularly based on all of the above so as to empower the monitoring team. This will ensure faster issue resolution or higher application availability
- Continuous improvement to positively impact eProcurement's KPIs

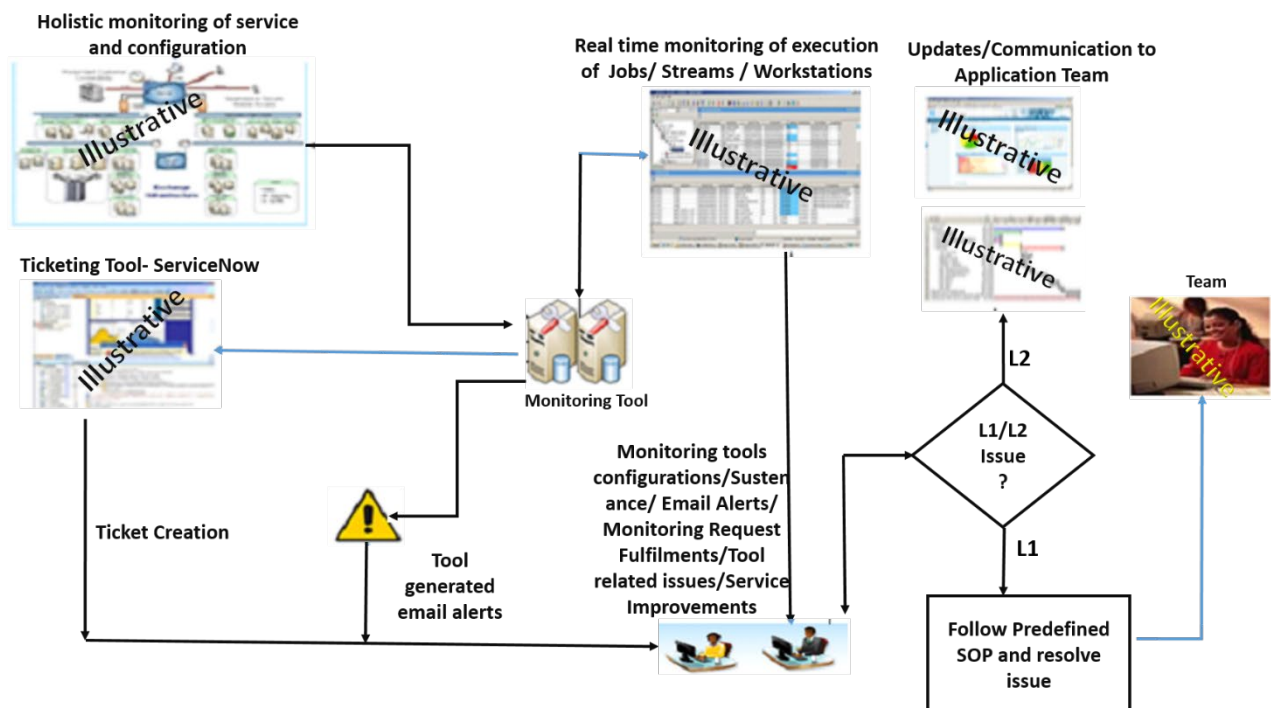


Figure 132. Infosys Support Monitoring Process

Monitoring Workflow

Monitoring Control will monitor all the nuances related to all application / batch processing, workstations and other associated applications. In case of a job failure, it will analyze the issue to detect the key point of failure and resolve it following the pre-defined SOP. If the issue is not in purview of the monitoring scope, then it will be routed to the L2 application team for necessary resolution. Once the issue is resolved, application monitoring controls will continuously monitor and send all the related updates, communication and reporting to the eProcurement security team as applicable. SOPs will be updated in consultation with the application team for any specific inputs as need be.

Application Monitoring: Proposed Approach to Continuous Monitoring of eProcurement

SAP Ariba Continuous Monitoring Service

SAP Ariba uses a centralized monitoring server to provide maximum alerting capability. It monitors network traffic, processes system messages and alerts, application status, transaction status, etc. using a combination of third-party ISAE 3402 assurance audit, PCI DSS certification audit, SOX compliance audit and internal audit to plan, monitor and maintain our security and privacy program.

SAP Ariba has a dedicated Tools Team that has established monitoring for key performance indicators within the solution and production environment. Both monitoring of IDS (intrusion detection system) / IPS (intrusion prevention system) traffic and configuration monitoring of all systems within the production environment is under the tools team purview. This monitoring system is linked to an auto-alerting system and an internal ticketing system for tracking anomalies and environmental incidents. Through these internal tools, development teams can establish active monitoring systems with alerting and automated escalation. This includes log monitoring from the backend of the systems and this is tied to established internal processes related to security incident management. The environment, policies, tickets and reports are reviewed under ISAE 3402 assurance audit every six months.

eProcurement Solution Risk Management follows Risk Management model comprising five process steps:

- Risk Planning
- Risk Identification
- Risk Analysis
- Risk Response
- Risk Monitoring

Infrastructure Monitoring

Since we are proposing Cloud/SaaS application components for eProcurement (SAP Ariba and ServiceNow), infrastructure and continuous monitoring services will be provided by the respective providers.

The eProcurement SAP Ariba Monitoring Service has four key components to ensure continuous monitoring service resiliency:

Table 65. SAP Ariba Monitoring Service Key Components

Key Components	Description
Physical Connection	The proposed solution has highly dependable equipment, such as routers, switches, and load balancers, and are configured and deployed redundantly

Key Components	Description
	to provide high availability access. The solution also maintains a backup data center to enable the offsite storage of customer backup data. Solution uses a backup data center site within the same region as the primary data center whenever possible.
Business Continuity	The proposed SAP Ariba solution will set up a crisis management framework that responds and adapts rapidly to threats posed to its workforce. Crisis management operates on a local, regional and global level and uses a two-step approach: First, emergency response teams take immediate action in the event of a disaster. Following local rules and regulations, these teams have been trained, for example, to extinguish fires in an early stage, evacuate offices, and perform first aid. Second, crisis management teams are authorized to make necessary operational decisions to mitigate and control the situation. They are equipped with an alert network, required documentation and crisis rooms.
Disaster Recovery	Proposed solution critical systems and related infrastructure recovery plans are in place – documenting the continuity arrangements and recovery processes. Disaster recovery testing such as regular cluster failover testing or periodical recovery procedure tests are performed. The plans are periodically tested, reviewed for potential enhancements by SAP and external auditors, and updated if required.
Data Backup	The proposed solution has a formal system backup process and schedule, which includes hardware independent restore and recovery capabilities. All backups are run automatically; their respective frequency depends on system availability requirements. The restore of data can be requested via ticket and needs approval before being executed. Appropriate processes and automated tools are in place to validate backup integrity and backup logs are reviewed daily to detect and correct backup failures. The backups are stored off-site on redundant media in the designated region.

Analysis Methods, Response Mechanism, and Review and Updates

Based on our analysis of the State of Maine's requirements, one of the key focus areas is to deliver seamless services to eProcurement users. One of the key aspects of seamless delivery to control the lifecycle of all the incidents / problems and ensure that the data gathered is analyzed and the learning from the same helps in making better future decisions. This function dedicated to analyzing the incidents, follows the these activities:

- Log all problems and create problem tickets with the applicable priority level.
- Determine the root cause of the incidents comprising a problem, and then, initiate actions to improve or correct the problem.
- Implement permanent resolution or acceptable work-around
- Validate that problem resolution and corrective actions taken are sufficient to confirm that the root cause identified does not reoccur in same or similar environments. This includes update of manuals, procedures, and other documentation. Communicate the problem management process to the State of Maine and to each necessary stakeholder.
- Regularly survey incidents to identify reoccurring Incidents for which the cause is unknown.

- Update the KEDB (known error database) with all relevant information, including documented workarounds for known errors.
- Perform trend analyses on the volume and nature of problems in order to identify areas for improvement, and report on the trend analyses and improvements to the required stakeholders.
- Recommend measures to avoid unnecessary reoccurrence of problems and implement measures including via the change control management process, if applicable.
- Coordinate problem tracking efforts and notifications to all relevant parties and maintain regular communications between all parties until problem resolution.
- Implement measures to avoid reoccurrence of problems.

The flow chart below illustrates a typical problem management flow. This would be refined based on discussions with the State of Maine Service Management team before it is implemented in the context of the eProcurement application and infrastructure operations support.

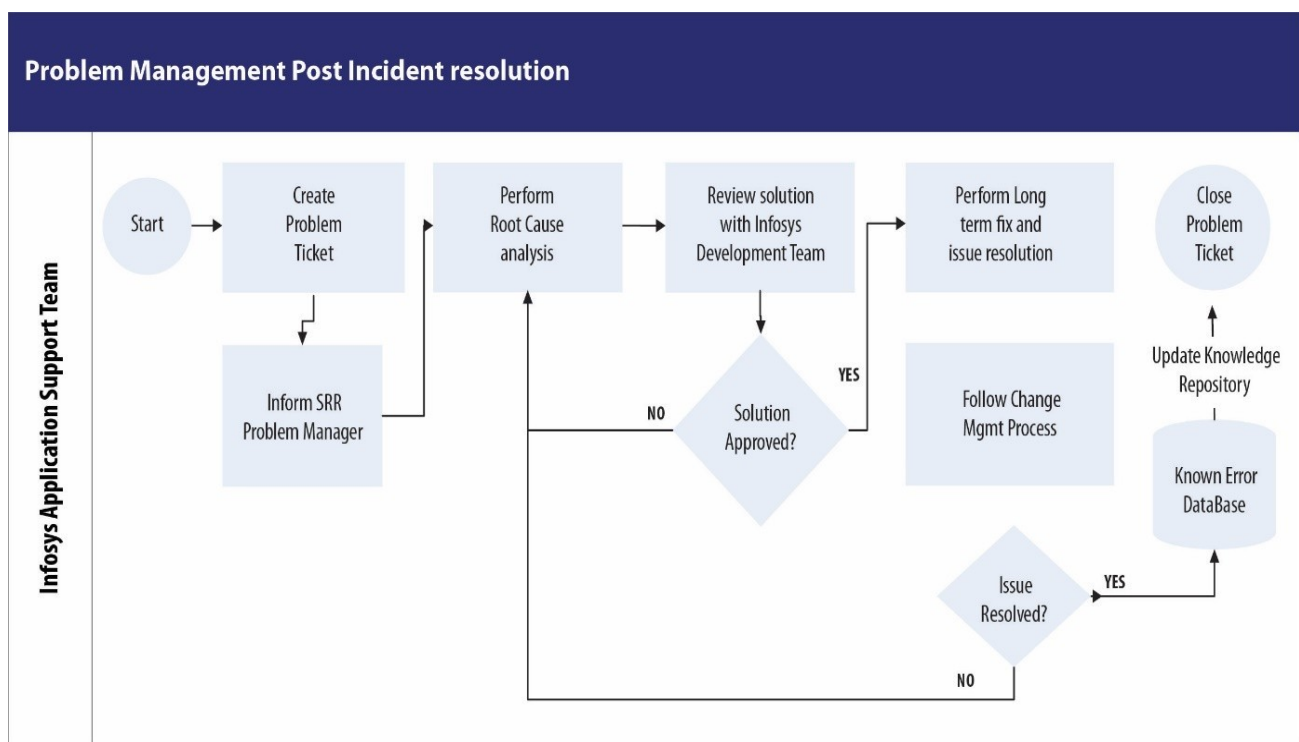


Figure 133. Problem Management and Post Incident Resolution Model

Program Management Incident Resolution Flow

Continual Service Improvement

Infosys uses the principles of process management, combined with industry leading process improvement techniques, to map process measurements to business value and thus creates a systematic approach to continuous value creation. To have strategic focus on continuous improvement, Infosys proposes to create a separate team as Service Excellence Office (SEO). The SEO is a centralized managed service that continually evaluates current performance against those attributes that create value for an organization. Performance gaps are identified and, with tight linkages to governance and IT service management, are driven through the SEO's value improvement cycles.

Listed below are some of the key proactive initiatives that SEO would take to keep propelling forward eProcurement's improvement journey:

- Continual Service Improvement (CSI) library: Focused on sharing/ leveraging best practices.

SEO office is a centralized office for knowledge and improvement in the current process and suggests emerging technologies insights helpful for any pain points in the current process.

- Value tracking: Focused on value delivery, tracking continuous improvement, aligning all Infosys efforts to specific improvement levers and change enablers and quantifying benefits and value.
- Transformation workbook: Focused on collation and overall tracking of optimization opportunities.

Implement Lean IT Operations

Process Quality Assurance

Process Quality Assurance will be a key focus area for SEO to ensure process adoption, adherence, and productivity improvements. The SEO team will drive ITSM- and process-based improvements by working collaboratively with the State of Maine and Infosys delivery teams. Objective of this function is to sustain the existing process and ensure compliance with process standards. This layer will also focus on conducting periodic reviews and benchmarking exercises to identify process improvement opportunities. This function will focus on measuring the maturity and quality of the processes and how the process performance benchmark with the industry.

The diagram below depicts the proposed model for process quality assurance:

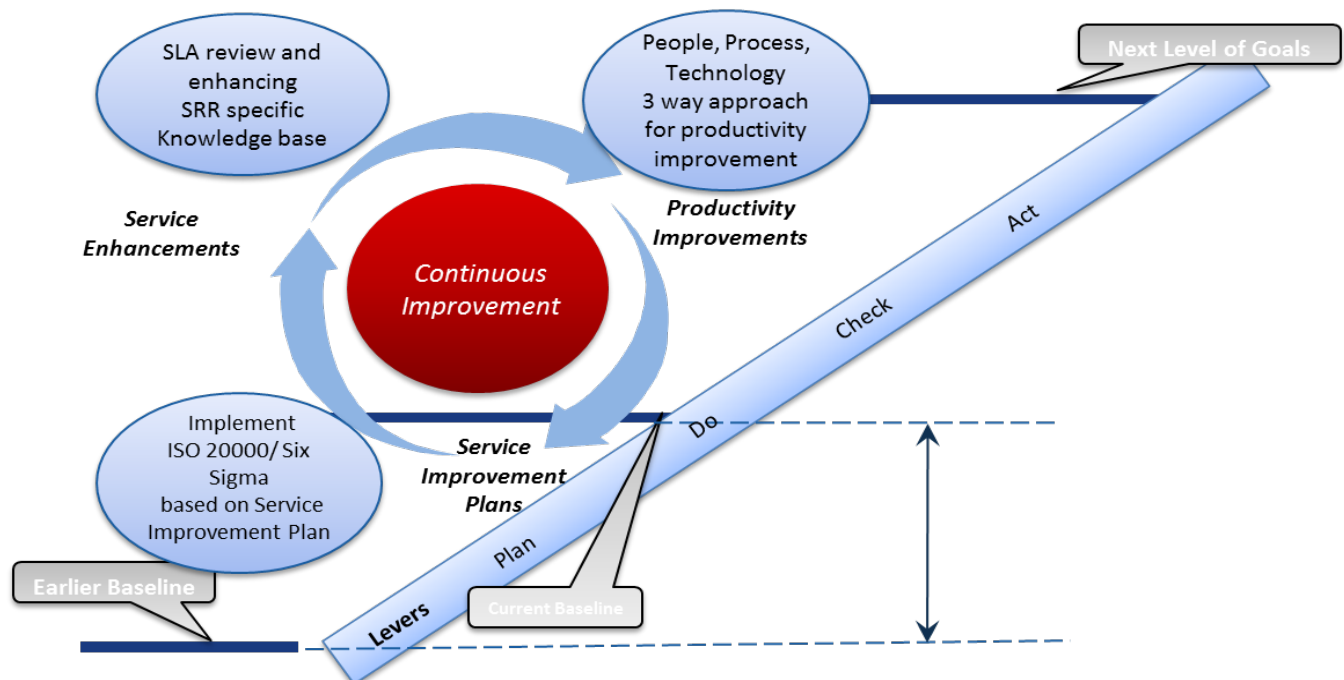


Figure 134. Process Quality Assurance Model

Continuous Service Improvement Model

Infosys will identify the potential areas of optimization that would be focused on by the Service Excellence office to drive continuous improvement on an on-going basis. The table below details the potential areas of optimization and corresponding value delivered for each area:

Table 66. Areas of Optimization

Optimization Areas	Description of Value delivered
Resolution Optimization – Reduce Mean Time to Resolve (MTTR) to improve availability	The Resolution Optimization Component is a unique differentiator of our delivery model and is supported by the Service Excellence Office. This model continually analyzes all support requests to determine the appropriate support level and the effort required while maintaining SLAs. Opportunities for resolution automation, process improvement and effort reduction are identified and driven through SEO
Drive Proactive Problem Management to eliminate of Incidents through Problem Management Platform	- Identify the frequently occurring issues, patterns and related trends through “Pareto Analysis tool” - Focus on high impact apps for problem management, possible automation areas - Identify common issues/problems across applications components through correlation analysis - Prevent common causes of multiple application component failures, related tickets
Service Management Optimization	Variance and exception-oriented reporting and analysis that helps to guides problem management efforts, as well as oversight of ticket coding accuracy and quality to maintain accurate information for data analysis and mining.
Quality Oversight and Defect Management	The reporting, analysis and action plans for service defects, such as miss-assigned incident records, incorrect diagnosis, and excessive resolution times.
Industry Best-Practice Guidance	Connection point to the metrics, targets, and methods that industry best-practice standard authorities – such as Gartner, and the Service Desk Institute – espouse, and a roadmap for implementation and/or achievement.
Strong Opportunity Pursuit/Corrective Action	A tested method that applies the core principles of Lean Six Sigma, incorporating use of known solution

Optimization Areas	Description of Value delivered
	libraries to enable known solutions for previously experienced undesired conditions, and a highly structured investigative and recommendation process for new unexpected, undesired conditions.
Multi-Dimensional Metric Methodology aligned with the State of Maine's Business Goals	Development and application of a Value Map Control Plan, including a value map that establishes and rationalizes all measurements against a clearly stated Business Goal, and accompanying Critical Success Factors.
Automation of Services through Infosys Automation Platform	Infosys will come up with the areas of Operations and Maintenance of eProcurement Application Support operation services which can be automated. Typically, routine monitoring and administration areas of services can be considered for automation e.g. database monitoring, database storage alerts, data cloning tasks, data backup tasks, code migration etc. With approval from the State of Maine, Infosys will automate the tasks and/or activities identified earlier.

Manage the security functions related to the solution including administrative access and passwords and the related security controls to maintain the integrity of the solution, based on the Contractor's standard security processes.

Identity, Credential and Access Management

SAP Ariba System Access

SAP Ariba supports remote authentication and single sign-on (SSO) via the client's Corporate Authenticator using SAML 1.1 and 2.0. The following benefits of using a corporate authenticator over basic application managed user ID/password authentication are:

- Convenience for users: Users do not need to remember separate usernames and passwords for their Ariba On-Demand solution accounts. If your organization uses SSO, users will be automatically authenticated for Ariba On-Demand solutions whenever they log in to your corporate network.
- Better security control: Your organization might have greater security requirements than the authentication mechanism of Ariba On-Demand solutions.
- Better account management: When users leave your organization, their access to Ariba On-

Demand solutions is automatically revoked as part of your organization's network policy. Removing their log in permission from your corporate network means that they can no longer access Ariba On-Demand solutions.

- Configuration Steps:
 - Provide Ariba your corporate authenticator's public certificate, authentication URL and logout page URL.
 - Ariba provides you a return URL for posting the SAML Response, to be configured in the corporate authenticator.
- Process Flow:
 - A user accesses the URL of an Ariba On-Demand solution.
 - The Ariba On-Demand solution notices that your organization is configured for Remote Authentication and, instead of displaying a login page, it redirects the user to your corporate authenticator. Other relevant information such as the Ariba landing page (after login) will be stored in the session details for this interaction.
 - The corporate authenticator authenticates the user and redirects to Ariba for login.

A unique username and password for user authentication is required to sign in to the eProcurement solution. A password complexity scheme is in place and mandates case-sensitivity between 8 and 16 characters in length. Passwords can include any Latin characters and punctuation marks and must include at least one numeral between the first and last character. They must also include at least one letter.

The technology is configured to require users to change passwords at least every 180 days. The password complexity scheme applies to all systems. Password complexity and change management is technically enforced where feasible or testing is performed for compliance.

The standard prior-password parameter is that no one password can be reused for four password change cycles. This count can be customized to be more or less than four if needed. Lock out occurs after five failed attempts to log in. Once logged in, session timeout occurs at 30 idle minutes. Both of these parameters cannot be customized.

eProcurement Application Access

Application access is controlled by groups assigned to users. Groups have roles that control permissions for resources and actions. Users can be assigned to multiple groups, and therefore can have multiple roles. Once the user is deactivated or suspended in the ERP System or in eProcurement system, the user would lose access to eProcurement system and would not be able receive emails from the eProcurement system (notifications, approval requests and workflow related status emails). The user will not be able to access the eProcurement until they are reactivated.

There are 2 groups which distinguishes internal and external users. They are mentioned as below:

- External: This permission defines external users of eProcurement, who are typically suppliers and other outside entities. It is used to distinguish them from users with internal permission, who are usually members of buying organizations.
- Internal: This permission defines internal users of eProcurement such as Buyers and other State of Maine employees.

The internal users in turn will have specific groups to perform specific tasks for example: A purchasing user can only create requisitions, query and run reports for the requisitions that have been created by him/her and his/her subordinates.

On the other hand, the user with the purchasing administrator group can do the administration activity on the purchasing documents like querying all requisitions, managing approvals for requisitions and closing/reopening Purchase Orders.

Similarly, supplier users who are external users when they punch in to the Ariba solution to create invoices for contracts can view and create invoices only for a particular contract and will not be able to see any other contract or documents for which they don't have access to. The user group mapping is loaded using the Import User Group Mapping task in Ariba. This will be done on a daily basis, which will keep the group assignment up to date.

All of the State of Maine users in the cloud application will be created from the backend authentication system, while the sign in ID would remain the same as their network login ID.

State of Maine Internal User Process Flow

State of Maine Internal User: User would be required to login the State of Maine's network and adhere to the current login security. Once logged in to the State of Maine's network, then the internal user will be able to access the cloud application without re-entering the login credentials, via SSO. The internal user will be assigned the permission called Internal.

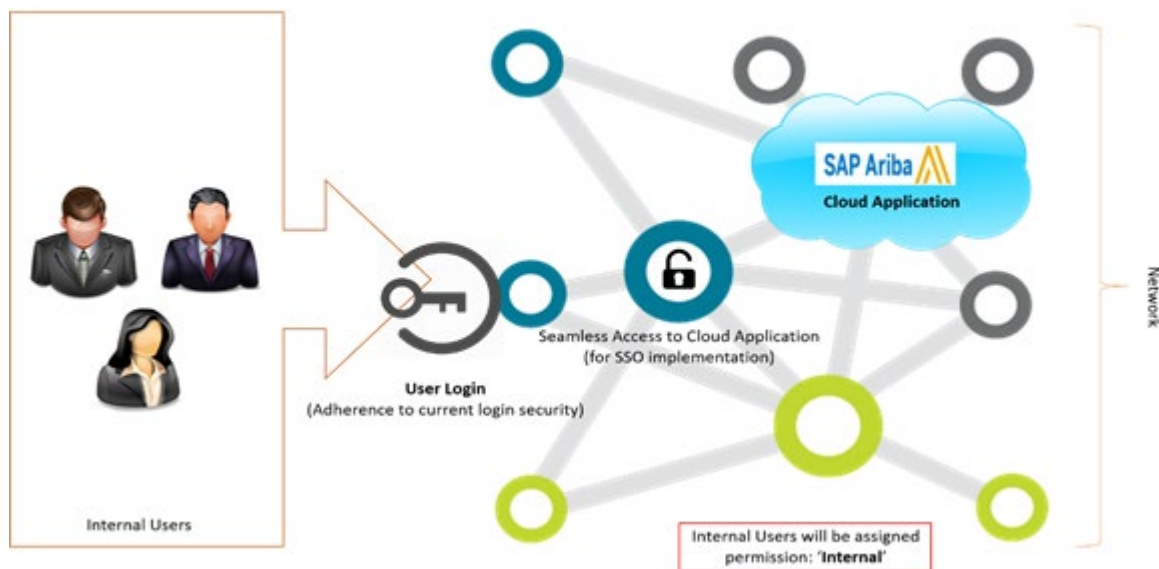


Figure 128. Internal Users Process Flow

State of Maine External User Process Flow

State of Maine External User: External users are not required to log in to the State of Maine's network and their details need not exist in the State of Maine's user database. These users will be created by loading a .csv file, however the external users are required to log in to the cloud application, and the authentication process can be customized to implement login authentication process which are similar to the current State of Maine's internal authentication process. These users will be updated with a permission called External as shown in the graphic below.

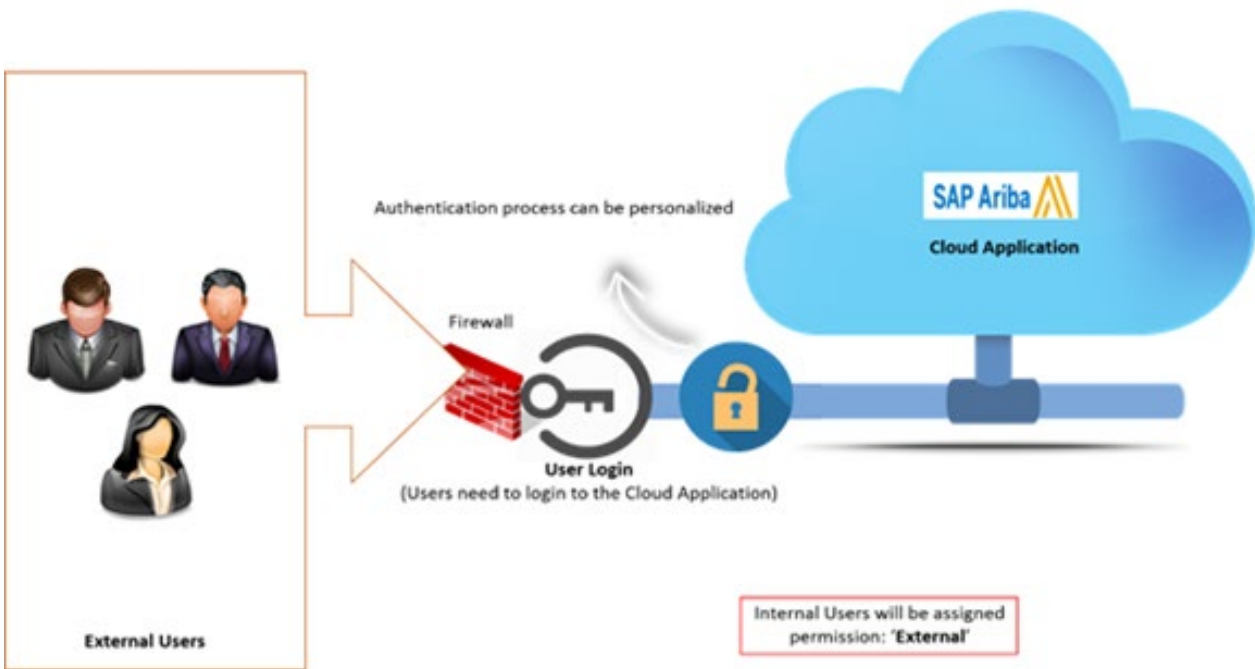


Figure 129. External Users Process Flow

System Admin Process Flow

System Administrators: System administrators are the “super users” who have the capability of accessing and verifying every object in the system, these users are granted with all the groups, roles and permission that are required by system administrators. These users are similar to the State of Maine Internal users. The State of Maine must create the contractors in the State of Maine employee database. These users are required to log in to access the cloud application using the SSO authentication provided by the State of Maine, which is same as the State of Maine internal user authentication process. The figure below illustrates this process flow.

- **Infosys Support Team:** The Infosys support team and the cloud provider’s support team would access the Cloud application outside of the State of Maine’s network. The support team would also need to have their accounts created in the cloud application and assigned with all the necessary groups, roles and permissions or privileges to access the incident.
- **Data Separation:** The software's data model keeps different customers' data strictly separate. Realms isolate customer data. A distinct realm is used to identify individual customers and store their data. Realms are sealed off from other realms such that it is not possible for a given realm to see or access data from another realm.

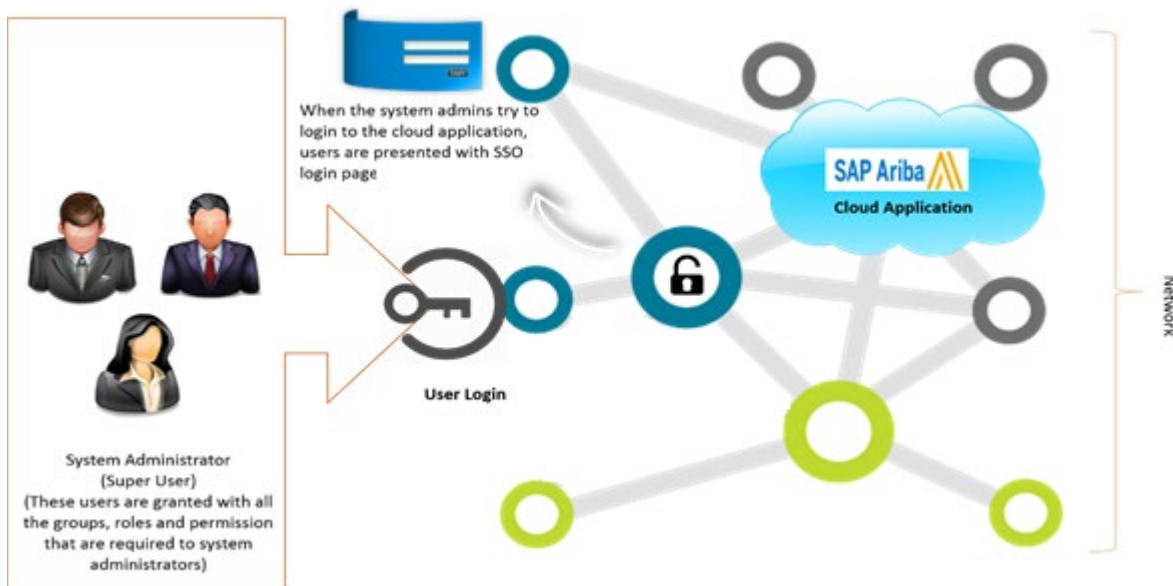


Figure 130. System Admin Process Flow

Every object in the system is marked with the customer account to which that object belongs. The mark is persisted in a column in the table associated with the database object. Users logged in to a customer's account may only view and edit objects that belong to that customer only. This is enforced every time an object is retrieved into a user's session by validating that the customer account of the object is identical to that of the user.

All internal processes must be designed according to the three basic principles outlined below.

Needs Basis Privileges

Individuals within the State of Maine must be given only those privileges that are needed to fulfill his or her duties. Access to data and functionality within eProcurement modules is based on groups that determine which features of the service a user can see and work with, and what data the user can access. Groups allow customers to manage access control in a way that reflects their organizational structures and the roles of users within those structures.

eProcurement provides a single point of integration and administration for users and user profiles, organizations, groups and group memberships. This common data is shared and synchronized across eProcurement modules automatically. The User and Group objects can be managed from the provided UI or populated from a variety of sources, such as corporate systems and/or flat files. For example, the user object can be populated from an external HR system. eProcurement provides capabilities to perform batch upload from the user interface, either through webpage-based interactive file upload, or via an automated (scripted/scheduled) HTTPS push of data from HR and ERP systems.

Verify the Need before Granting the Access

Authorized State of Maine administrators have to verify the need for the access request before a privilege is granted to an individual. The authorized administrator knows the details of the access rights and the consequences and justification for access rights. It is strongly suggested that the administrator user who grants the access must be different from the access requestor.

Separation of Duties

Critical business processes must be designed to obey the principle of separation of duties. Separation of duties means that different individuals must fulfill different tasks to complete a process. No individual can run the complete process alone. The concept of “separation of duties” can further be implemented as “two-person control” or “dual control”:

- Four-Eye Principle/ Two-Person Control mean that two individuals check each other’s work. A single individual is allowed to run the whole process, but a second individual must verify the completed process.
- Dual control means that two individuals have to do the same job together or work together to complete the job. A typical “dual control” example is the practice in which two individuals are required to open a sealed envelope containing an administrator password together.

The distribution of tasks across different individuals is usually more cost efficient than “two-person control” or “dual control”. Management defines which processes are business-critical processes. The default rating for all processes pertaining to the transfer of funds is as critical unless the process owner specifically states otherwise.

All processes for granting access rights and privileges must be documented for audit purposes and checked whether the request conforms to the principles of “need basis”. Employees can, for example, get confirmation from the requestor’s direct superior, but in general this should be part of the process definition. For auditing purposes, employees must document the access rights and privileges that are granted.

Revoking Access

A process must be defined to ensure that privileges and access rights which are no longer needed, are revoked accordingly. Regular time intervals are defined when all the access rights and privileges granted must be confirmed again.

The events “termination of employment”, “internal relocation” and “reassignment of tasks” must trigger an immediate revoking of access rights and privileges.

Summary of Identity, Credential and Access Management

Application access is controlled by groups assigned to users. Groups have roles that control permissions for resources and actions. Users can be assigned to multiple groups, and therefore can have multiple roles.

All the State of Maine users in the cloud application will be created from the backend authentication system, while the login would remain same as the network login ID. Roles and groups can be assigned and revoked based on the need.

1.2.6.2 *Organizational Change Management (OCM) Services*

Deployment and Post Go-Live Support during the managed services period entails a set of activities that take the State of Maine through go-live decision making into the desired future state, with a focus on sustaining performance, new ways of working proficiency, and continuing to enhance user adoption and solution stabilization.

Proper support before, during, and following full solution go-lives is critical for a program and its people to successfully adopt new ways of working and transition from program-led activity to business as usual. It is also vital so that the deployment can deliver on the expected value. During delivery of managed services, we will work with each State of Maine to ensure that communications and training are updated when required to continue to support user adoption.

Continuous learning process

We are invested in continuous learning by complimenting and expanding knowledge of new skills and expertise of those impacted groups; both within State of Maine's workforce and their suppliers. A successful continuous learning process delivered as part of solution managed services encourages learning by providing clear communications of solution changes along with the requisite tools and knowledge. The following three pillars described below are key elements in maintaining a stable solution (process and technology) where high levels of user adoption and solution capabilities are maintained and enhanced.

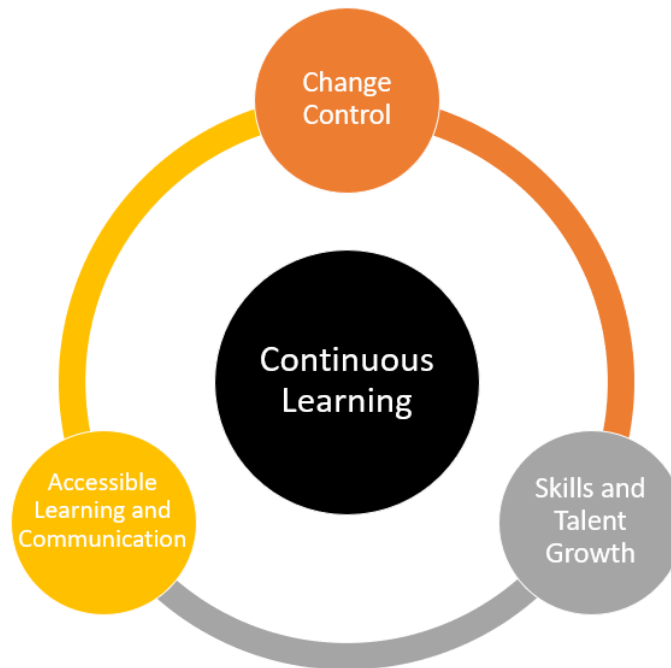


Figure 131.Continuous Learning Process

Change control

The change control governance process is the source of enterprise architecture changes that will impact the eProcurement solution. The leading practice for identifying a solution change request is to include the change to the personas or organization impacts which is part of the enterprise architecture. Learning organizations actively participate in the change control process to identify and assess stakeholder impacts as key inputs to organize and plan for ongoing communication and training needs.

Skills and talent growth

The personas that are refined throughout the implementation are carried through the continuous learning journey that is maintained during the managed services period. The impacts to user groups, internal and external, are identified during the change control process such that there is adequate lead time to respond, incorporate, communicate, and re-train where needed. Once incorporated into the solution, the learning roadmap mapped to those personas are applicable to those that are new to the organization or transitioning into existing roles.

Accessible learning and communication

Throughout the implementation, the State of Maine's existing learning management processes and tools will be engaged to increase the access to the relevant and timely information that provides the foundation of adherence to processes and yields better decision making for the states' impacted

stakeholders. The development of training content and digital training solutions will consider their end-state use platforms to encourage re-usability compliance with those platforms.

To ensure that users are kept abreast of updates and new releases associated with the solution, update and new release scope/impact outlines will be created and provided to the State of Maine to support creation of stakeholder communications using the applicable State of Maine channels and media.

1.2.6.3 *Training Services*

As described in the preceding section on the Continuous Learning Process, training materials will be updated as required to reflect solution updates and new releases so that they can be utilized for refresher training as well as training for new users.

1.2.6.4 *Catalog Support Services*

Setup/Configuration of hosted catalogs

The solution provides self service capabilities to suppliers to manage catalogs. Suppliers can create catalog files that describe products and services and upload them to customers that have an active trading relationship on Ariba Network.

Once the supplier publishes the catalogs, these files are routed to designated approvers from the State of Maine. These approvers review the content of the catalogs and approve the same.

The Infosys Managed services team will provide the following services to support setup and configuration of hosted catalogs:

1. Monitor status of catalogs uploaded by suppliers and notify State of Maine of any errors.
2. Push catalogs uploaded by suppliers to the State of Maine identified catalog approvers via the system.
3. Activate approved catalogs.
4. Make activated catalogs visible to end users.
5. Setup catalog views to restrict visibility of catalogs.
6. Setup key words and equivalent words
7. If the suppliers do not have the capability or technical proficiency to manage their own catalogs, the managed services team will convert supplier's catalog content to a format acceptable by the solution and load the files.
8. Deactivate catalogs upon State of Maine's request.
9. Suppliers can also contact the product vendor (SAP Ariba) for obtaining support on issues encountered during catalog loads.

Setup/configuration of punchout sites

Configuration of PunchOut catalogs also involves uploading a catalog file by the supplier via Ariba Network. All the functionalities and services described in the above section are applicable to punchout sites as well.

The following additional services are provided by the managed services team:

1. Support the State of Maine in verifying connectivity with supplier's punchout site.
2. Product vendor (SAP Ariba) supports the supplier's efforts of establishing connectivity between State of Maine's procurement solution and supplier's punchout site.

3. Product vendor also supports the resolution of connectivity issues with the supplier's punchout site.

1.2.6.5 *Help Desk Services*

ADSL's familiarity with eProcurement solutions includes SAP Ariba, Coupa, Kissflow, Microsoft Dynamics, and Oracle Netsuite. ADSL can support any eProcurement solution by leveraging standard operating procedures (SoPs) and its Knowledge Base (KB). These would be developed and validated during transition and shadow support. During shadow support the KB's and SOP's are tested and validated for accuracy and effectiveness. They are reviewed and renewed as needed.

Additionally, IPS will staff a Service Desk Governance Lead, well versed in running a procurement service desk. The Lead will work closely with ADSL during the implementation and steady-state phase of the engagement. As a part of characterization and steady-state support, the governance lead will work with ADSL to hone and stabilize the following:

- Update and enhance the support model with SAP Ariba and other State of Maine helpdesks including but not limited to those managing integrations with backend ERP, IT infrastructure.
- Update and enhance FAQs and KB articles that will help suppliers, buying officers and other consumers of the helpdesk with an eye on providing self-service options. The governance lead will also identify opportunities for new KB articles by using different techniques like pareto-analysis, proactive problem management, trend analysis etc.
- The lead will act as the liaison between the help desk T1 and other support teams and vendor teams including SAP Ariba to drive MIM (major incident management) calls; problem management calls, process improvement initiatives, shift-left initiatives, identify opportunities for automation or self-service.
- IPS and ADSL will work together to baseline SLAs/ metrics. IPS shall review the reports, validate and present to the State of Maine's management. Requests for new metrics or updates to existing metrics, failure credit calculations shall be handled by the governance lead in tandem with ADSL.
- IPS shall be responsible for managing end user escalations including from suppliers, State of Maine officers; tracking the escalations to closure, making sure they are resolved in the shortest possible time frame; if needed engage our relationship with SAP Ariba to drive incidents that have a dependency on Ariba's support personnel to closure.

1.2.6.6 *Transition Out Assistance Services*

Infosys takes great pride in the relationships we have with our clients. The fact that over 98% of our revenue is from repeat business is testimony to that. As a responsible business solution provider, Infosys is committed to business continuity for our clients. At the end of the contract period, should the State of Maine choose to change to a different service provider or insource, Infosys will transfer the knowledge and handover the service delivery (transition-out) to personnel identified by the State of Maine.

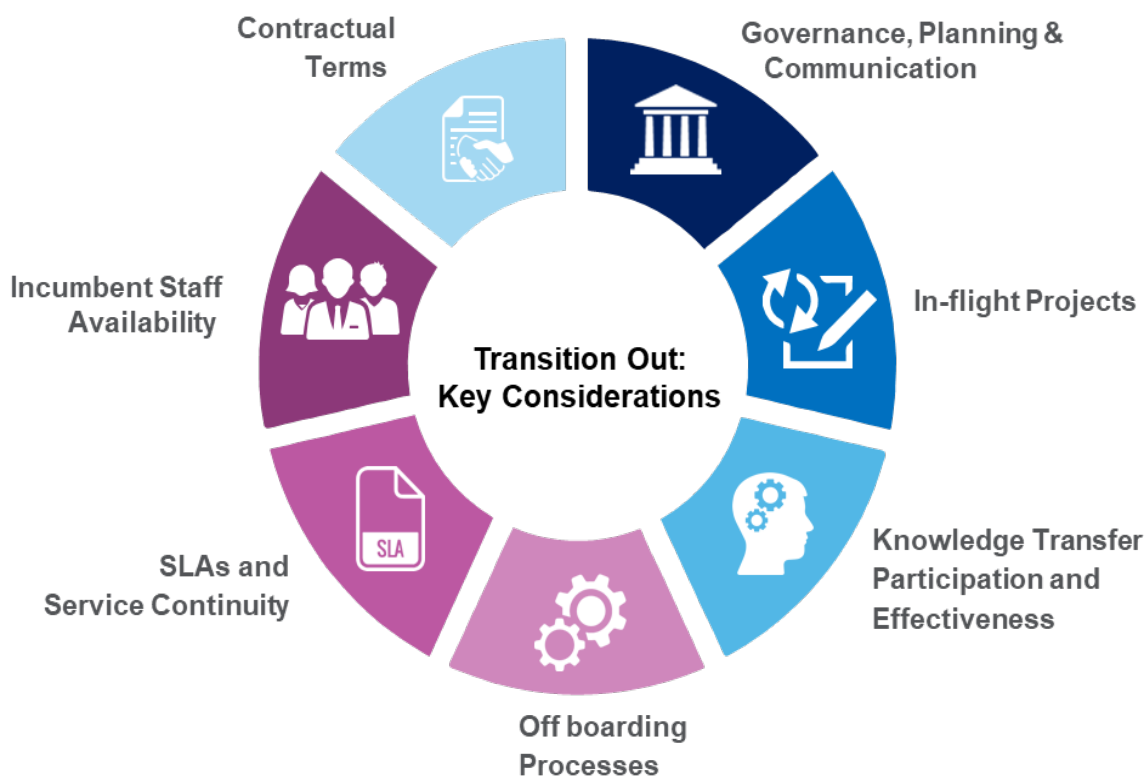


Figure 132. Transition-Out Methodology

Infosys has a comprehensive inflight project methodology (depicted in the following figure) based on the following:

- Project categorization based on project lifecycle (Early, Late and Mid lifecycle)
- Specific project evaluation criteria (business value, monetary impact, end user impact, project complexity, SME availability, and so on)

Inflight Project Ownership Transfer

During the transition's planning phase, Infosys conducts a detailed assessment of the in-scope projects and develops a project specific ownership transfer roadmap. Infosys leverages its in-house project categorization and risk assessment tool for accelerating this exercise.

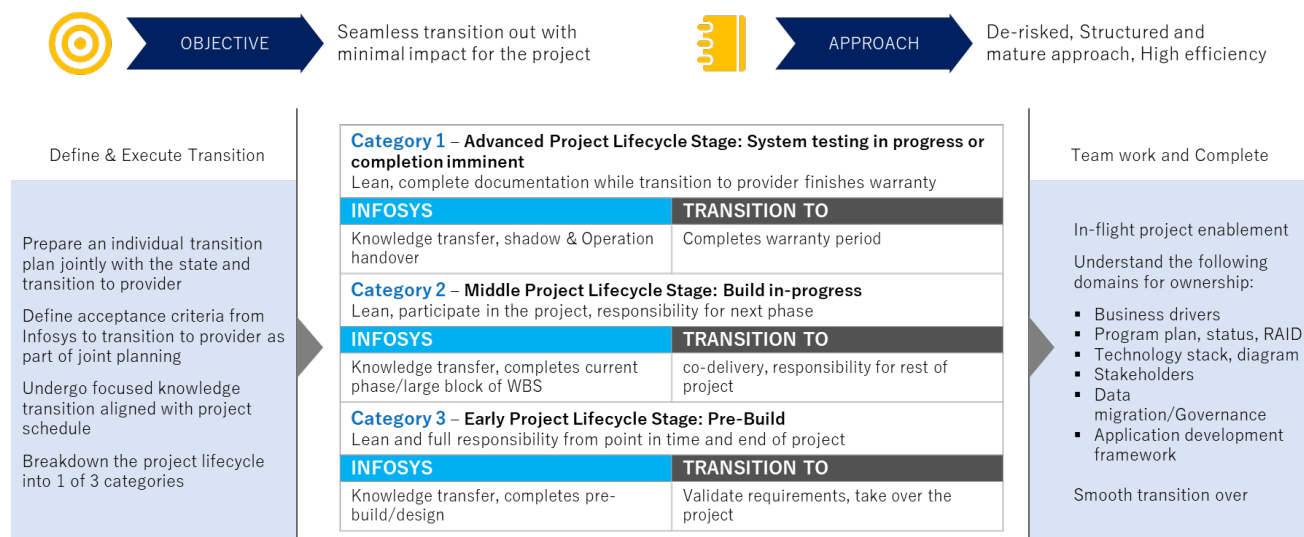


Figure 133. Infosys Inflight Project Transfer Approach

Managed Ownership Transfer

Once the program has been delivered and managed services are to be transitioned out, Infosys provides our approach in a 4-step process for the new service provider.

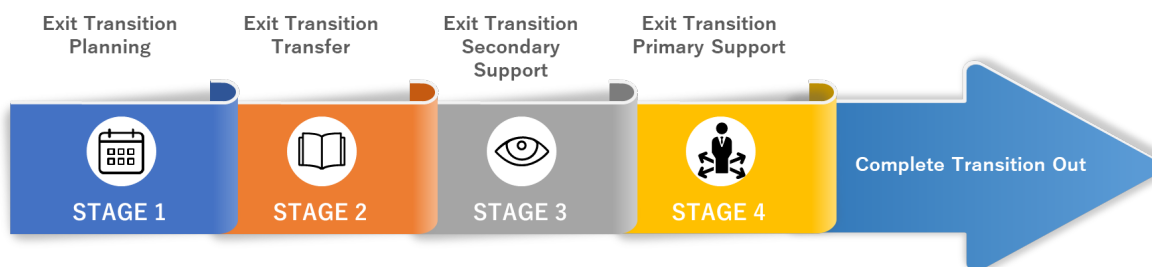


Figure 134.4 Step Managed Services Transition Out

Transition out planning for either situation, in-flight project or during managed services, will be jointly developed between Infosys and the incoming service provider.

Table 67. Transition Out Approach

Stage	Name	Description
1	Exit Transition Planning	In this stage, Infosys and the incoming services team leadership will plan out the details of the transition out process
2	Exit Transition Knowledge Transfer	In this stage, Infosys functional and technical SMEs and program manager will conduct sessions of knowledge transfer to the incoming transition service team
3	Exit Transition Secondary Support	Secondary support is the stage when the incoming team “shadows” and observes the day-to-day operations of the helpdesk, production support, response, resolution, and implementation procedures with a view to learn these activities. SLAs will continue to be owned by Infosys.
4	Exit Transition Primary Support	In this stage, the incoming service team will take over as primary responsible for the day-to-day operations of helpdesk, production support, response, and resolution and implementation procedures. These will be performed under the supervision of Infosys SMEs. SLAs will continue to be owned by Infosys. However, at the end of this stage, Infosys completely transfers ownership of SLAs to the incoming service provider.

Infosys will comply with the below Transition-Out, assistance requested by the State of Maine:

Table 68. Transition Out Assistance

#	Transition-Out Assistance
1	Provide assistance, cooperation and information as is reasonably necessary to help enable a smooth transition of the applicable services to the participating entity or its designated service provider
2	Provide information as the participating entity may reasonably request relating to the number and function of each of the contractor personnel performing the services
3	Transfer participating entity-owned data, information, deliverables, work products (WP), documentation, etc.
4	Identify any dependencies on the new service provider necessary for the Contractor to perform

#	Transition-Out Assistance
	the transition out assistance services.
5	Assist the participating entity in the identification of significant potential risk factors relating to the transition
6	Assist the participating entity in designing plans and contingencies to help mitigate identified risks.
7	Submit a transition plan, for approval by the participating entity, which includes a timeline for successfully completing the transition out assistance services.
8	Provide a schedule and plan for contractor's return to the participating entity of (i) the Participating Entity service locations then occupied by contractor (if any), and (ii) the participating entity confidential information, the participating entity data, documents, records, files, tapes and disks in contractor's possession.

Provide information as the Participating Entity may reasonably request

We approach Knowledge Transfer (KT) top down from business knowledge to technical knowledge with Infosys landing teams having superior functional, technical, and functional domain expertise.

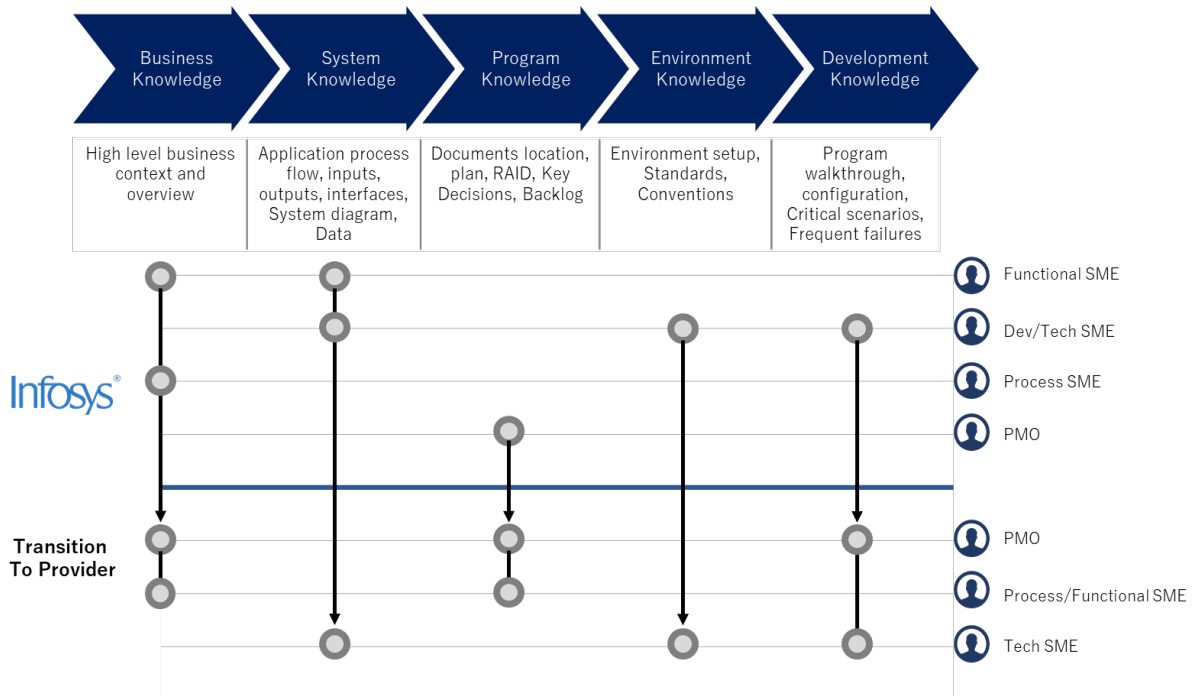


Figure 135. Infosys Knowledge Transfer Approach

There are several ways in which Infosys provides knowledge transfer:

- Targeted follow-up inquiries after documentation review by transition to provider
- Providing RTM and access to documentation for self-review
- Formal KT workshops with Infosys domain experts
- Supporting post systematic follow-ups by the transition to provider

Transfer Participating Entity-owned data, information, deliverables

The Transition planning phase clearly details the plan to successfully execute the remaining phases of transition and is a collaborative effort between Infosys and the State of Maine (with representation

from incumbent vendors) to ensure that requirements are fully understood and that the dependencies are clearly documented.

Identify any dependencies on the new service provider necessary for the Contractor...

To reach the desired outcome from the transition out process, the new service provider has the following major dependencies:

- New service provider to have conducted targeted questionnaires and interviews with State of Maine subject matter experts (SMEs)
- Review of available documentation
- Independent systematic study using reengineering tools from the new service provider
- Availability of new service provider to shadow/parallel key in-flight activities
- Properly experienced SMEs for each key roles from the new service provider
- Transition governance framework from the new service provider
- Objective transition out measurements

Assist the Participating Entity in the identification of significant potential risk...

As part of the transition out, Infosys shall conduct workshop(s) to review and discuss the project RAID log. Infosys has a strict and robust risk and issue process, which follows best practice of grooming the log with dates, responsible, detailed next steps and comments, which maintained in a timely manner. Using this approach, most of the data points that are imperative and known are transparent and ready for review/audit.

Additionally, the Senior Leadership Team (SLT) concerns, asks and next step topics that are not in the RAID will be reviewed for a comprehensive top-bottom transfer.

Lastly, the transition out process will inherently have risks, which will be jointly documented and reasonably addressed by Infosys, State of Maine and/or transition to provider.

Assist the Participating Entity in designing plans and contingencies...

Infosys will participate in developing an end-to-end transition out plan, factoring existing commitments, timing and approaches that have minimal disruption to the in-flight project. As Infosys has been in both sides of the situation, we will be an advocate for the State of Maine during the transition out and plan accordingly.

Typical stages of Exit Transition include the following:

- Exit Transition planning - In this stage, Infosys and the incoming services team leadership will plan out the details of the exit transition process
- Exit Transition Knowledge Transfer - In this stage, Infosys SMEs, program managers, and portfolio leads will conduct sessions of knowledge transfer to the incoming teams.

Cluster	April					May				June				July				Aug				Sep				Oct				
	5	12	19	26	3	10	17	24	31	7	14	21	28	5	12	19	26	2	9	16	23	30	6	13	20	27	4	11	18	25
Program Management	TP	TP	TP	TP	TP	KT	KT	KT	KT	KT	KT	SS	SS	SS	SS	SS	SS	SS	PS	PS	PS	PS	PS	PS	PS					
Core Application	TP	TP	TP	TP	TP	KT	KT	KT	KT	KT	KT	SS	SS	SS	SS	SS	SS	SS	PS	PS	PS	PS	PS	PS	PS					
Financial Management Services	TP	TP	TP	TP	TP	KT	KT	KT	KT	KT	KT	SS	SS	SS	SS	SS	SS	SS	PS	PS	PS	PS	PS	PS	PS					
Interfaces	TP	TP	TP	TP	TP			KT	KT	KT	KT	SS	SS	SS	SS	SS	SS	SS	PS	PS	PS	PS	PS	PS	PS					
Business Reporting	TP	TP	TP	TP	TP			KT	KT	KT	KT	SS	SS	SS	SS	SS	SS	SS	PS	PS	PS	PS	PS	PS	PS					
Information Management Services	TP	TP	TP	TP	TP			KT	KT	KT	KT	SS	SS	SS	SS	SS	SS	SS	PS	PS	PS	PS	PS	PS	PS					
Governance Risk Compliance (GRC)	TP	TP	TP	TP	TP			KT	KT	KT	KT	SS	SS	SS	SS	SS	SS	SS	PS	PS	PS	PS	PS	PS	PS					
Security Information & Event Mgmt	TP	TP	TP	TP	TP			KT	KT	KT	KT	SS	SS	SS	SS	SS	SS	SS	PS	PS	PS	PS	PS	PS	PS					
Minor Enhancements	TP	TP	TP	TP	TP					KT	KT	KT	KT	KT	KT	SS	SS	SS	SS	SS	PS	PS	PS	PS	PS					
Change and Release Mgmt	TP	TP	TP	TP	TP					KT	KT	KT	KT	KT	KT	SS	SS	SS	SS	SS	PS	PS	PS	PS	PS					
Vulnerability Mgmt	TP	TP	TP	TP	TP					KT	KT	KT	KT	KT	KT	SS	SS	SS	SS	SS	PS	PS	PS	PS	PS					
Notices	TP	TP	TP	TP	TP							KT	KT	KT	KT	SS	SS	SS	SS	SS	PS	PS	PS	PS	PS					
Workflow	TP	TP	TP	TP	TP							KT	KT	KT	KT	SS	SS	SS	SS	SS	PS	PS	PS	PS	PS					
Health Coverage Operations	TP	TP	TP	TP	TP							KT	KT	KT	KT	SS	SS	SS	SS	SS	PS	PS	PS	PS	PS					
Command Center/Batch Ops	TP	TP	TP	TP	TP							KT	KT	KT	KT	SS	SS	SS	SS	SS	PS	PS	PS	PS	PS					
Servers(Windows,VMWare)	TP	TP	TP	TP	TP							KT	KT	KT	KT	SS	SS	SS	SS	SS	PS	PS	PS	PS	PS					
Servers (Linux)	TP	TP	TP	TP	TP							KT	KT	KT	KT	SS	SS	SS	SS	SS	PS	PS	PS	PS	PS					
Database	TP	TP	TP	TP	TP							KT	KT	KT	KT	SS	SS	SS	SS	SS	PS	PS	PS	PS	PS					
Middleware	TP	TP	TP	TP	TP							KT	KT	KT	KT	SS	SS	SS	SS	SS	PS	PS	PS	PS	PS					
Network	TP	TP	TP	TP	TP							KT	KT	KT	KT	SS	SS	SS	SS	SS	PS	PS	PS	PS	PS					
Storage & Backup	TP	TP	TP	TP	TP							KT	KT	KT	KT	SS	SS	SS	SS	SS	PS	PS	PS	PS	PS					
Disaster Recovery	TP	TP	TP	TP	TP							KT	KT	KT	KT	SS	SS	SS	SS	SS	PS	PS	PS	PS	PS					
File Operations (ETL)	TP	TP	TP	TP	TP							KT	KT	KT	KT	SS	SS	SS	SS	SS	PS	PS	PS	PS	PS					
Operations Reporting	TP	TP	TP	TP	TP							KT	KT	KT	KT	SS	SS	SS	SS	SS	PS	PS	PS	PS	PS					
Environment Mgmt	TP	TP	TP	TP	TP							KT	KT	KT	KT	SS	SS	SS	SS	SS	PS	PS	PS	PS	PS					
Hardware/Software Upgrades	TP	TP	TP	TP	TP							KT	KT	KT	KT	SS	SS	SS	SS	SS	PS	PS	PS	PS	PS					
Tools Integration	TP	TP	TP	TP	TP							KT	KT	KT	KT	SS	SS	SS	SS	SS	PS	PS	PS	PS	PS					
Identity and Access Mgmt	TP	TP	TP	TP	TP							KT	KT	KT	KT	SS	SS	SS	SS	SS	PS	PS	PS	PS	PS					

Figure 136.Example Transition Out Plan

Submit a transition plan, for approval by the Participating Entity, which includes a timeline for successfully.

The transition out timeline will be mutually agreed between Infosys and the transition to provider and formally approved.

Provide a schedule and plan for Contractor's return to the Participating Entity of (i) the Participating Entity service locations then occupied by Contractor (if any), and (ii) the Participating Entity confidential information, the Participating Entity data, documents, records, files, tapes and disks in Contractor's possession.

Part of the transition out plan will outline in conjunction to the details from the MSA, Infosys will return physical items (e.g. badges, data, records, documents, files, tapes, disks) from the approved transition checklist. A comprehensive list of names/user ID and formal off-boarding date(s) will be provided to the State of Maine for deactivation.

Infosys will conduct the above in a timely manner as developed in the transition out plan.

1.2.7 Other Available Services

Team Infosys has carefully reviewed the requirements of the State of Maine and has proposed an industry best practice e-Procurement solution that is tried and tested for our government clients. The Infosys Team is pleased to propose below additional tools and services that we consider as a value add to the State of Maine.

Table 69. Value Add solution

S.No.	Tool/Service Name	Description	Cost Indication
1	Celonis Process Mining	Celonis Process Mining makes business processes 100% transparent to uncover inefficiencies, bottlenecks and compliance violations. These insights are used to increase the efficiency and quality of processes dramatically. Infosys has developed strong competency across the procurement value chain to deliver value to our customers using Celonis.	Celonis Process Mining is an optional component and can be provided to State of Maine for an additional cost
2	Power Approver	Power Approver mobile application is one stop shop for all approval requests. It provides the ease of access & comfort to users to approve various approvable documents at one place. App sends approval notifications to the approvers. This makes it very convenient and easy for managers to approve the requests on the go. Infosys team developed a customized mobile app “Power Approver” which would be the One Stop Shop for all approval requests. Managers (Approvers) need to install single app, which would integrate with multiple applications (e.g., Ariba) at the back end.	Power Approver is an optional component and can be provided to State of Maine for an additional cost
3	SAP Field Glass	SAP Fieldglass is a cloud-based, open vendor management system (VMS) that helps organizations find, engage and manage their external workforce and services procurement resources – from temporary staff to Statement of Work-based consultants to freelance workers, gig workers, contractors and more. The only solution in the industry that offers a direct candidate website within our core application enabling contingent workers to apply directly for temporary roles.	SAP Field Glass is an optional component and can be provided to State of Maine for an additional cost
4	Spend Analysis	Ariba Spend Analysis is the only solution that combines internal spend classification, supplier information and market dynamics to give organizations the strategic insights needed to identify and prioritize sourcing opportunities.	Spend Analysis is an optional component and can be provided to State of Maine for an additional cost

Infosys is a full-service provider for ERP applications and system integrations. In addition to the services requested by the State of Maine as part of this RFP, Infosys can also provide additional services that are relevant to this transformational initiative, including:

- **IT and ERP Strategy Services.** Over the years, Infosys has built strong capabilities for all major ERP Platforms, such as SAP, Oracle, Peoplesoft, Microsoft Dynamics, etc. With enterprise-level alliances with these industry-leading product vendors, as well as our extensive insights and experiences with end user communities, Infosys can help our clients in establishing and executing their Business and IT strategies and roadmaps. Costs for such services have not been included in the cost workbook submitted. We can provide a quote based on discussion with the State of Maine to align delivery scope and service levels required.

System Integration Services. Infosys is a leader in application integrations using various technologies available in the marketplace. We have specialties in building and enabling integrations among different platforms and difference applications, by leveraging our ERP expertise along with our experiences with middleware technologies such as Oracle ESB, SAP CPI, IBM WebSphere, TIBCO, MuleSoft, Boomi, etc. Some of the integration services costs for eProcurement systems are included in the cost workbook submitted, we can provide additional integration services to extend coverage to relevant ERP systems and business processes used by the States.

- **IVS Services.** Infosys provides independent verification services for many clients. Infosys Validation Solutions delivers enterprise digital assurance through engineering-led QA. In line with shifting QA needs of organizations, we help our clients become resilient by increasing their business agility and future-proofing their organization while ensuring speed and efficiency in a digital world. With client centrality at the core, our key testing offerings:
 - Ensure business continuity and resilience through changing situations
 - Strengthen cyber security for businesses by identifying vulnerabilities, prioritizing, tracking and eliminating security weaknesses
 - Elevate customer experience and power digital transformation
 - Accelerate legacy modernization to help companies stay relevant

Some of the IVS services costs for eProcurement systems testing are included in the cost workbook submitted, we can provide additional IVS services to extend coverage to relevant ERP systems and business processes.

- **Business Process Management (BPM) Services.** Infosys BPM is an end-to-end outsourcing services provider for Business Process Managements, such as Customer Services, Human Capital Management, Financials, Procurement, etc. With proven capabilities and deep domain expertise, we address your business challenges through our integrated IT and business process outsourcing solutions that address critical business functions. We enable our clients to achieve their cost reduction objectives, improve process efficiencies, enhance effectiveness, and deliver superior customer experience, utilizing innovative business excellence frameworks, ongoing productivity improvements, process reengineering, automation, and innovative technology platforms. Costs for such services have not been included in the cost workbook submitted. We can provide a quote based on discussion with the State of Maine to align delivery scope and service levels required.

1.3 Video Demonstrations (Team Infosys Proprietary Content)

We hope you enjoy the video summarizing our proposal response and key features of our solution. The video can be found at the below link-

[eProcurement Video by Infosys Public Services](https://app.redbangle.com/infosys-share) (Web URL - <https://app.redbangle.com/infosys-share>)

As noted previously, in understanding your requirements in this RFP, several critical items stood out to us:

- Need for Full Functionality in One Product. Team Infosys brings:
 - A complete and implemented vision for a cloud-based eProcurement solution
 - No integration required inside the SaaS (Ariba) solution - minimizes the total integrations required
 - A solution with multiple components but a “tight” fit
 - Modules, functions, and services that can be added as you go
- A Commitment to Long Term Operations/Support. We start from the basis of:
 - A plan from Day 1 for the 10-year support term
 - Excellence in technology and business process management
 - An understanding of, and planning for, future needs via the ongoing solution Roadmap
- Need for Benefits Achievement. Customers need to achieve value from business and technology investments. Team Infosys brings:
 - People, tools, and techniques to drive value
 - Commitment to accelerate benefits via early adoption
 - Passion to drive more thorough solution usage

We have a long history of delivering client solutions in partnership, including enterprise e-Procurement solution implementations of similar size and complexity to State of Maine program. Our response will not only meet the critical requirements in this RFP but will also demonstrate our partnership's unique qualifications to meet and exceed your expectations. We distinguish ourselves through our key differentiators:

- Team – a team experienced through 100+ SAP Ariba and public sector technology deployments
- Experience - over the last 20 years, Infosys and our partners including Ernst & Young have successfully delivered over 780 supply chain and procurement transformation programs for organizations across public and commercial sectors. The most recent one is for Public Services and Procurement Canada.
- Solution - an integrated solution that is scalable and secure, improves comptrollership, promotes collaboration and improves management of procurement spend. SAP Ariba offers a modern, scalable eProcurement platform that supports over \$3.3 trillion in global commerce through a network of over 4.8 million suppliers
- Approach - a business-led agile implementation approach, with embedded flexibility for State of Maine to make changes, that proactively embeds stakeholder engagement, process optimization, training, change management and value-added services into its core methodology
- Schedule - Early ROI with UpStream and DownStream modules implementation in parallel. UpStream modules like Source to Contract go live within 6 months and DownStream modules Procure to Pay in parallel and within 9 months from start of the Large State program

1.4 Annexure 1 - Service Level Agreement for SAP Cloud Services

SERVICE LEVEL AGREEMENT FOR SAP CLOUD SERVICES

1. DEFINITIONS

- 1.1. **"Credit"** means 2% of Monthly Subscription Fees for each 1% below the System Availability SLA, not to exceed 100% of Monthly Subscription Fees.
- 1.2. **"Downtime"** means the Total Minutes in the Month during which the production version of the Cloud Service is not available, except for Excluded Downtimes.
- 1.3. **"Excluded Downtime"** means the Total Minutes in the Month attributable to a Maintenance Window; or any Major Upgrade Window for which the Customer has been notified at least five (5) business days in advance; or unavailability caused by factors outside of SAP's reasonable control, such as unpredictable and unforeseeable events that could not have been avoided even if reasonable care had been exercised.
- 1.4. **"Maintenance Window"** means the weekly maintenance windows for the Cloud Service identified in <https://support.sap.com/maintenance-windows>. SAP may update the Maintenance Window from time to time in accordance with the Agreement.
- 1.5. **"Major Upgrade Window"** means the extended upgrade maintenance windows for the Cloud Service identified in <https://support.sap.com/maintenance-windows>. SAP may update the Major Upgrade Window from time to time in accordance with the Agreement.
- 1.6. **"Month"** means a calendar month.
- 1.7. **"Monthly Subscription Fees"** means the monthly (or 1/12 of the annual fee) subscription fees paid for the applicable Cloud Service which did not meet the System Availability SLA.
- 1.8. **"System Availability Percentage"** is calculated and defined as follows:

$$\left(\frac{\text{Total Minutes in the Month} - \text{Excluded Downtime} - \text{Downtime}}{\text{Total Minutes in the Month} - \text{Excluded Downtime}} \right) * 100$$
- 1.9. **"System Availability SLA"** means a 99.5% System Availability Percentage during each Month for the production version of the Cloud Service.
- 1.10. **"Total Minutes in the Month"** are measured 24 hours at 7 days a week during a Month.
- 1.11. **"UTC"** means Coordinated Universal Time standard being the start time for the applicable Maintenance Window and Major Upgrade Window.

2. SYSTEM AVAILABILITY SLA AND CREDITS

- 2.1. **Credit**
 If SAP fails to meet the System Availability SLA for a particular Month, Customer may claim a Credit, which Customer may apply to a future invoice relating to the Cloud Service that did not meet the System Availability SLA (subject to Sections 2.1.1 and 2.1.2 below).
- 2.1.1. Claims for a Credit must be made in good faith and through a documented submission of a support case within thirty (30) business days after the end of the relevant Month in which SAP did not meet the System Availability SLA for the Cloud Service.
- 2.1.2. Customers who have not subscribed to the Cloud Service directly from SAP must claim the Credit from their applicable SAP partner.
- 2.2. **System Availability Report**
 SAP will provide Customer with a monthly report describing the System Availability Percentage for the Cloud Service either by email following a request to Customer's assigned SAP account manager; through the Cloud Service; or through an online portal made available to Customer, if and when such online portal becomes available.

3. CHANGES TO WINDOWS

- 3.1. If Customer wishes to be notified of changes to Maintenance Windows and Major Upgrade Windows, it must subscribe to receive notifications at <https://support.sap.com/maintenance-windows>.