



Contract #: AR3094

STATE OF UTAH COOPERATIVE CONTRACT

1. CONTRACTING PARTIES: This contract is between the Utah Division of Purchasing and the following Contractor:

DXC Technology Services LLC

Name

1775 Tysons Blvd

Street Address

Tysons

VA

22102

City

State

Zip

Vendor # VC226569 Commodity Code #: 920-05 Legal Status of Contractor: Limited Liability Company

Contact Name: Chris Van Vlack Phone Number: 916-846-7356 Email: chris.van-vlack@dxc.com

2. CONTRACT PORTFOLIO NAME: Cloud Solutions.

3. GENERAL PURPOSE OF CONTRACT: Provide Cloud Solutions under the service models awarded in Attachment B.

4. PROCUREMENT: This contract is entered into as a result of the procurement process on FY2018, Solicitation# SK18008

5. CONTRACT PERIOD: Effective Date: Wednesday, June 12, 2019. Termination Date: Tuesday, September 15, 2026 unless terminated early or extended in accordance with the terms and conditions of this contract.

6. Administrative Fee: Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) of contract sales no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services.

7. ATTACHMENT A: NASPO ValuePoint Master Terms and Conditions, including the attached Exhibits

ATTACHMENT B: Scope of Services Awarded to Contractor

ATTACHMENT C: Pricing Discounts and Schedule

ATTACHMENT D: Contractor's Response to Solicitation # SK18008

ATTACHMENT E: Service Offering EULAs, SLAs

Any conflicts between Attachment A and the other Attachments will be resolved in favor of Attachment A.

9. DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:

- All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this contract.
- Utah Procurement Code, Procurement Rules, and Contractor's response to solicitation #SK18008.

10. Each signatory below represents that he or she has the requisite authority to enter into this contract.

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed. Notwithstanding verbal or other representations by the parties, the "Effective Date" of this Contract shall be the date provided within Section 5 above.

CONTRACTOR

June 18, 2019

Contractor's signature

Date

Edward Ho

Offerings, Executive Vice President, and General Manager

Type or Print Name and Title

DIVISION OF PURCHASING

Christopher Hughes (Jun 19, 2019)

Jun 19, 2019

Director, Division of Purchasing

Date



Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

1. Master Agreement Order of Precedence

a. Any Order placed under this Master Agreement shall consist of the following documents:

- (1) A Participating Entity's Participating Addendum¹ ("PA");
- (2) NASPO ValuePoint Master Agreement Terms & Conditions, including the applicable Exhibits² to the Master Agreement;
- (3) The Solicitation;
- (4) Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State; and
- (5) A Service Level Agreement issued against the Participating Addendum.

b. These documents shall be read to be consistent and complementary. Any conflict among these documents shall be resolved by giving priority to these documents in the order listed above. Contractor terms and conditions that apply to this Master Agreement are only those that are expressly accepted by the Lead State and must be in writing and attached to this Master Agreement as an Exhibit or Attachment.

2. Definitions - Unless otherwise provided in this Master Agreement, capitalized terms will have the meanings given to those terms in this Section.

Confidential Information means any and all information of any form that is marked as confidential or would by its nature be deemed confidential obtained by Contractor or its employees or agents in the performance of this Master Agreement, including, but not necessarily limited to (1) any Purchasing Entity's records, (2) personnel records, and (3) information concerning individuals, is confidential information of Purchasing Entity.

Contractor means the person or entity providing solutions under the terms and conditions set forth in this Master Agreement. Contractor also includes its employees, subcontractors, agents and affiliates who are providing the services agreed to under the Master Agreement.

Data means all information, whether in oral or written (including electronic) form,

¹ A Sample Participating Addendum will be published after the contracts have been awarded.

² The Exhibits comprise the terms and conditions for the service models: PaaS, IaaS, and PaaS.

created by or in any way originating with a Participating Entity or Purchasing Entity, and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by or in any way originating with a Participating Entity or Purchasing Entity, in the course of using and configuring the Services provided under this Agreement.

Data Breach means any actual or reasonably suspected non-authorized access to or acquisition of computerized Non-Public Data or Personal Data that compromises the security, confidentiality, or integrity of the Non-Public Data or Personal Data, or the ability of Purchasing Entity to access the Non-Public Data or Personal Data.

Data Categorization means the process of risk assessment of Data. See also “High Risk Data”, “Moderate Risk Data” and “Low Risk Data”.

Disabling Code means computer instructions or programs, subroutines, code, instructions, data or functions, (including but not limited to viruses, worms, date bombs or time bombs), including but not limited to other programs, data storage, computer libraries and programs that self-replicate without manual intervention, instructions programmed to activate at a predetermined time or upon a specified event, and/or programs purporting to do a meaningful function but designed for a different function, that alter, destroy, inhibit, damage, interrupt, interfere with or hinder the operation of the Purchasing Entity’s software, applications and/or its end users processing environment, the system in which it resides, or any other software or data on such system or any other system with which it is capable of communicating.

Fulfillment Partner means a third-party contractor qualified and authorized by Contractor, and approved by the Participating State under a Participating Addendum, who may, to the extent authorized by Contractor, fulfill any of the requirements of this Master Agreement including but not limited to providing Services under this Master Agreement and billing Customers directly for such Services. Contractor may, upon written notice to the Participating State, add or delete authorized Fulfillment Partners as necessary at any time during the contract term. Fulfillment Partner has no authority to amend this Master Agreement or to bind Contractor to any additional terms and conditions.

High Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems (“High Impact Data”).

Infrastructure as a Service (IaaS) as used in this Master Agreement is defined the capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Intellectual Property means any and all patents, copyrights, service marks, trademarks, trade secrets, trade names, patentable inventions, or other similar proprietary rights, in tangible or intangible form, and all rights, title, and interest therein.

Lead State means the State centrally administering the solicitation and any resulting Master Agreement(s).

Low Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems (“Low Impact Data”).

Master Agreement means this agreement executed by and between the Lead State, acting on behalf of NASPO ValuePoint, and the Contractor, as now or hereafter amended.

Moderate Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems (“Moderate Impact Data”).

NASPO ValuePoint is the NASPO ValuePoint Cooperative Purchasing Program, facilitated by the NASPO Cooperative Purchasing Organization LLC, a 501(c)(3) limited liability company (doing business as NASPO ValuePoint) is a subsidiary organization the National Association of State Procurement Officials (NASPO), the sole member of NASPO ValuePoint. The NASPO ValuePoint Cooperative Purchasing Organization facilitates administration of the cooperative group contracting consortium of state chief procurement officials for the benefit of state departments, institutions, agencies, and political subdivisions and other eligible entities (i.e., colleges, school districts, counties, cities, some nonprofit organizations, etc.) for all states and the District of Columbia. The NASPO ValuePoint Cooperative Development Team is identified in the Master Agreement as the recipient of reports and may be performing contract administration functions as assigned by the Lead State.

Non-Public Data means High Risk Data and Moderate Risk Data that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the Purchasing Entity because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

Participating Addendum means a bilateral agreement executed by a Contractor and a Participating Entity incorporating this Master Agreement and any other additional Participating Entity specific language or other requirements, e.g. ordering procedures specific to the Participating Entity, other terms and conditions.

Participating Entity means a state, or other legal entity, properly authorized to enter into a Participating Addendum.

Participating State means a state, the District of Columbia, or one of the territories of the United States that is listed in the Request for Proposal as intending to participate.

Upon execution of the Participating Addendum, a Participating State becomes a Participating Entity.

Personal Data means data alone or in combination that includes information relating to an individual that identifies the individual by name, identifying number, mark or description can be readily associated with a particular individual and which is not a public record. Personal Information may include the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, passport); financial account information, including account number, credit or debit card numbers; or Protected Health Information (PHI) relating to a person.

Platform as a Service (PaaS) as used in this Master Agreement is defined as the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or -acquired applications created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Product means any deliverable under this Master Agreement, including Services, software, and any incidental tangible goods.

Protected Health Information (PHI) means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer. PHI may also include information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Purchasing Entity means a state, city, county, district, other political subdivision of a State, and a nonprofit organization under the laws of some states if authorized by a Participating Addendum, who issues a Purchase Order against the Master Agreement and becomes financially committed to the purchase.

Services mean any of the specifications described in the Scope of Services that are supplied or created by the Contractor pursuant to this Master Agreement.

Security Incident means the reasonably possible or actual unauthorized access to a

Purchasing Entity's Non-Public Data and Personal Data the Contractor believes could reasonably result in the use, disclosure or theft of a Purchasing Entity's Non-Public Data within the possession or control of the Contractor. A Security Incident also includes a major security breach to the Contractor's system, regardless if Contractor is aware of unauthorized access to a Purchasing Entity's Non-Public Data. A Security Incident may or may not turn into a Data Breach.

Service Level Agreement (SLA) means a written agreement between both the Purchasing Entity and the Contractor that is subject to the terms and conditions in this Master Agreement and relevant Participating Addendum unless otherwise expressly agreed in writing between the Purchasing Entity and the Contractor. SLAs should include: (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, (4) remedies, such as credits, and (5) an explanation of how remedies or credits are calculated and issued.

Software as a Service (SaaS) as used in this Master Agreement is defined as the capability provided to the consumer to use the Contractor's applications running on a Contractor's infrastructure (commonly referred to as 'cloud infrastructure'). The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Solicitation means the documents used by the State of Utah, as the Lead State, to obtain Contractor's Proposal.

Statement of Work means a written statement in a solicitation document or contract that describes the Purchasing Entity's service needs and expectations.

3. Term of the Master Agreement: Unless otherwise specified as a shorter term in a Participating Addendum, the term of the Master Agreement will run from contract execution to September 15, 2026.

4. Amendments: The terms of this Master Agreement shall not be waived, altered, modified, supplemented or amended in any manner whatsoever without prior written approval of the Lead State and Contractor.

5. Assignment/Subcontracts: Contractor shall not assign, sell, transfer, or sublet rights, or delegate responsibilities under this Master Agreement, in whole or in part, without the prior written approval of the Lead State.

The Lead State reserves the right to assign any rights or duties, including written assignment of contract administration duties to the NASPO Cooperative Purchasing Organization LLC, doing business as NASPO ValuePoint.

6. Discount Guarantee Period: All discounts must be guaranteed for the entire term of the Master Agreement. Participating Entities and Purchasing Entities shall receive the immediate benefit of price or rate reduction of the services provided under this Master Agreement. A price or rate reduction will apply automatically to the Master Agreement and an amendment is not necessary.

7. Termination: Unless otherwise stated, this Master Agreement may be terminated by either party upon 60 days written notice prior to the effective date of the termination. Further, any Participating Entity may terminate its participation upon 30 days written notice, unless otherwise limited or stated in the Participating Addendum. Termination may be in whole or in part. Any termination under this provision shall not affect the rights and obligations attending orders outstanding at the time of termination, including any right of any Purchasing Entity to indemnification by the Contractor, rights of payment for Services delivered and accepted, data ownership, Contractor obligations regarding Purchasing Entity Data, rights attending default in performance an applicable Service Level of Agreement in association with any Order, Contractor obligations under Termination and Suspension of Service, and any responsibilities arising out of a Security Incident or Data Breach. Termination of the Master Agreement due to Contractor default may be immediate.

8. Confidentiality, Non-Disclosure, and Injunctive Relief

a. Confidentiality. Subject to applicable Public Records/Freedom of Information Act laws and regulations, each Party acknowledges that it and its employees or agents may, in the course of providing, or receiving, a Product under this Master Agreement, be exposed to or acquire information that is confidential to the other Party or their clients. Any reports or other documents or items (including software) that result from the use of the Confidential Information by either Party shall be treated in the same manner as the Confidential Information. Confidential Information does not include information that (1) is or becomes (other than by disclosure by the receiving Party) publicly known; (2) is furnished by the receiving Party to others without restrictions similar to those imposed by this Master Agreement; (3) is rightfully in the receiving Party's possession without the obligation of nondisclosure prior to the time of its disclosure under this Master Agreement; (4) is obtained from a source other than the disclosing Party without the obligation of confidentiality, (5) is disclosed with the written consent of the disclosing Party or; (6) is independently developed by employees, agents or subcontractors of the receiving Party who can be shown to have had no access to the Confidential Information.

b. Non-Disclosure. Each Party shall hold Confidential Information in confidence, using at least the industry standard of confidentiality, and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties (other than Contractor's affiliates and Fulfillment Partners to the extent necessary to the performance of Orders placed under this Master Agreement) or use Confidential Information for any purposes whatsoever other than what is necessary to the performance of Orders placed under this Master Agreement. Each Party shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. Each Party shall use commercially reasonable

efforts to assist the disclosing Party in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the generality of the foregoing, the receiving Party shall advise the disclosing Party immediately if the receiving Party learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Master Agreement, and the receiving Party shall cooperate with the disclosing Party in seeking injunctive or other equitable relief in the name of Purchasing Entity or Contractor against any such person. Except as directed by the disclosing Party, the receiving Party will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at the disclosing Party's request, the receiving Party shall turn over to the disclosing Party, or destroy, all documents, papers, and other matter in the receiving Party's possession that embody Confidential Information. Notwithstanding the foregoing, the receiving Party may keep one copy of such Confidential Information necessary for quality assurance, audits and evidence of the performance of this Master Agreement.

c. **Injunctive Relief.** Each Party acknowledges that breach of this section, including disclosure of any Confidential Information, may cause irreparable injury to the disclosing Party that is inadequately compensable in damages. Accordingly, the disclosing Party may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. Each Party acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of both Parties and are reasonable in scope and content.

d. **Purchasing Entity Law.** These provisions shall be applicable only to extent they are not in conflict with the applicable public disclosure laws of any Purchasing Entity.

9. Right to Publish: Throughout the duration of this Master Agreement, Contractor must secure prior approval from the Lead State or Participating Entity for the release of any information that pertains to the potential work or activities covered by the Master Agreement, including but not limited to reference to or use of the Lead State or a Participating Entity's name, Great Seal of the State, Coat of Arms, any Agency or other subunits of the State government, or any State official or employee, for commercial promotion which is strictly prohibited. News releases or release of broadcast e-mails pertaining to this Master Agreement or Participating Addendum shall not be made without prior written approval of the Lead State or a Participating Entity.

The Contractor shall not make any representations of NASPO ValuePoint's opinion or position as to the quality or effectiveness of the services that are the subject of this Master Agreement without prior written consent. Failure to adhere to this requirement may result in termination of the Master Agreement for cause.

10. Defaults and Remedies

a. The occurrence of any of the following events shall be an event of default under this Master Agreement:

- (1) Nonperformance of contractual requirements; or
- (2) A material breach of any term or condition of this Master Agreement; or
- (3) Any certification, representation or warranty by Contractor in response to the solicitation or in this Master Agreement that proves to be untrue or materially misleading; or
- (4) Institution of proceedings under any bankruptcy, insolvency, reorganization or similar law, by or against Contractor, or the appointment of a receiver or similar officer for Contractor or any of its property, which is not vacated or fully stayed within thirty (30) calendar days after the institution or occurrence thereof; or
- (5) Any default specified in another section of this Master Agreement.

b. Upon the occurrence of an event of default, the Party claiming default shall issue a written notice of default, identifying the nature of the default, and providing a period of 30 calendar days in which the defaulting Party shall have an opportunity to cure the default. The Lead State shall not be required to provide advance written notice or a cure period and may immediately terminate this Master Agreement in whole or in part if the Lead State, in its sole discretion, determines that it is reasonably necessary to preserve public safety or prevent immediate public crisis. Time allowed for cure shall not diminish or eliminate the defaulting Party's liability for damages.

c. If the defaulting party is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, the defaulting party shall be in breach of its obligations under this Master Agreement and the non-defaulting party shall have the right to exercise any or all of the following remedies:

- (1) Exercise any remedy provided by law; and
- (2) Terminate this Master Agreement and any related Contracts or portions thereof; and
- (3) Suspend Contractor from being able to respond to future bid solicitations; and
- (4) Suspend Contractor's performance; and
- (5) Withhold payment of the disputed amounts until the default is remedied.

d. Unless otherwise specified in the Participating Addendum, in the event of a default under a Participating Addendum, a Participating Entity shall provide a written notice of default as described in this section and have all of the rights and remedies under this paragraph regarding its participation in the Master Agreement, in addition to those set forth in its Participating Addendum. Nothing in these Master Agreement Terms and Conditions shall be construed to limit the rights and remedies available to a Purchasing Entity under the applicable commercial code.

11. Changes in Contractor Representation: The Contractor must notify the Lead State of changes in the Contractor's key administrative personnel, in writing within 10 calendar days of the change. The Lead State reserves the right to approve changes in key personnel, as identified in the Contractor's proposal. The Contractor agrees to propose replacement key personnel having substantially equal or better education, training, and

experience as was possessed by the key person proposed and evaluated in the Contractor's proposal.

12. Force Majeure: Neither party shall be in default by reason of any failure in performance of this Contract in accordance with reasonable control and without fault or negligence on their part. Such causes may include, but are not restricted to, acts of nature or the public enemy, acts of the government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes and unusually severe weather, but in every case the failure to perform such must be beyond the reasonable control and without the fault or negligence of the party.

13. Indemnification

a. Each Party shall defend, indemnify and hold harmless the other Party, along with their officers, agents, and employees as well as any person or entity for which they may be liable, from and against third-party claims, damages or causes of action including reasonable attorneys' fees and related costs for any death, injury, or damage to property arising from the gross negligence or willful misconduct of the other Party, its employees or subcontractors or volunteers, at any tier, relating to the performance under the Master Agreement.

b. Indemnification – Intellectual Property. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, Purchasing Entities, along with their officers, agents, and employees as well as any person or entity for which they may be liable ("Indemnified Party"), from and against third-party claims, damages or causes of action including reasonable attorneys' fees and related costs arising out of a claim alleging that a Service provided to a Purchasing Entity under this Agreement infringes any patent, trademark, copyright or trade secret ("Intellectual Property Claim") of the third-party asserting the Intellectual Property Claim, but not where the Intellectual Property Claim arises out of or results from:

(a) Contractor's compliance with Participating Entity/Purchasing Entity's designs, specifications or instructions; or

(b) Contractor's use of technical information or technology provided by the Participating Entity/Purchasing Entity; or

(c) non-Contractor software, modifications a Participating Entity/Purchasing Entity makes to, or any specifications or materials a Participating Entity/Purchasing Entity provides or makes available for a Service; or

(d) Participating Entity/Purchasing Entity's combination of the Service with a non-Contractor product, data or business process; or damages based on the use of a non-Contractor product, data or business; or

(e) Participating Entity/Purchasing Entity's use of either Contractor's

trademark.

(2) The Indemnified Party shall notify the other Party ("Indemnifying Party") within a reasonable time after receiving notice of claim. If the Indemnifying Party promptly and reasonably investigates and defends the claim, it shall have control over the defense and settlement of it. However, the Indemnified Party must consent in writing for any money damages or obligations for which it may be responsible. The Indemnified Party shall furnish, at the Indemnifying Party's reasonable request and expense, information and assistance necessary for such defense. If the Indemnifying Party fails to vigorously pursue the defense or settlement of the claim, the Indemnified Party may assume the defense or settlement of it and the Indemnifying Party shall be liable for all proven direct damages incurred by the Indemnified Party in the pursuit of the claim. Unless otherwise agreed in writing, this section is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.

(c) for purposes of this Section 13(a), only, the term "Party" shall mean Contractor, Lead State, NASPO and NASPO ValuePoint.

14. Independent Contractor: The Contractor shall be an independent contractor. Contractor shall have no authorization, express or implied, to bind the Lead State, Participating States, other Participating Entities, or Purchasing Entities to any agreements, settlements, liability or understanding whatsoever, and agrees not to hold itself out as agent except as expressly set forth herein or as expressly agreed in any Participating Addendum.

15. Individual Customers: Except to the extent modified by a Participating Addendum, each Purchasing Entity shall follow the terms and conditions of the Master Agreement and applicable Participating Addendum and will have the same rights and responsibilities for their purchases as the Lead State has in the Master Agreement, including but not limited to, any indemnity or right to recover any costs as such right is defined in the Master Agreement and applicable Participating Addendum for their purchases. Each Purchasing Entity will be responsible for its own charges, fees, and liabilities. The Contractor will apply the charges and invoice each Purchasing Entity individually.

16. Insurance

a. Unless otherwise agreed in a Participating Addendum, Contractor shall, during the term of this Master Agreement, maintain in full force and effect, the insurance described in this section. Contractor shall acquire such insurance from an insurance carrier or carriers licensed to conduct business in each Participating Entity's state and having a rating of A-, Class VII or better, in the most recently published edition of Best's Reports. Failure to buy and maintain the required insurance may result in this Master Agreement's termination or, at a Participating Entity's option, result in termination of its Participating Addendum.

b. Coverage shall be written on an occurrence basis. The minimum acceptable limits

shall be as indicated below, with no deductible for each of the following categories:

(1) Commercial General Liability covering premises operations, independent contractors, products and completed operations, blanket contractual liability, personal injury (including death), advertising liability, and property damage, with a limit of not less than \$1 million per occurrence/\$3 million general aggregate;

(2) CLOUD MINIMUM INSURANCE COVERAGE:

Level of Risk	Data Breach and Privacy/Cyber Liability including Technology Errors and Omissions Minimum Insurance Coverage
Low Risk Data	\$2,000,000
Moderate Risk Data	\$5,000,000
High Risk Data	\$10,000,000

(3) Contractor must comply with any applicable State Workers Compensation or Employers Liability Insurance requirements.

(4) Professional Liability. As applicable, Professional Liability Insurance Policy in the minimum amount of \$1,000,000 per occurrence and \$1,000,000 in the aggregate, written on an occurrence form that provides coverage for its work undertaken pursuant to each Participating Addendum.

c. Contractor shall pay premiums on all insurance policies. Such policies shall also reference this Master Agreement and shall have a condition that they not be revoked by the insurer until thirty (30) calendar days after notice of intended revocation thereof shall have been given to Purchasing Entity and Participating Entity by the Contractor.

d. Prior to commencement of performance, Contractor shall provide to the Lead State a written endorsement to the Contractor's general liability insurance policy or other documentary evidence acceptable to the Lead State that (1) names the Participating States identified in the Request for Proposal as additional insureds, (2) provides that no material alteration, cancellation, non-renewal, or expiration of the coverage contained in such policy shall have effect unless the named Participating State has been given at least thirty (30) days prior written notice, and (3) provides that the Contractor's liability insurance policy shall be primary, with any liability insurance of any Participating State as secondary and noncontributory. Unless otherwise agreed in any Participating Addendum, the Participating Entity's rights and Contractor's obligations are the same as those specified in the first sentence of this subsection. Before performance of any Purchase Order issued after execution of a Participating Addendum authorizing it, the Contractor shall provide to a Purchasing Entity or Participating Entity who requests it the same information described in this subsection.

e. Contractor shall furnish to the Lead State, Participating Entity, and, on request, the

Purchasing Entity copies of certificates of all required insurance within thirty (30) calendar days of the execution of this Master Agreement, the execution of a Participating Addendum, or the Purchase Order's effective date and prior to performing any work. The insurance certificate shall provide the following information: the name and address of the insured; name, address, telephone number and signature of the authorized agent; name of the insurance company (authorized to operate in all states); a description of coverage in detailed standard terminology (including policy period, policy number, limits of liability, exclusions and endorsements); and an acknowledgment of the requirement for notice of cancellation. Copies of renewal certificates of all required insurance shall be furnished within thirty (30) days after any renewal date. These certificates of insurance must expressly indicate compliance with each and every insurance requirement specified in this section. Failure to provide evidence of coverage may, at sole option of the Lead State, or any Participating Entity, result in this Master Agreement's termination or the termination of any Participating Addendum.

f. Coverage and limits shall not limit Contractor's liability and obligations under this Master Agreement, any Participating Addendum, or any Purchase Order.

17. Laws and Regulations: Any and all Services offered and furnished shall comply fully with all applicable Federal and State laws and regulations.

18. No Waiver of Sovereign Immunity: In no event shall this Master Agreement, any Participating Addendum or any contract or any Purchase Order issued thereunder, or any act of a Lead State, a Participating Entity, or a Purchasing Entity be a waiver of any form of defense or immunity, whether sovereign immunity, governmental immunity, immunity based on the Eleventh Amendment to the Constitution of the United States or otherwise, from any claim or from the jurisdiction of any court.

This section applies to a claim brought against the Participating State only to the extent Congress has appropriately abrogated the Participating State's sovereign immunity and is not consent by the Participating State to be sued in federal court. This section is also not a waiver by the Participating State of any form of immunity, including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

19. Ordering

a. Master Agreement order and purchase order numbers shall be clearly shown on all acknowledgments, shipping labels, packing slips, invoices, and on all correspondence.

b. This Master Agreement permits Purchasing Entities to define project-specific requirements and informally compete the requirement among other firms having a Master Agreement on an "as needed" basis. This procedure may also be used when requirements are aggregated or other firm commitments may be made to achieve reductions in pricing. This procedure may be modified in Participating Addenda and adapted to Purchasing Entity rules and policies. The Purchasing Entity may in its sole discretion determine which firms should be solicited for a quote. The Purchasing Entity may select the quote that it considers most advantageous, cost and other factors

considered.

c. Each Purchasing Entity will identify and utilize its own appropriate purchasing procedure and documentation. Contractor is expected to become familiar with the Purchasing Entities' rules, policies, and procedures regarding the ordering of supplies and/or services contemplated by this Master Agreement.

d. Contractor shall not begin providing Services without a valid Service Level Agreement or other appropriate commitment document compliant with the law of the Purchasing Entity.

e. Orders may be placed consistent with the terms of this Master Agreement during the term of the Master Agreement.

f. All Orders pursuant to this Master Agreement, at a minimum, shall include:

- (1) The services or supplies being delivered;
- (2) The place and requested time of delivery;
- (3) A billing address;
- (4) The name, phone number, and address of the Purchasing Entity representative;
- (5) The price per unit or other pricing elements consistent with this Master Agreement and the contractor's proposal;
- (6) A ceiling amount of the order for services being ordered; and
- (7) The Master Agreement identifier and the Participating State contract identifier.

g. All communications concerning administration of Orders placed shall be furnished solely to the authorized purchasing agent within the Purchasing Entity's purchasing office, or to such other individual identified in writing in the Order.

h. Orders must be placed pursuant to this Master Agreement prior to the termination date of this Master Agreement. Contractor is reminded that financial obligations of Purchasing Entities payable after the current applicable fiscal year are contingent upon agency funds for that purpose being appropriated, budgeted, and otherwise made available.

i. Notwithstanding the expiration or termination of this Master Agreement, Contractor agrees to perform in accordance with the terms of any Orders then outstanding at the time of such expiration or termination. Contractor shall not honor any Orders placed after the expiration or termination of this Master Agreement. Orders from any separate indefinite quantity, task orders, or other form of indefinite delivery order arrangement priced against this Master Agreement may not be placed after the expiration or termination of this Master Agreement, notwithstanding the term of any such indefinite delivery order agreement.

20. Participants and Scope

a. Contractor may not deliver Services under this Master Agreement until a Participating Addendum acceptable to the Participating Entity and Contractor is executed. The NASPO ValuePoint Master Agreement Terms and Conditions are applicable to any Order by a Participating Entity (and other Purchasing Entities covered by their Participating Addendum), except to the extent altered, modified, supplemented or amended by a Participating Addendum. By way of illustration and not limitation, this authority may apply to unique delivery and invoicing requirements, confidentiality requirements, defaults on Orders, governing law and venue relating to Orders by a Participating Entity, indemnification, and insurance requirements. Statutory or constitutional requirements relating to availability of funds may require specific language in some Participating Addenda in order to comply with applicable law. The expectation is that these alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with the consent of the Purchasing Entity and Contractor, may be included in the ordering document (e.g. purchase order or contract) used by the Purchasing Entity to place the Order.

b. Subject to subsection 20c and a Participating Entity's Participating Addendum, the use of specific NASPO ValuePoint cooperative Master Agreements by state agencies, political subdivisions and other Participating Entities (including cooperatives) authorized by individual state's statutes to use state contracts is subject to the approval of the respective State Chief Procurement Official.

c. Unless otherwise stipulated in a Participating Entity's Participating Addendum, specific services accessed through the NASPO ValuePoint cooperative Master Agreements for Cloud Services by state executive branch agencies, as required by a Participating Entity's statutes, are subject to the authority and approval of the Participating Entity's Chief Information Officer's Office³.

d. Obligations under this Master Agreement are limited to those Participating Entities who have signed a Participating Addendum and Purchasing Entities within the scope of those Participating Addenda. States or other entities permitted to participate may use an informal competitive process to determine which Master Agreements to participate in through execution of a Participating Addendum. Financial obligations of Participating States are limited to the orders placed by the departments or other state agencies and institutions having available funds. Participating States incur no financial obligations on behalf of political subdivisions.

e. NASPO ValuePoint is not a party to the Master Agreement. It is a nonprofit cooperative purchasing organization assisting states in administering the NASPO ValuePoint cooperative purchasing program for state government departments, institutions, agencies and political subdivisions (e.g., colleges, school districts, counties, cities, etc.) for all 50 states, the District of Columbia and the territories of the United

³ Chief Information Officer means the individual designated by the Governor with Executive Branch, enterprise-wide responsibility for the leadership and management of information technology resources of a state.

States.

f. Participating Addenda shall not be construed to amend the terms of this Master Agreement between the Lead State and Contractor.

g. Participating Entities who are not states may under some circumstances sign their own Participating Addendum, subject to the approval of participation by the Chief Procurement Official of the state where the Participating Entity is located. Coordinate requests for such participation through NASPO ValuePoint. Any permission to participate through execution of a Participating Addendum is not a determination that procurement authority exists in the Participating Entity; they must ensure that they have the requisite procurement authority to execute a Participating Addendum.

h. Resale. Subject to any explicit permission in a Participating Addendum, Purchasing Entities may not resell goods, software, or Services obtained under this Master Agreement. This limitation does not prohibit: payments by employees of a Purchasing Entity as explicitly permitted under this agreement; sales of goods to the general public as surplus property; and fees associated with inventory transactions with other governmental or nonprofit entities under cooperative agreements and consistent with a Purchasing Entity's laws and regulations. Any sale or transfer permitted by this subsection must be consistent with license rights granted for use of intellectual property.

21. Payment: Orders under this Master Agreement are fixed-price or fixed-rate orders, not cost reimbursement contracts. Unless otherwise stipulated in the Participating Addendum, Payment is normally made within 30 days following the date of a correct invoice is received. Purchasing Entities reserve the right to withhold payment of a portion (including all if applicable) of disputed amount of an invoice. After 45 days the Contractor may assess overdue account charges up to a maximum rate of one percent per month on the outstanding balance. Payments will be remitted by mail. Payments may be made via a State or political subdivision "Purchasing Card" with no additional charge.

22. Data Access Controls: Contractor will provide access to Purchasing Entity's Data only to those Contractor employees, contractors and subcontractors ("Contractor Staff") who need to access the Data to fulfill Contractor's obligations under this Agreement. Contractor shall not access a Purchasing Entity's user accounts or Data, except on the course of data center operations, response to service or technical issues, as required by the express terms of this Master Agreement, or at a Purchasing Entity's written request.

Contractor may not share a Purchasing Entity's Data with its parent corporation, other affiliates, or any other third party without the Purchasing Entity's express written consent.

Contractor will ensure that, prior to being granted access to the Data, Contractor employees who perform work under this Agreement have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all Data protection provisions of this Agreement; and possess all qualifications appropriate

to the nature of the employees' duties and the sensitivity of the Data they will be handling. Contractor will have data protection provisions in its contracts with contractors, subcontractors and/or Fulfillment Partners that obligate such entities to comply with data privacy laws and treat Data as Purchasing Entity's confidential information. Any additional data protection obligations for the applicable contractors, subcontractors and/or Fulfillment Partners shall be set forth in the Order.

23. Operations Management: Contractor shall maintain the administrative, physical, technical, and procedural infrastructure associated with the provision of the Product in a manner that is, at all times during the term of this Master Agreement, at a level equal to or more stringent than those specified in the Solicitation.

24. Public Information: This Master Agreement and all related documents are subject to disclosure pursuant to the Purchasing Entity's public information laws.

25. Purchasing Entity Data: Purchasing Entity retains full right and title to Data provided by it and any Data derived therefrom, including metadata. Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third-party without the consent of Purchasing Entity unless required by law or regulation or by an order of a court of competent jurisdiction. The obligation shall extend beyond the term of this Master Agreement in perpetuity.

Contractor shall not use any information collected in connection with this Master Agreement, including Purchasing Entity Data, for any purpose other than fulfilling its obligations under this Master Agreement.

26. Records Administration and Audit.

a. The Contractor shall maintain books, records, documents, and other evidence pertaining to this Master Agreement and orders placed by Purchasing Entities under it to the extent and in such detail as shall adequately reflect performance and administration of payments and fees. Contractor shall permit the Lead State, a Participating Entity, a Purchasing Entity, the federal government (including its grant awarding entities and the U.S. Comptroller General), and any other duly authorized agent of a governmental agency, to audit, inspect, examine, copy and/or transcribe Contractor's books, documents, papers and records directly pertinent to this Master Agreement or orders placed by a Purchasing Entity under it for the purpose of making audits, examinations, excerpts, and transcriptions. This right shall survive for a period of six (6) years following termination of this Agreement or final payment for any order placed by a Purchasing Entity against this Agreement, whichever is later, to assure compliance with the terms hereof or to evaluate performance hereunder.

b. Without limiting any other remedy available to any governmental entity, the Contractor shall reimburse the applicable Lead State, Participating Entity, or Purchasing Entity for any overpayments inconsistent with the terms of the Master Agreement or orders or underpayment of fees found as a result of the examination of the Contractor's

records.

c. The rights and obligations herein exist in addition to any quality assurance obligation in the Master Agreement requiring the Contractor to self-audit contract obligations and that permits the Lead State to review compliance with those obligations.

d. The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement and applicable Participating Addendum terms. The purchasing entity may perform this audit or contract with a third party at its discretion and at the purchasing entity's expense.

e. The Purchasing Entity shall provide at least 10 business days' prior written notice of the audit. Audits pursuant to this section shall take place during normal business hours, no more frequently than once per year, and with minimum disruption to Contractor's business. Audits of Contractor shall not include audits of the records or premises of Fulfillment Partners unless expressly agreed to in an Order. For clarity, Contractor will employ reasonable efforts to facilitate obtaining information from Fulfillment Partners if requested by Purchasing Entity's auditors.

27. Administrative Fees: The Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services. The NASPO ValuePoint Administrative Fee is not negotiable. This fee is to be included as part of the pricing submitted with proposal.

Additionally, some states may require an additional administrative fee be paid directly to the state on purchases made by Purchasing Entities within that state. For all such requests, the fee level, payment method and schedule for such reports and payments will be incorporated into the Participating Addendum that is made a part of the Master Agreement. The Contractor may adjust the Master Agreement pricing accordingly for purchases made by Purchasing Entities within the jurisdiction of the state. All such agreements shall not affect the NASPO ValuePoint Administrative Fee percentage or the prices paid by the Purchasing Entities outside the jurisdiction of the state requesting the additional fee. The NASPO ValuePoint Administrative Fee shall be based on the gross amount of all sales at the adjusted prices (if any) in Participating Addenda.

28. System Failure or Damage: In the event of system failure or damage caused by Contractor or its Services, the Contractor agrees to use reasonable commercial efforts to restore or assist in restoring the system to operational capacity.

29. Title to Product: If access to the Product requires an application program interface (API), Contractor shall convey to Purchasing Entity an irrevocable license as necessary to use the API during the term of the applicable Order or Statement of Work.

30. Data Privacy: The Contractor must comply with all applicable laws related to data

privacy and security, including IRS Pub 1075. Prior to entering into a SLA with a Purchasing Entity, the Contractor and Purchasing Entity must cooperate and hold a meeting to determine the Data Categorization to determine whether the Contractor will hold, store, or process High Risk Data, Moderate Risk Data and Low Risk Data. The Contractor must document the Data Categorization in the SLA or Statement of Work.

31. Warranty: At a minimum the Contractor must warrant the following:

- a. Contractor has acquired any and all rights, grants, assignments, conveyances, licenses, permissions, and authorization for the Contractor to provide the Services described in this Master Agreement.
- b. Contractor will perform materially as described in this Master Agreement, SLA, Statement of Work, including any performance representations contained in the Contractor's response to the Solicitation by the Lead State.
- c. Contractor represents and warrants that the representations contained in its response to the Solicitation by the Lead State.
- d. The Contractor will not interfere with a Purchasing Entity's access to and use of the Services it acquires from this Master Agreement.
- e. The Services provided by the Contractor are compatible with and will operate successfully with any environment (including web browser and operating system) specified by the Contractor in its response to the Solicitation by the Lead State.
- f. The Contractor warrants that the Products it provides under this Master Agreement are free of malware. The Contractor must use industry-leading technology to detect and remove worms, Trojans, rootkits, rogues, dialers, spyware, etc.

32. Transition Assistance:

- a. The Contractor shall reasonably cooperate with other parties in connection with all Services to be delivered under this Master Agreement, including without limitation any successor service provider to whom a Purchasing Entity's Data is transferred in connection with the termination or expiration of this Master Agreement. The Contractor shall assist a Purchasing Entity in exporting and extracting a Purchasing Entity's Data, in a format usable without the use of the Services and as agreed by a Purchasing Entity, at no additional cost to the Purchasing Entity. Any transition services requested by a Purchasing Entity involving additional knowledge transfer and support may be subject to a separate transition Statement of Work.
- b. A Purchasing Entity and the Contractor shall, when reasonable, create a Transition Plan Document identifying the transition services to be provided and including a Statement of Work if applicable.

c. The Contractor must maintain the confidentiality and security of a Purchasing Entity's Data during the transition services and thereafter as required by the Purchasing Entity.

33. Waiver of Breach: Failure of the Lead State, Participating Entity, or Purchasing Entity to declare a default or enforce any rights and remedies shall not operate as a waiver under this Master Agreement or Participating Addendum. Any waiver by the Lead State, Participating Entity, or Purchasing Entity must be in writing. Waiver by the Lead State or Participating Entity of any default, right or remedy under this Master Agreement or Participating Addendum, or by Purchasing Entity with respect to any Purchase Order, or breach of any terms or requirements of this Master Agreement, a Participating Addendum, or Purchase Order shall not be construed or operate as a waiver of any subsequent default or breach of such term or requirement, or of any other term or requirement under this Master Agreement, Participating Addendum, or Purchase Order.

34. Assignment of Antitrust Rights: Contractor irrevocably assigns to a Participating Entity who is a state any claim for relief or cause of action which the Contractor now has or which may accrue to the Contractor in the future by reason of any violation of state or federal antitrust laws (15 U.S.C. § 1-15 or a Participating Entity's state antitrust provisions), as now in effect and as may be amended from time to time, in connection with any goods or services provided to the Contractor for the purpose of carrying out the Contractor's obligations under this Master Agreement or Participating Addendum, including, at a Participating Entity's option, the right to control any such litigation on such claim for relief or cause of action.

35. Debarment : The Contractor certifies, to the best of its knowledge, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction (contract) by any governmental department or agency. This certification represents a recurring certification made at the time any Order is placed under this Master Agreement. If the Contractor cannot certify this statement, attach a written explanation for review by the Lead State.

36. Performance and Payment Time Frames that Exceed Contract Duration: All maintenance or other agreements for services entered into during the duration of an SLA and whose performance and payment time frames extend beyond the duration of this Master Agreement shall remain in effect for performance and payment purposes (limited to the time frame and services established per each written agreement). No new leases, maintenance or other agreements for services may be executed after the Master Agreement has expired. For the purposes of this section, renewals of maintenance, subscriptions, SaaS subscriptions and agreements, and other service agreements, shall not be considered as "new."

37. Governing Law and Venue

a. The procurement, evaluation, and award of the Master Agreement shall be governed by and construed in accordance with the laws of the Lead State sponsoring and administering the procurement. The construction and effect of the Master Agreement

after award shall be governed by the law of the state serving as Lead State (in most cases also the Lead State). The construction and effect of any Participating Addendum or Order against the Master Agreement shall be governed by and construed in accordance with the laws of the Participating Entity's or Purchasing Entity's State.

b. Unless otherwise specified in the RFP, the venue for any protest, claim, dispute or action relating to the procurement, evaluation, and award is in the Lead State. Venue for any claim, dispute or action concerning the terms of the Master Agreement shall be in the state serving as Lead State. Venue for any claim, dispute, or action concerning any Order placed against the Master Agreement or the effect of a Participating Addendum shall be in the Purchasing Entity's State.

c. If a claim is brought in a federal forum, then it must be brought and adjudicated solely and exclusively within the United States District Court for (in decreasing order of priority): the Lead State for claims relating to the procurement, evaluation, award, or contract performance or administration if the Lead State is a party; the Participating State if a named party; the Participating Entity state if a named party; or the Purchasing Entity state if a named party.

d. This section is also not a waiver by the Participating State of any form of immunity, including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

38. No Guarantee of Service Volumes: The Contractor acknowledges and agrees that the Lead State and NASPO ValuePoint makes no representation, warranty or condition as to the nature, timing, quality, quantity or volume of business for the Services or any other products and services that the Contractor may realize from this Master Agreement, or the compensation that may be earned by the Contractor by offering the Services. The Contractor acknowledges and agrees that it has conducted its own due diligence prior to entering into this Master Agreement as to all the foregoing matters.

39. NASPO ValuePoint eMarket Center: In July 2011, NASPO ValuePoint entered into a multi-year agreement with JAGGAER, formerly SciQuest, whereby JAGGAER will provide certain electronic catalog hosting and management services to enable eligible NASPO ValuePoint's customers to access a central online website to view and/or shop the goods and services available from existing NASPO ValuePoint Cooperative Contracts. The central online website is referred to as the NASPO ValuePoint eMarket Center.

The Contractor will have visibility in the eMarket Center through Ordering Instructions. These Ordering Instructions are available at no cost to the Contractor and provided customers information regarding the Contractors website and ordering information.

At a minimum, the Contractor agrees to the following timeline: NASPO ValuePoint eMarket Center Site Admin shall provide a written request to the Contractor to begin Ordering Instruction process. The Contractor shall have thirty (30) days from receipt of

written request to work with NASPO ValuePoint to provide any unique information and ordering instructions that the Contractor would like the customer to have.

40. Contract Provisions for Orders Utilizing Federal Funds: Pursuant to Appendix II to 2 Code of Federal Regulations (CFR) Part 200, Contract Provisions for Non-Federal Entity Contracts Under Federal Awards, Orders funded with federal funds may have additional contractual requirements or certifications that must be satisfied at the time the Order is placed or upon delivery. These federal requirements may be proposed by Participating Entities in Participating Addenda and Purchasing Entities for incorporation in Orders placed under this master agreement.

41. Government Support: No support, facility space, materials, special access, personnel or other obligations on behalf of the states or other Participating Entities, other than payment, are required under the Master Agreement.

42. NASPO ValuePoint Summary and Detailed Usage Reports: In addition to other reports that may be required by this solicitation, the Contractor shall provide the following NASPO ValuePoint reports.

a. Summary Sales Data. The Contractor shall submit quarterly sales reports directly to NASPO ValuePoint using the NASPO ValuePoint Quarterly Sales/Administrative Fee Reporting Tool found at <http://calculator.naspovaluepoint.org>. Any/all sales made under the contract shall be reported as cumulative totals by state. Even if Contractor experiences zero sales during a calendar quarter, a report is still required. Reports shall be due no later than 30 day following the end of the calendar quarter (as specified in the reporting tool).

b. Detailed Sales Data. Contractor shall also report detailed sales data by: (1) state; (2) entity/customer type, e.g. local government, higher education, K12, non-profit; (3) Purchasing Entity name; (4) Purchasing Entity bill-to and ship-to locations; (4) Purchasing Entity and Contractor Purchase Order identifier/number(s); (5) Purchase Order Type (e.g. sales order, credit, return, upgrade, determined by industry practices); (6) Purchase Order date; (7) and line item description, including product number if used. The report shall be submitted in any form required by the solicitation. Reports are due on a quarterly basis and must be received by the Lead State and NASPO ValuePoint Cooperative Development Team no later than thirty (30) days after the end of the reporting period. Reports shall be delivered to the Lead State and to the NASPO ValuePoint Cooperative Development Team electronically through a designated portal, email, CD-Rom, flash drive or other method as determined by the Lead State and NASPO ValuePoint. Detailed sales data reports shall include sales information for all sales under Participating Addenda executed under this Master Agreement. The format for the detailed sales data report is in shown in Attachment H.

c. Reportable sales for the summary sales data report and detailed sales data report includes sales to employees for personal use where authorized by the solicitation and the Participating Addendum. Report data for employees should be limited to ONLY the

state and entity they are participating under the authority of (state and agency, city, county, school district, etc.) and the amount of sales. No personal identification numbers, e.g. names, addresses, social security numbers or any other numerical identifier, may be submitted with any report.

d. Contractor shall provide the NASPO ValuePoint Cooperative Development Coordinator with an executive summary each quarter that includes, at a minimum, a list of states with an active Participating Addendum, states that Contractor is in negotiations with and any PA roll out or implementation activities and issues. NASPO ValuePoint Cooperative Development Coordinator and Contractor will determine the format and content of the executive summary. The executive summary is due 30 days after the conclusion of each calendar quarter.

e. Timely submission of these reports is a material requirement of the Master Agreement. The recipient of the reports shall have exclusive ownership of the media containing the reports. The Lead State and NASPO ValuePoint shall have a perpetual, irrevocable, non-exclusive, royalty free, transferable right to display, modify, copy, and otherwise use reports, data and information provided under this section.

f. If requested by a Participating Entity, the Contractor must provide detailed sales data within the Participating State.

43. NASPO ValuePoint Cooperative Program Marketing, Training, and Performance Review:

a. Contractor agrees to work cooperatively with NASPO ValuePoint personnel. Contractor agrees to present plans to NASPO ValuePoint for the education of Contractor's contract administrator(s) and sales/marketing workforce regarding the Master Agreement contract, including the competitive nature of NASPO ValuePoint procurements, the Master agreement and participating addendum process, and the manner in which qualifying entities can participate in the Master Agreement.

b. Contractor agrees, as Participating Addendums become executed, if requested by ValuePoint personnel to provide plans to launch the program within the participating state. Plans will include time frames to launch the agreement and confirmation that the Contractor's website has been updated to properly reflect the contract offer as available in the participating state.

c. Contractor agrees, absent anything to the contrary outlined in a Participating Addendum, to consider customer proposed terms and conditions, as deemed important to the customer, for possible inclusion into the customer agreement. Contractor will ensure that their sales force is aware of this contracting option.

d. Contractor agrees to participate in an annual contract performance review at a location selected by the Lead State and NASPO ValuePoint, which may include a discussion of marketing action plans, target strategies, marketing materials, as well as

Contractor reporting and timeliness of payment of administration fees.

e. Contractor acknowledges that the NASPO ValuePoint logos may not be used by Contractor in sales and marketing until a logo use agreement is executed with NASPO ValuePoint.

f. The Lead State expects to evaluate the utilization of the Master Agreement at the annual performance review. Lead State may, in its discretion, terminate the Master Agreement pursuant to section 6 when Contractor utilization does not warrant further administration of the Master Agreement. The Lead State may exercise its right to not renew the Master Agreement if vendor fails to record or report revenue for three consecutive quarters, upon 60-calendar day written notice to the Contractor. This subsection does not limit the discretionary right of either the Lead State or Contractor to terminate the Master Agreement pursuant to section 7.

44. Limitation of Liability: (A) For purposes of this Section 44 only, the term “Party,” means the Lead State, the Participating Entity, and/or the Purchasing Entity on the one hand, and means DXC on the other.

(1) Either Party’s entire liability and the other Party’s exclusive remedy for damages on account of any claim arising out of and not disclaimed under this Agreement shall be:

(a) For bodily injury, death or damage to real property or to tangible personal property proximately caused by a Party’s negligence, proven direct damages;

(b) For breach of Section 8 (Confidentiality, Non-Disclosure, and Injunctive Relief), proven direct damages;

(c) For any third-party claims, the remedies available under Section 13 (Indemnification);

(d) For claims arising from the other Party’s gross negligence or willful misconduct, proven damages; or

(e) For claims other than those set forth in Section 44(A)(1)(a-d), proven direct damages not to exceed, on an aggregate basis during any twelve (12) month period, an amount equal to two times the total net charges incurred by a Purchasing Entity during that twelve (12) month time-period under a corresponding Participating Addendum, or \$3,000,000, whichever is greater.

(2) Except as set forth in Section 13 (Indemnification), or in the case of a Party’s gross negligence or willful misconduct, neither Party will be liable to the other Party for any consequential or special damages of any kind which may result directly or indirectly from such performance, including, without limitation, damages resulting from the loss of use or loss of profit by the Purchasing Entity, the Contractor, or by others.

45. NASPO ValuePoint Cloud Offerings Search Tool: In support of the Cloud Offerings Search Tool here: <http://www.naspovaluepoint.org/#/contract-details/71/search> Contractor shall ensure its Cloud Offerings are accurately reported and updated to the Lead State in the format/template shown in Attachment I.

46. Entire Agreement: This Master Agreement, along with any attachment, contains the entire understanding of the parties hereto with respect to the Master Agreement unless a term is modified in a Participating Addendum with a Participating Entity. No click-through, or other end user terms and conditions or agreements required by the Contractor (“Additional Terms”) provided with any Services hereunder shall be binding on Participating Entities or Purchasing Entities, even if use of such Services requires an affirmative “acceptance” of those Additional Terms before access is permitted.

Exhibit 1 to the Master Agreement: Software-as-a-Service

1. Data Ownership: The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding a Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Master Agreement.

2. Data Protection: Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of Purchasing Entity information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Purchasing Entity information and comply with the following conditions:

- a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.
- b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.
- c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.
- d. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.
- e. At no time shall any data or processes — that either belong to or are intended for the use of a Purchasing Entity or its officers, agents or employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Entity.
- f. The Contractor shall not use any information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

3. Data Location: The Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S. Storage of Purchasing Entity data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide the Services. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in a Participating Addendum.

4. Security Incident or Data Breach Notification:

- a. Incident Response: Contractor may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the Purchasing Entity should be handled on an urgent as-needed basis, as part of Contractor's communication and mitigation processes as mutually agreed upon, defined by law or contained in the Master Agreement.
- b. Security Incident Reporting Requirements: The Contractor shall report a security incident to the Purchasing Entity identified contact immediately as soon as possible or promptly without out reasonable delay, or as defined in the SLA.
- c. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any purchasing entity's content that is subject to applicable data breach notification law, the Contractor shall (1) as soon as possible or promptly without out reasonable delay notify the Purchasing Entity, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.

5. Personal Data Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor.

- a. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.
- b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a Data Breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably requested by the Purchasing Entity to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

c. Unless otherwise stipulated, if a data breach is a direct result of Contractor's breach of its contractual obligation to encrypt personal data or otherwise prevent its release as reasonably determined by the Purchasing Entity, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service required by state (or federal) law or as otherwise agreed to; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws — all not to exceed the average per record per person cost calculated for data breaches in the United States (currently \$217 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

6. Notification of Legal Requests: The Contractor shall contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Purchasing Entity's data under the Master Agreement, or which in any way might reasonably require access to the data of the Purchasing Entity. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying and obtaining the approval of the Purchasing Entity, such approval not to be unreasonably withheld, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

a. In the event of a termination of the Master Agreement or applicable Participating Addendum, the Contractor shall implement an orderly return of purchasing entity's data in a CSV or another mutually agreeable format at a time agreed to by the parties or allow the Purchasing Entity to extract its data and the subsequent secure disposal of purchasing entity's data.

b. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's data.

c. In the event of termination of any services or agreement in entirety, the Contractor shall not take any action to intentionally erase purchasing entity's data for a period of:

- 10 days after the effective date of termination, if the termination is in accordance with the contract period
- 30 days after the effective date of termination, if the termination is for convenience
- 60 days after the effective date of termination, if the termination is for cause

After such period, the Contractor shall have no obligation to maintain or provide any purchasing entity's data and shall thereafter, unless legally prohibited, delete all purchasing entity's data in its systems or otherwise in its possession or under its control.

d. The purchasing entity shall be entitled to any post termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of an SLA.

e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD, backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. Background Checks: Upon the request of the Purchasing Entity and at Purchase Entity's expense, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, shall have the right to either (1) request immediate replacement of the person, or (2) act in accordance with the Termination provision of the Master Agreement and/or applicable Participating Addendum.

9. Access to Security Logs and Reports: The Contractor shall provide reports on a schedule specified in the SLA to the Purchasing Entity in a format as specified in the SLA agreed to by both the Contractor and the Purchasing Entity. Reports shall include latency statistics, user access, user access IP address, user access history and security logs for all public jurisdiction files related to this Master Agreement and applicable Participating Addendum.

10. Contract Audit: The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a third party at its discretion and at the Purchasing Entity's expense.

11. Data Center Audit: The Contractor shall perform an independent audit of its data centers at least annually at its expense, and provide an unredacted version of the audit report upon request to a Purchasing Entity. The Contractor may remove its proprietary information from the unredacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

12. Change Control and Advance Notice: The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

Contractor will make updates and upgrades available to Purchasing Entity at no additional costs when Contractor makes such updates and upgrades generally available to its users.

No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect Purchasing Entity's use of or access to the Service, or increase the cost of the Service to the Purchasing Entity without the approval of the Purchasing Entity.

Contractor will notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade.

13. Security: As requested by a Purchasing Entity, the Contractor shall disclose its non-proprietary system security plans (SSP) or security processes and technical limitations to the Purchasing Entity such that adequate protection and flexibility can be attained between the Purchasing Entity and the Contractor. For example: virus checking and port sniffing — the Purchasing Entity and the Contractor shall understand each other's roles and responsibilities.

14. Non-disclosure and Separation of Duties: The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. Import and Export of Data: The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity. This includes the ability for the Purchasing Entity to import or export data to/from other Contractors. Contractor shall specify if Purchasing Entity is required to provide its' own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.

16. Responsibilities and Uptime Guarantee: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

17. Subcontractor Disclosure: Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Contractor, and who shall be involved in any application development and/or operations.

18. Right to Remove Individuals: The Purchasing Entity shall have the right at any time to require that the Contractor remove from interaction with Purchasing Entity any Contractor representative who the Purchasing Entity believes is detrimental to its working relationship with the Contractor. The Purchasing Entity shall provide the Contractor with notice of its determination, and the reasons it requests the removal. If the Purchasing Entity signifies that a potential security violation exists with respect to the request, the Contractor shall immediately remove such individual. The Contractor shall not assign the

person to any aspect of the Master Agreement or future work orders without the Purchasing Entity's consent.

19. Business Continuity and Disaster Recovery: The Contractor shall provide a business continuity and disaster recovery plan upon request and ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) Contractor must work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

20. Compliance with Accessibility Standards: The Contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973, or any other state laws or administrative regulations identified by the Participating Entity.

21. Web Services: The Contractor shall use Web services exclusively to interface with the Purchasing Entity's data in near real time.

22. Encryption of Data at Rest: The Contractor shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data, unless the Purchasing Entity approves in writing for the storage of Personal Data on a Contractor portable device in order to accomplish work as defined in the statement of work.

23. Subscription Terms: Contractor grants to a Purchasing Entity a license to: (i) access and use the Service for its business purposes; (ii) for SaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

No Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement.

Exhibit 2 to the Master Agreement: Platform-as-a-Service

1. Data Ownership: The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding a Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Master Agreement.

2. Data Protection: Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of Purchasing Entity information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Purchasing Entity information and comply with the following conditions:

- a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.
- b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.
- c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.
- d. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.
- e. At no time shall any data or processes — that either belong to or are intended for the use of a Purchasing Entity or its officers, agents or employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Entity.
- f. The Contractor shall not use any information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

3. Data Location: The Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S. Storage of Purchasing Entity data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide the Services. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in a Participating Addendum.

4. Security Incident or Data Breach Notification: The Contractor shall inform the Purchasing Entity of any security incident or data breach within the possession and control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or SLA. Such notice shall include, to the best of Contractor's knowledge at that time, the persons affected, their identities, and the Confidential Information and Data disclosed, or shall include if this information is unknown.

a. Incident Response: The Contractor may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Master Agreement, Participating Addendum, or SLA. Discussing security incidents with the Purchasing Entity should be handled on an urgent as-needed basis, as part of Contractor's communication and mitigation processes as mutually agreed, defined by law or contained in the Master Agreement, Participating Addendum, or SLA.

b. Security Incident Reporting Requirements: Unless otherwise stipulated, the Contractor shall immediately report a security incident related to its service under the Master Agreement, Participating Addendum, or SLA to the appropriate Purchasing Entity.

c. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any Purchasing Entity data that is subject to applicable data breach notification law, the Contractor shall (1) promptly notify the appropriate Purchasing Entity within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner

5. Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor.

a. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.

b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a data breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably

requested by the Purchasing Entity to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

c. Unless otherwise stipulated, if a Data Breach is a direct result of Contractor's breach of its contractual obligation to encrypt Personal Data or otherwise prevent its release, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service required by state (or federal) law or as otherwise agreed to; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws — all not to exceed the average per record per person cost calculated for data breaches in the United States (currently \$217 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

6. Notification of Legal Requests: The Contractor shall contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Purchasing Entity's data under the Master Agreement, or which in any way might reasonably require access to the data of the Purchasing Entity. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying and obtaining the approval of the Purchasing Entity, such approval not to be unreasonably withheld, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

a. In the event of an early termination of the Master Agreement, Participating or SLA, Contractor shall allow for the Purchasing Entity to retrieve its digital content and provide for the subsequent secure disposal of the Purchasing Entity's digital content.

b. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's data.

c. In the event of early termination of any Services or agreement in entirety, the Contractor shall not take any action to intentionally erase any Purchasing Entity's data for a period of 1) 45 days after the effective date of termination, if the termination is for convenience; or 2) 60 days after the effective date of termination, if the termination is for cause. After such day period, the Contractor shall have no obligation to maintain or provide any Purchasing Entity data and shall thereafter, unless legally prohibited, delete all Purchasing Entity data in its systems or otherwise in its possession or under its control. In the event of either termination for cause, the Contractor will impose no fees for access and retrieval of digital content to the Purchasing Entity.

d. The Purchasing Entity shall be entitled to any post termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of an SLA.

e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD, backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. Background Checks:

a. Upon the request of the Purchasing Entity and at Purchasing Entity's expense, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents.

b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

c. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity shall have the right to either (1) request immediate replacement of the person or (2) act in accordance with the Termination provision of the Master Agreement and/or applicable Participating Addendum. .

9. Access to Security Logs and Reports:

a. The Contractor shall provide reports on a schedule specified in the SLA to the Purchasing Entity in a format as specified in the SLA and agreed to by both the Contractor and the Purchasing Entity. Reports will include latency statistics, user access, user access IP address, user access history and security logs for all Purchasing Entity files related to the Master Agreement, Participating Addendum, or SLA.

b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

10. Contract Audit: The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a third party at its discretion and at the Purchasing Entity's expense.

11. Data Center Audit: The Contractor shall perform an independent audit of its data centers at least annually at its expense, and provide an unredacted version of the audit report upon request to a Purchasing Entity. The Contractor may remove its proprietary information from the unredacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

12. Change Control and Advance Notice: The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

Contractor will make updates and upgrades available to Purchasing Entity at no additional costs when Contractor makes such updates and upgrades generally available to its users.

No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect Purchasing Entity's use of or access to the Service, or increase the cost of the Service to the Purchasing Entity without the approval of the Purchasing Entity.

Contractor will notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade.

13. Security: As requested by a Purchasing Entity, the Contractor shall disclose its non-proprietary system security plans (SSP) or security processes and technical limitations to the Purchasing Entity such that adequate protection and flexibility can be attained between the Purchasing Entity and the Contractor. For example: virus checking and port sniffing — the Purchasing Entity and the Contractor shall understand each other's roles and responsibilities.

14. Non-disclosure and Separation of Duties: The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. Import and Export of Data: The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity. This includes the ability for the Purchasing Entity to import or export data to/from other Contractors. Contractor shall specify if Purchasing Entity is required to provide its' own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.

16. Responsibilities and Uptime Guarantee: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

17. Subcontractor Disclosure: Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Contractor, and who shall be involved in any application development and/or operations.

18. Business Continuity and Disaster Recovery: The Contractor shall provide a business continuity and disaster recovery plan upon request and ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) Contractor must work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

19. Compliance with Accessibility Standards: The Contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973 or any other state laws or administrative regulations identified by the Participating Entity..

20. Web Services: The Contractor shall use Web services exclusively to interface with the Purchasing Entity's data in near real time.

21. Encryption of Data at Rest: The Contractor shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data as identified in the SLA, unless the Contractor presents a justifiable position that is approved by the Purchasing Entity that Personal Data, is required to be stored on a Contractor portable device in order to accomplish work as defined in the scope of work.

22. Subscription Terms: Contractor grants to a Purchasing Entity a license to: (i) access and use the Service for its business purposes; (ii) for PaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

No Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement.

Exhibit 3 to the Master Agreement: Infrastructure-as-a-Service

1. Data Ownership: The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding a Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Master Agreement.

2. Data Protection: Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of Purchasing Entity information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Purchasing Entity information and comply with the following conditions:

- a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.
- b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.
- c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.
- d. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.
- e. At no time shall any data or processes — that either belong to or are intended for the use of a Purchasing Entity or its officers, agents or employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Entity.
- f. The Contractor shall not use any information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

3. Data Location: The Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S. Storage of Purchasing Entity data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide the Services. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in a Participating Addendum.

4. Security Incident or Data Breach Notification: The Contractor shall inform the Purchasing Entity of any security incident or data breach related to Purchasing Entity's Data within the possession or control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or SLA. Such notice shall include, to the best of Contractor's knowledge at that time, the persons affected, their identities, and the Confidential Information and Data disclosed, or shall include if this information is unknown.

a. **Security Incident Reporting Requirements:** The Contractor shall report a security incident to the Purchasing Entity identified contact immediately as soon as possible or promptly without out reasonable delay, or as defined in the SLA.

b. **Breach Reporting Requirements:** If the Contractor has actual knowledge of a confirmed data breach that affects the security of any purchasing entity's content that is subject to applicable data breach notification law, the Contractor shall (1) as soon as possible or promptly without out reasonable delay notify the Purchasing Entity, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.

5. Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or SLA.

a. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.

b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a data breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably requested by the Purchasing Entity to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

c. Unless otherwise stipulated, if a Data Breach is a direct result of Contractor's breach of its contractual obligation to encrypt Personal Data or otherwise prevent its release, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service required by state (or federal) law or as otherwise agreed to; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws — all not to exceed the average per record per person cost calculated for data breaches in the United States (currently \$217 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

6. Notification of Legal Requests: The Contractor shall contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Purchasing Entity's data under the Master Agreement, or which in any way might reasonably require access to the data of the Purchasing Entity. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying and obtaining the approval of the Purchasing Entity, such approval not to be unreasonably withheld, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

a. In the event of an early termination of the Master Agreement, Participating or SLA, Contractor shall allow for the Purchasing Entity to retrieve its digital content and provide for the subsequent secure disposal of the Purchasing Entity's digital content.

b. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's data.

c. In the event of early termination of any Services or agreement in entirety, the Contractor shall not take any action to intentionally erase any Purchasing Entity's data for a period of 1) 45 days after the effective date of termination, if the termination is for convenience; or 2) 60 days after the effective date of termination, if the termination is for cause. After such day period, the Contractor shall have no obligation to maintain or provide any Purchasing Entity data and shall thereafter, unless legally prohibited, delete all Purchasing Entity data in its systems or otherwise in its possession or under its control. In the event of either termination for cause, the Contractor will impose no fees for access and retrieval of digital content to the Purchasing Entity.

d. The Purchasing Entity shall be entitled to any post termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of an SLA.

e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD, backup tape and

paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. Background Checks:

- a. Upon the request of the Purchasing Entity and at Purchasing Entity's expense, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents.
- b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.
- c. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity shall have the right to either (1) request immediate replacement of the person, or (2) act in accordance with the Termination provision of the Master Agreement and/or applicable Participating Addendum.

9. Access to Security Logs and Reports:

- a. The Contractor shall provide reports on a schedule specified in the SLA to the Contractor directly related to the infrastructure that the Contractor controls upon which the Purchasing Entity's account resides. Unless otherwise agreed to in the SLA, the Contractor shall provide the public jurisdiction a history or all API calls for the Purchasing Entity account that includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters and the response elements returned by the Contractor. The report will be sufficient to enable the Purchasing Entity to perform security analysis, resource change tracking and compliance auditing
- b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

10. Contract Audit: The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a third party at its discretion and at the Purchasing Entity's expense.

11. Data Center Audit: The Contractor shall perform an independent audit of its data centers at least annually and at its own expense, and provide an unredacted version of the audit report upon request. The Contractor may remove its proprietary information from the unredacted version. For example, a Service Organization Control (SOC) 2 audit report would be sufficient.

12. Change Control and Advance Notice: The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

Contractor will make updates and upgrades available to Purchasing Entity at no additional costs when Contractor makes such updates and upgrades generally available to its users.

No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect Purchasing Entity's use of or access to the Service, or increase the cost of the Service to the Purchasing Entity without the approval of the Purchasing Entity.

Contractor will notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade.

13. Security: As requested by a Purchasing Entity, the Contractor shall disclose its non-proprietary system security plans (SSP) or security processes and technical limitations to the Purchasing Entity such that adequate protection and flexibility can be attained between the Purchasing Entity and the Contractor. For example: virus checking and port sniffing — the Purchasing Entity and the Contractor shall understand each other's roles and responsibilities.

14. Non-disclosure and Separation of Duties: The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. Import and Export of Data: The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity. This includes the ability for the Purchasing Entity to import or export data to/from other Contractors. Contractor shall specify if Purchasing Entity is required to provide its' own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.

16. Responsibilities and Uptime Guarantee: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

17. Subcontractor Disclosure: Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Contractor, and who shall be involved in any application development and/or operations.

18. Business Continuity and Disaster Recovery: The Contractor shall provide a business continuity and disaster recovery plan upon request and ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) Contractor must work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

19. Subscription Terms: Contractor grants to a Purchasing Entity a license to: (i) access and use the Service for its business purposes; (ii) for IaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

No Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement.

Attachment B – Scope of Services Awarded to Contractor

1.1 Awarded Service Model(s).

Contractor is awarded the following Service Model:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

1.2 Risk Categorization.*

Contractor's offered solutions offer the ability to store and secure data under the following risk categories:

Service Model	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered
Saas 1. Application - Custom Development using .NET (Azure) Java (AWS) 2. Application - Testing and Digital Assurance 3. DXC Migration Services for Oracle Cloud 4. ServiceNow Applications 5. Emerging Practices – Salesforce 6. Emerging Practices – Workday 7. Workplace AD - Integration, Migration 8. Workplace - O365 on Azure 9. Workplace- Skype for business 10. Workplace - Mobility Service 11. Security Services- Consulting service 12. Microsoft Dynamics 365	X	X	X	Public Cloud (FedRAMP Moderate) **

Saas 1. Workplace-Desktop/Application Virtualization 2. DXC Migration Services for Oracle Cloud 3. Application - Testing and Digital Assurance	X	X	X	Community Cloud (Oracle Cloud) **
Saas 1. DXC Migration Services for Oracle Cloud	X	X	X	Private Cloud **
IaaS 1. Oracle As Service 2. Cloud Security Advisory Services 3. Managed Cloud Access Security Broker 4. On-Demand Workload Protection 5. Infrastructure & Endpoint Security Advisory Services 6. Managed Endpoint Threat Detection & Response 7. DXC Managed Service for Azure 8. DXC Managed Service for AWS 9. Cloud & Platform Advisory Services	X	X	X	Public Cloud (FedRAMP Moderate) **
IaaS 1. Virtual Private Cloud 2. Managed Services for VMware 3. Workplace AD-Integration, Migration 4. Workplace-Desktop/Application Virtualization 5. Oracle As Service 6. On-Demand Workload Protection 7. Cloud & Platform for Advisory Services	X	X	X	Community Cloud (Oracle Cloud) **

IaaS 1. Virtual Private Cloud 2. Managed Services for VMware	X	X	X	Private Cloud **
PaaS 1. PaaS for SAP on AWS 2. PaaS for SAP on Azure 3. Managed Container PaaS for RedShift	X	X	X	Public Cloud (FedRAMP Moderate) **
PaaS 1. PaaS for SAP	X	X	X	Community Cloud (SAP Cloud Platform) **
PaaS 1. PaaS for SAP	X	X	X	Private Cloud **

* Contractor may add additional OEM solutions during the life of the contract.

** Note: The risk ratings represent the low-risk data, moderate-risk data, or high-risk data that a client could process and store on our provided cloud services and solutions.

- Low-risk data includes non-production, development, de-identified data, aggregate, temporary or throw-away data.
- Moderate-risk data would include production data, intellectual property, confidential and sensitive documents.
- High-risk data includes personally identifiable information, protected healthcare information, customer private data, credit-card data, etc.
- As required, even higher-risk data would be data of national security importance, or data that is required to be run in a Department of Defense or ITAR GovCloud or FedRAMP High environment. This higher GovCloud, FedRAMP High level of security can also be provided.

DXC inherits and leverages the security controls provided by the underlying Microsoft Azure, Amazon Web Services, or Oracle Cloud or SAP Cloud Platform cloud providers. A FedRAMP Moderate cloud environment from these cloud providers supports encryption of the customer data in transit and at rest and provides the necessary controls to help safeguard state and local government clients' important information assets and data. The security, availability, integrity and confidentiality risks to the client from running in a secure FedRAMP Moderate cloud environment are relatively low. A FedRAMP moderate environment is designed to support production data and systems and mission critical operations.

Additional or enhanced security controls are available in a GovCloud or FedRAMP High cloud environment, should even higher level of controls be needed for customers with stringent ITAR, Department of Defense, National Institute of Standards and Technology (NIST) High, or FedRAMP High security controls requirements.

2.1 Deployment Models.

Contractor may provide cloud based services through the following deployment methods:

- **Private cloud.** The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
- **Community cloud.** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
- **Public cloud.** The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- **Hybrid cloud.** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Attachment C - Pricing Discounts and Schedule

Contractor: DXC Technology Services, LLC

Pricing Notes

1. % discounts are based on minimum discounts off Contractor's commercially published pricelists versus fixed pricing. Nonetheless, Orders will be fixed-price or fixed-rate and not cost reimbursable contracts. Contractor has the ability to update and refresh its respective price catalog, as long as the agreed-upon discounts are fixed.
2. Minimum guaranteed contract discounts do not preclude an Offeror and/or its authorized resellers from providing deeper or additional, incremental discounts at their sole discretion.
3. Purchasing entities shall benefit from any promotional pricing offered by Contractor to similar customers. Promotional pricing shall not be cause for a permanent price change.
4. Contractor's price catalog include the price structures of the cloud service models, value added services (i.e., Maintenance Services, Professional Services, Etc.), and deployment models that it intends to provide including the types of data it is able to hold under each model. Pricing shall all-inclusive of infrastructure and software costs and management of infrastructure, network, OS, and software.
5. Contractor provides tiered pricing to accompany its named user licensing model, therefore, as user count reaches tier thresholds, unit price decreases.

Cloud Service Model: Infrastructure as a Service (IaaS)

Description	Minimum Discount % Off
MICROSOFT AZURE	2.00%
AWS	2.00%
ORACLE	2.00%
DXC (Managed VPC)	2.00%
Average IaaS OEM Discount Off	2.00%

Cloud Service Model: Platform as a Service (PaaS)

Description	Discount
SAP HANA	7.00%
ORACLE	2.00%
Average PaaS OEM Discount Off	4.50%

Cloud Service Model: Software as a Service (SaaS)

Description	Discount
ORACLE	9.00%
Average SaaS OEM Discount Off	9.00%

Additional Value Added Services

Item Description	Onsite Hourly Rate		Remote Hourly Rate	
	NVP Price	Catalog Price	NVP Price	Catalog Price
Maintenance Services				
Professional Services				
Deployment Services				
Integration Services)				
Consulting/Advisory Services				
Junior Technical Consultant	120.18	126.50	104.50	110.00
Technical Consultant	152.95	161.00	133.00	140.00
Lead Technical Consultant	196.65	207.00	171.00	180.00
Managing Technical Consultant	234.89	247.25	204.25	215.00
Business Consultant	120.18	126.50	104.50	110.00
Senior Business Consultant	152.95	161.00	133.00	140.00
Lead Business Consultant	196.65	207.00	171.00	180.00
Managing Business Consultant	234.89	247.25	204.25	215.00
Consulting Architect	210.42	221.49	182.97	192.60
Senior Consulting Architect	251.33	264.56	218.55	230.05
Consulting Engagement Project Manager	126.19	132.83	109.73	115.50
Senior Consulting Engagement Project Manager	160.60	169.05	139.65	147.00
Consulting Engagement Program Manager	206.48	217.35	179.55	189.00
Senior Consulting Engagement Program Manager	246.63	259.61	214.46	225.75
Architectural Design Services				
Statement of Work Services				
Partner Services				
Training Deployment Services				
Applications & Oracle Services				
Junior Technical SME	81.94	86.25	71.25	75.00
Technical SME	100.51	105.80	87.40	92.00
Lead Technical SME	114.71	120.75	99.75	105.00
Managing Technical SME	136.56	143.75	118.75	125.00

Attachment C - Pricing Discounts and Schedule

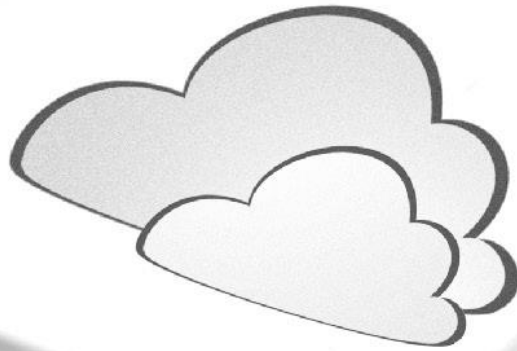
Contractor: DXC Technology Services, LLC

Junior Business Analyst	81.94	86.25	71.25	75.00
Business Analyst	100.51	105.80	87.40	92.00
Lead Business Analyst	114.71	120.75	99.75	105.00
Managing Business Analyst	136.56	143.75	118.75	125.00
Enterprise Architect	122.74	129.20	106.73	112.35
Senior Enterprise Architect	146.12	153.81	127.06	133.75
Junior Developer	81.94	86.25	71.25	75.00
Developer	100.51	105.80	87.40	92.00
Lead Developer	114.71	120.75	99.75	105.00
Project Manager	86.03	90.56	74.81	78.75
Senior Project Manager	105.54	111.09	91.77	96.60
Program Manager	120.45	126.79	104.74	110.25
Senior Program Manager	143.39	150.94	124.69	131.25
Oracle Application Specialist Technical	114.71	120.75	99.75	105.00
Oracle DBA Senior	136.56	143.75	118.75	125.00
Oracle Application Specialist Functional	158.41	166.75	137.75	145.00
Oracle Delivery Manager	207.58	218.50	180.50	190.00
Oracle Cloud Migration Specialist	202.11	212.75	175.75	185.00
Oracle Cloud Integration Specialist	245.81	258.75	213.75	225.00
Oracle Cloud Administrator	267.66	281.75	232.75	245.00
Oracle Cloud Architect	355.06	373.75	308.75	325.00
Workplace Services				
Workplace Engineers Messaging/ VDI	103.66	109.11	90.14	94.88
Senior Workplace Engineers Messaging/ VDI	129.15	135.94	112.30	118.21
Lead Workplace Engineers Messaging/ VDI	153.34	161.41	133.34	140.36
Service Desk Services				
Level 1/Tier I Agent	48.15	50.68	41.87	44.07
Operations Manager	168.62	177.50	146.63	154.35
Supervisor	95.23	100.25	82.81	87.17
Team Leader	113.08	119.04	98.33	103.51
Quality Analyst	99.33	104.56	86.37	90.92
Training Analyst	99.33	104.56	86.37	90.92
Knowledge Mgmt Analyst	99.33	104.56	86.37	90.92
BCRS Services				
BCRS Engineer Expert	149.30	157.16	129.83	136.66
BCRS Engineer Specialist	201.41	212.01	175.14	184.36
BCRS SME	237.03	249.50	206.11	216.96
BCRS Consultant	144.27	151.86	125.45	132.05
Project Delivery Engineer	124.82	131.39	108.54	114.25
Project Integration Engineer	88.53	93.18	76.98	81.03
Service Management Services				
CFGM-Configuration Manager	135.93	143.08	118.20	124.42
SOM-Incident Manager	135.93	143.08	118.20	124.42
SOM-Critical Incident Manager	135.93	143.08	118.20	124.42
SOM-Problem Manager	135.93	143.08	118.20	124.42
SOM-Change Manager	135.93	143.08	118.20	124.42
SVLM-Service Level Analyst	117.43	123.60	102.11	107.48
SVLM-Service Level Manager	135.93	143.08	118.20	124.42
CAPM-Capacity Manager	135.93	143.08	118.20	124.42
AVBM-Availability Manager	135.93	143.08	118.20	124.42
AVBM-Availability Manager	135.93	143.08	118.20	124.42
RPT-Standard Reports Support	135.93	143.08	118.20	124.42
Account Management Services				
Account Executive	160.32	168.76	139.41	146.75
Account Delivery Executive	160.32	168.76	139.41	146.75
Account PMO Manager	160.32	168.76	139.41	146.75
Account Chief Technologist	160.32	168.76	139.41	146.75
Chief Engineer	160.32	168.76	139.41	146.75
Program Manager	160.32	168.76	139.41	146.75

Attachment C - Pricing Discounts and Schedule

Contractor: DXC Technology Services, LLC

Program PMO Manager	135.86	143.01	118.14	124.36
Account Arch / Chief Architect	160.32	168.76	139.41	146.75
Lead Engineer	160.32	168.76	139.41	146.75
Account Operations Manager	307.42	323.60	267.32	281.39
CABO Services				
SRM-Account Manager (ABM Ops-SSR)	160.32	168.76	139.41	146.75
SRM-Account Manager (ABM Ops-NSSR)	160.32	168.76	139.41	146.75
ABO-ABOE FMO (Account Business Client Manager	133.49	140.52	116.08	122.19
AWS & Azure Services				
Sr. Architect / Engineer	373.75	393.43	325.00	342.11
Architect / Engineer	316.25	332.89	275.00	289.47
Associate Engineer	287.50	302.63	250.00	263.16
Program Manager	316.25	332.89	275.00	289.47



DXC Technology's Response to

The State of Utah

Division of Purchasing

NASPO ValuePoint Master Agreement
for Cloud Solutions

Technical Response

Utah Solicitation Number SK18008

July 06, 2018 at 3pm MT



Important Notice

This document has been prepared by DXC Technology in response to the RFP for Cloud Solutions issued by The State of Utah in conjunction with NASPO ValuePoint ("**Customer**").

The information contained in all contents of this document and all schedules, annexures and attachments to it (collectively "**Document**") is provided in accordance with DXC Technology's response to the RFP for Cloud Solutions. Any and all information contained in the document identified as "PROTECTED", "CONFIDENTIAL" or "PROPRIETARY" (collectively "**Confidential Information**") is confidential information of DXC Technology Company or its affiliates (collectively "**DXC**") and is provided for evaluation purposes only. In consideration of receipt of this Document, Customer agrees to maintain the Confidential Information of this Document in confidence and not to reproduce or otherwise disclose this information to any person or entity outside the Customer group directly responsible for evaluation of its contents, unless otherwise authorized by DXC in writing.

DXC has prepared this Document in good faith based on information made available to it by Customer and DXC reserves the right to make amendments and correct any errors that are identified after submission of it. Neither DXC nor its representatives make any representations or warranties as to the accuracy or completeness of the information provided in here and neither DXC nor its representatives shall have any liability towards Customer or any of its representatives resulting from Customer's use of the information provided.

This Document is provided subject to agreement on a mutually acceptable written contract. Except as agreed in such a contract, nothing in this Document or in any related discussions or correspondence should be construed as an offer or representation that should be relied upon.

The term "solution" in the context of this Document is defined as the products and services proposed in here. Since additional information may be required from Customer to develop the appropriate configuration for Customer's specific requirements, the term "solution" does not imply that those products or services as proposed are guaranteed to, or will, meet the Customer's requirements.

The use of the terms "partner" or "partnership" in this Document does not imply a formal, legal, or contractual partnership, but rather a mutually beneficial relationship arising from the teamwork between DXC and its vendors.

If this Document is submitted in both electronic format and hard copy formats and the contents differ, only the hard copy will constitute the valid DXC proposal. If no hard copy is submitted and if the content differs between the PDF version and any other electronic format, only the PDF version will constitute the valid DXC proposal.

If there are any concerns, questions, or issues regarding this Document please contact:

DXC Representative Name: Chris Van Vlack
Email: chris.van-vlack@dxc.com
Telephone: 916.846.7356





Table of Contents

8 Technical Response	4
8.1 Technical Requirements	6
8.2 Subcontractors	8
8.3 Working with Purchasing Entities	10
8.4 Customer Service	22
8.5 Security of Information.....	28
8.6 Privacy and Security.....	32
8.7 Migration and Redeployment Plan	44
8.8 Service or Data Recovery.....	46
8.9 Data Protection.....	55
8.10 Service Level Agreements.....	63
8.11 Data Disposal	69
8.12 Performance Measures and Reporting.....	72
8.13 Cloud Security Alliance.....	81
8.14 Service Provisioning	82
8.15 Back Up and Disaster Plan.....	83
8.16 Hosting and Provisioning	87
8.17 Trial and Testing Periods (Pre- and Post- Purchase).....	95
8.18 Integration and Customization.....	101
8.19 Marketing Plan.....	105
8.20 Related Value-Added Services to Cloud Solutions	106
8.22 Supporting Infrastructure	118
Attachment G – Identification of Service Models Matrix.....	120





8 Technical Response

A. A complete narrative of the Offeror's assessment of the Cloud Solutions to be provided, the Offeror's ability and approach, and the resources necessary to fulfill the requirements. This should demonstrate the Offeror's understanding of the desired overall performance expectations and clearly indicate any options or alternatives proposed.

NASPO ValuePoint's Participating Entities realize the strategic importance of having the right foundation for a digital platform, but also know that developing, implementing and managing a digital strategy across their organizations is no easy task. DXC Technology was founded on a mission and core enabling competencies aimed at serving our clients as their trusted advisor, guiding them on their journey to transform into substantially information-driven organizations, through digital platforms. We support this objective through best-practice advisory services, mature solutions across all NIST defined cloud service and deployment models, and proven transformational methodologies, to help our clients modernize traditional IT by designing, implementing and managing digital solutions.

In assembling our proposed catalog of cloud solutions for this solicitation, DXC's extensive portfolio of cloud services readily aligned to the broad scope of solutions which the NASPO ValuePoint RFP has specified. Throughout our responses to the below Technical Response sub-sections, DXC has strived to provide the essential details of our capabilities and approach to each posed question, often providing details and examples specific to key offerings in our catalog. Due to the extensive range of our service offerings – based on standard platforms and partner offerings but tailorable to each Purchasing Entity's unique requirements – we have attempted in our responses to cover the essential points to address each question, while recognizing that doing so exhaustively across every offering in our catalog would be a prohibitive exercise.

As cloud architecture has taken root in IT strategy, some businesses have adopted a public cloud-first approach. In certain circumstances, however, a public cloud may not be appropriate or desired for a particular workload, due to regulatory compliance, architecture constraints, software licensing or data sovereignty requirements. For most large organizations such as the NASPO Participating Entities, a more comprehensive portfolio of cloud solutions is needed, recognizing that "one size does *not* fit all", and that often a hybrid cloud approach that effectively integrates multiple deployment models including private, virtual private, and community clouds in addition to public cloud, is essential to service the entire spectrum of workloads that organizations rely on to operate effectively and efficiently. DXC's proposed catalog of cloud solutions addresses all these models with industry leading Managed Services, to ensure you leverage the greatest value from your digital solution investments.

Digital transformation is not about only adopting new technology, but also planning and operating differently, focusing on the end user experience at the center. Key to doing this successfully is having a true digital platform — a set of services that work together and enable the enterprise to derive value from a consistent data-driven operating model. By leveraging DXC's value added integration capabilities in combination with our cloud enablement services, Purchasing Entities are assured of having a solid foundation for a successful path to becoming agile, digitally enabled enterprises.

DXC stands ready with the experience, proven methodologies, and resources necessary to be the digital transformation partner of NASPO's Participating Entities. Our approach can be tailored to each client's goals and situation to deploy the right mix of transformation engagements from tactical to strategic, using a range of engagement types from QuickStarts





and proof of concepts, pilot deployments and assessments, through full strategic roadmaps that define a complete plan to migrate an enterprise over a series of waves and sprints.

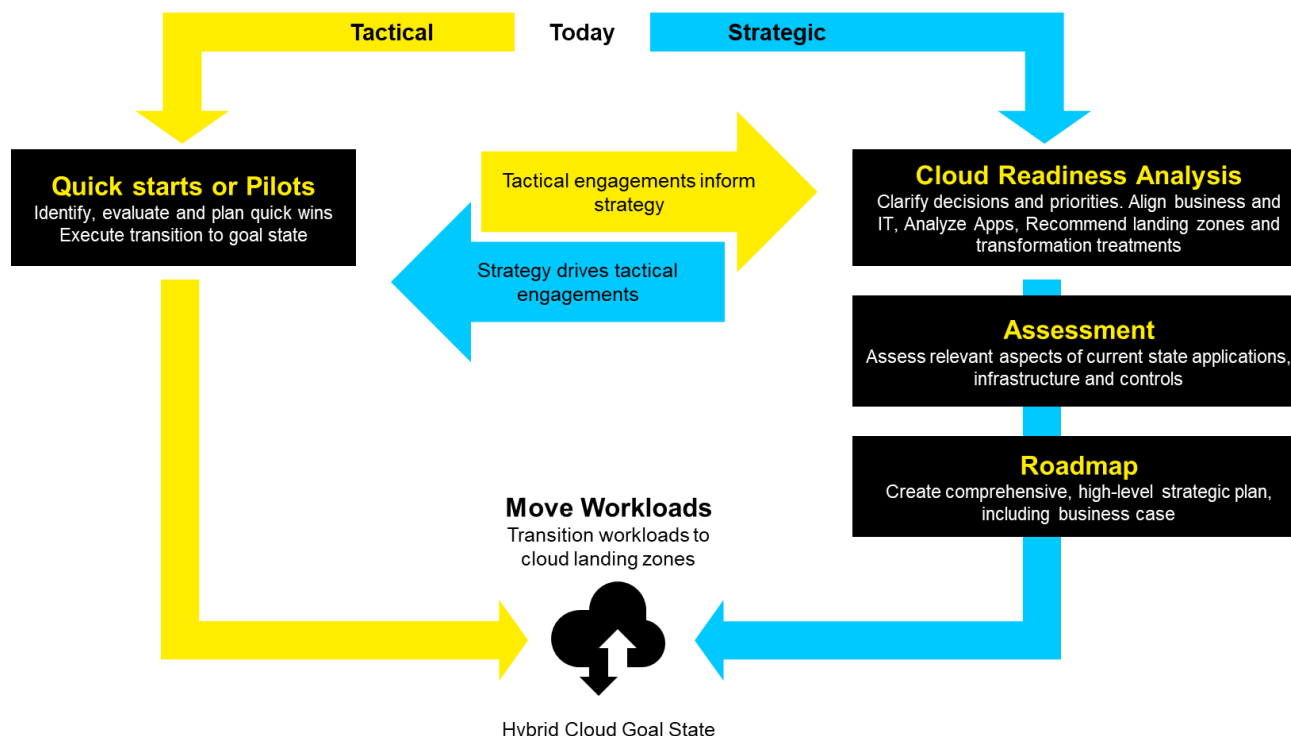


Figure 1: DXC Cloud transformation methodologies

When it comes to execution, our specialized transition teams have the mature, proven tools and methodologies, and experienced staff to migrate your workloads to the target landing zones efficiently and with minimal risk.

As the industry's leading provider of end-to-end IT services and solutions, DXC's integrated suite of capabilities provides NASPO ValuePoint and its Purchasing Entities the assurance that DXC can successfully and securely move the right workloads to the right cloud platforms, to rapidly modernize and integrate their applications, and that DXC will work with them to achieve the expected results at every step of the journey.





B. A specific point-by-point response, in the order listed, to each requirement in the Section 8 of the RFP. Offerors should not provide links to a website as part of its response.

8.1 Technical Requirements

The following subsections comprise DXC's response to meeting NIST essential characteristics, being willing to comply with the requirements stated in Attachments C and D, and describing how DXC's offerings adhere to the definitions, and deployment models identified in the Scope of Services.

8.1.1 *For the purposes of the RFP, meeting the NIST essential characteristics is a primary concern. As such, describe how your proposed solution(s) meets the characteristics defined in NIST Special Publication 800-145.*

DXC understands the requirement for a standardized approach to the cloud environment. Therefore, DXC's proposed portfolio of cloud-based offerings in this response comply with the NIST Special Publication 800-145 definition for Cloud Computing.

DXC's Chief Information Security Officer (CISO) establishes these policies and standards. A special publication describes flexibility for cloud computing in service models SAAS, PAAS and IAAS and in the cloud-deployment mode (private, public and hybrid). DXC provides the data security and privacy for the stated services and deployment models.

DXC Cloud infrastructure and Services solution, similar to those available from AWS or Azure, have been validated by third-party testing performed against the NIST 800-53 Revision 4 controls, as well as additional FedRAMP requirements.

Also, please refer to DXC's list of proposed cloud offerings, provided in our response to 8.1.3.

DXC will provide both cloud service and deployment models to the Purchasing Entities. We offer the NIST Service Model, which combines Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The deployment models are private cloud, community cloud, public cloud, and hybrid cloud.

With our extensive partner community, DXC provides its clients with innovative next-generation technology solutions and services that leverage deep industry expertise, global scale, and technology independence. We provide the essential characteristics of cloud computing, such as:

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity and expansion
- Measured services

DXC is committed to assisting our Federal customers, who are required to comply with the Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. We continue to develop tools and resources to address both the core risks outlined in NIST and implementing the NIST Cybersecurity Framework (CSF) as the order requires.

DXC provides Purchasing Entities with NIST-standardized data security methods to mitigate data breaches and adhere to data privacy compliance regulations. We do this by delivering a proven and NIST-standardized method of protecting data in use, at rest, and in motion, to enable government agencies, global enterprises, and European organizations to comply with





General Data Protection Regulation (GDPR) requirements. This includes Unicode format and character set-preserving encryption for data to help Purchasing Entities if a data breach occurs. Strong end-to-end encryption and tokenization will render stolen data useless to attackers, and thereby mitigates any financial, operational or reputational ramifications.

8.1.2 As applicable to an Offeror's proposal, Offeror must describe its willingness to comply with, the requirements of Attachments C & D.

DXC will comply with the requirements as stated in Attachment C, NIST Service Models, and Attachment D, Scope of Services.

8.1.3 As applicable to an Offeror's proposal, Offeror must describe how its offerings adhere to the services, definitions, and deployment models identified in the Scope of Services, in Attachment D.

DXC's Cloud Services Model(s) and Deployment Model(s) will provide the Purchasing Entities with market-leading, cloud-based service offerings and solutions. DXC has extensive experience customizing cloud architectures for state, local, federal governments, as well as enterprises that adhere to the services, definitions, and deployment models identified in the Scope of Services in Attachment D.

DXC's cloud services offering provides various templates from which a Purchasing Entity may choose. During negotiations, DXC will analyze the Purchasing Entities' needs and provide guidance them to accommodate their current processing capacities.

DXC's proposed portfolio of cloud offerings is aligned with the services, definitions and deployment models identified in Attachment D, as per the table below.

	Public Cloud	Community Cloud	Private Cloud
IaaS	1) Oracle As Service 2) Cloud Security Advisory Services 3) Managed Cloud Access Security Broker 4) On-demand Workload Protection 5) Infrastructure & Endpoint Security Advisory Services 6) Managed Endpoint Threat Detection and Response 7) DXC Managed Service for Azure and AWS 8) Cloud & Platform for Advisory Services	1) Virtual Private Cloud 2) Workplace AD-Integration, Migration 3) Workplace – Desktop/Application Virtualization (Delivery) 4) Oracle As Service 5) On-Demand Workload Protection 6) Cloud & Platform for Advisory Services 7) Managed Services for VMware	1) Virtual Private Cloud 2) Managed services for VMware
PaaS	1) PaaS for SAP on AWS 2) PaaS for SAP on Azure 3) Managed Container PaaS for RedShift	1) PaaS for SAP	1) PaaS for SAP
SaaS	1) Application – Custom development using .NET (Azure) Java (AWS) 2) Application – Testing and Digital Assurance 3) DXC Migration Services for Oracle Cloud 4) ServiceNow Applications 5) Emerging Practices – Salesforce 6) Emerging Practices – Workday 7) Workplace AD – Integration, Migration 8) Workplace – O365 on Azure 9) Workplace – Skype for business 10) Workplace – Mobility Service 11) Security Services – Consulting Service 12) Microsoft Dynamics 365	1) Workplace – Desktop / Application Virtualization (Delivery) 2) DXC Migration Services for Oracle Cloud 3) Application-Testing and Digital Assurance	1) DXC Migration Service for Oracle Cloud





8.2 Subcontractors

8.2.1 Offerors must explain whether they intend to provide all cloud solutions directly or through the use of Subcontractors. Higher points may be earned by providing all services directly or by providing details of highly qualified Subcontractors; lower scores may be earned for failure to provide detailed plans for providing services or failure to provide detail regarding specific Subcontractors. Any Subcontractor that an Offeror chooses to use in fulfilling the requirements of the RFP must also meet all Administrative, Business and Technical Requirements of the RFP, as applicable to the Solutions provided. Subcontractors do not need to comply with Section 6.3.

As part of the Master Services Agreement (MSA), DXC will perform the services requested. If we find that an additional need exists, we will identify the proper subcontractor who can participate in our overall solution framework. We will determine the service to be provided, and the given percentage of their involvement within the respective solution or service delivery.

One of our key differentiators in the industry is our robust programmatic structure of our more than 250 industry-leading, proven, strategic and solution partners. They work closely with us to address complex, critical client business challenges. Together, DXC and our partners offer a wide range of solutions at significant scale that enables us to accelerate innovation, and serve clients more efficiently and effectively worldwide.

The following content describes the categories of partnerships within the DXC Partner Network.

DXC Partner Network Categories

 Strategic Partners	 Solution Partners	 Channel Sales Partners	 Supplier/Reseller Partners
Deep, comprehensive, global partnerships with joint business objectives and a drive to continuously solve complex, critical client challenges 	Regional, industry, offering or frontier relationships with specialized expertise to exceed our clients' expectations 	Ability to scale globally and market and resell DXC offerings and services through experienced sales teams 	Providing the essential components that complete DXC solution offerings with consistent, replicable outcomes for each client 

Note: Partner list not exhaustive

Strategic Partners

Our Strategic Partners represent our deepest, most comprehensive partner relationships. Our joint business objectives, mutual investments, co-development, and scalability help our clients harness the power of technology to transform their business. Each partner also shares our drive to continuously exceed expectations, along with the ability to deliver solutions globally.

Solution Partners

Our more than 200 Solution Partners focus on specific technology-focused objectives. These partners are designated across four complimentary ecosystems:

- Offering Partners who bring critical solutions that enhance our ability to build our offerings





- Regional Partners who provide capabilities that help us deliver in specific geographic areas
- Industry Partners who provide expertise, intellectual property, or niche-market access for specific industries
- Frontier Partners who offer emerging solutions and significant future potential for bringing innovative approaches to solutions.

They work with us to provide technical expertise and differentiation at all levels of digital transformation.

8.2.2 Offeror must describe the extent to which it intends to use subcontractors to perform contract requirements. Include each position providing service and provide a detailed description of how the subcontractors are anticipated to be involved under the Master Agreement.

DXC has the staff, experience, and capability to manage Purchasing Entities' work under the contract. The solutions being proposed for the Master Agreement are standard DXC offerings that do not rely on subcontractors for delivery of the services. We only use subcontractors if a unique or custom requirement in a task order calls for a niche subcontractor to be leveraged to help expedite effective service delivery.

8.2.3 If the subcontractor is known, provide the qualifications of the subcontractor to provide the services; if not, describe how you will guarantee selection of a subcontractor that meets the experience requirements of the RFP. Include a description of how the Offeror will ensure that all subcontractors and their employees will meet all Statement of Work requirements.

DXC will serve as the managed service provider with the capabilities necessary to fulfill the requirements of the Purchasing Entities. We are able to eliminate dependencies on subcontracting requirements.

If a subcontractor is identified as needed to meet a requirement, DXC will make certain that the selected subcontractor meets the experience requirements of the RFP. DXC sources, selects and works with only the most reputable business partners, agents, subcontractors, suppliers and vendors. To manage the risk in these third-party relationships, some measure of risk-based due diligence is prudent. We have an established Third-Party Risk Management policy, which provides risk-based guidelines for evaluating and engaging third parties. All third-party relationships are proactively monitored and managed to make certain that they comply with negotiated agreements.





8.3 Working with Purchasing Entities

8.3.1 Offeror must describe how it will work with Purchasing Entities before, during, and after a Data Breach, as defined in the Attachments and Exhibits. Include information such as:

- Personnel who will be involved at various stages, include detail on how the Contract Manager in Section 7 will be involved;
- Response times;
- Processes and timelines;
- Methods of communication and assistance; and
- Other information vital to understanding the service you provide.

DXC has a standard and organized approach to provide security services in the Purchasing Entity's cloud infrastructure environment, which will be embedded in DXC service-delivery model. For Purchasing Entities, these services are intended to simplify and improve the overall security posture and enforce compliance with standards and regulations. DXC provides security as a service, building security into the fabric of DXC's overall delivery capabilities, meeting reporting obligations, and supporting audit requirements set forth by the Purchasing Entities.

The standard security services to support Purchasing Entity security and compliance requirements encompass data center, server, operations, storage and backup, audit, automation, and network areas, as highlighted in the following figure.

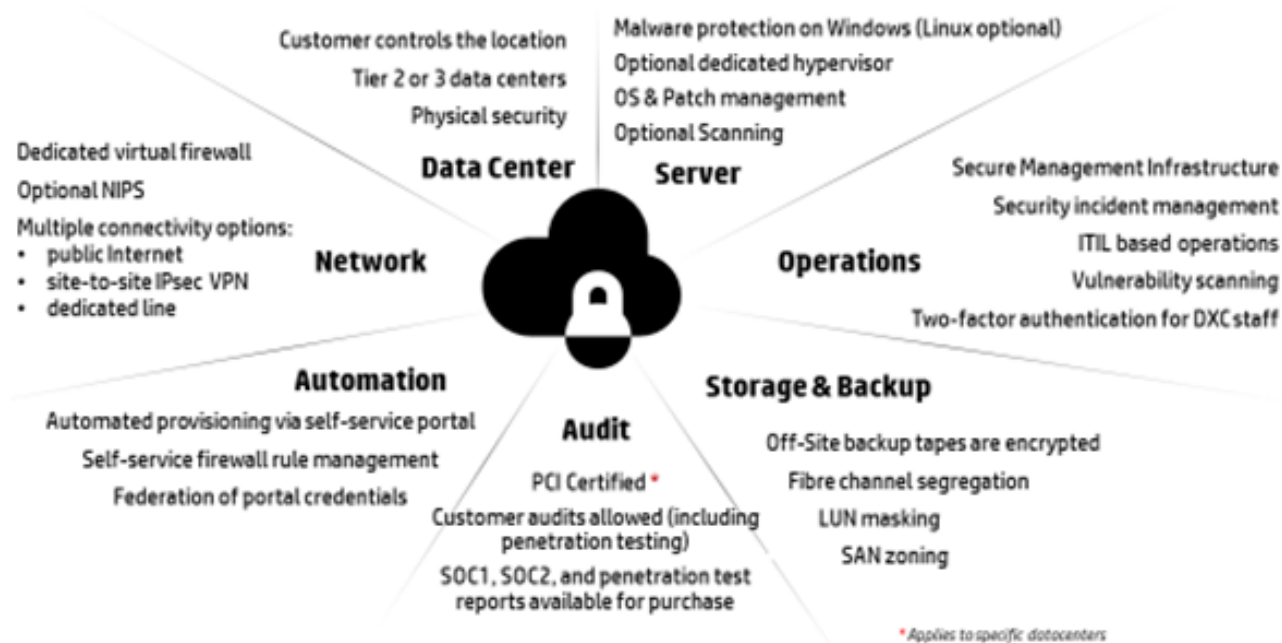


Figure 2: Security and Compliance

DXC always works toward security of client/personal data, and to achieve this DXC follows the industry-standard security solution and data protection approach supported by best resources. However, in the case of a data breach, DXC supports our clients during all three phases of data breach to provide enhanced security and forensics as detailed in the descriptions that follow.





Before Data Breach: Data is secured while at rest, in transit, and in use, and access to the data is controlled.

- DXC cloud solution uses volumetric key management for secure replication of keys across multiple appliances with automated backups and transparent database encryption for both Oracle and SQL.
- Preventing unauthorized access to information resources in the cloud is a major consideration for cloud consumers. One recurring issue is that the organizational identification and authentication framework may not naturally extend into the hybrid cloud environment.
- DXC uses identity federation, which allows Purchasing Entity and DXC to trust and share digital identities and attributes across both domains, and to provide a means for single sign-on. Clear separation of the managed identities of Purchasing Entity from those of DXC is enforced to protect Purchasing Entity's resources from DXC-authenticated entities and vice versa.
- Endpoint Threat Management (EPTM) is a managed service designed to guard servers against viruses, malware, spyware, and other unauthorized intrusions. DXC remotely manages and monitors supported virus technologies (EPTM Agents) by operating the EPTM management infrastructure (Management Console) using DXC delivery organizations, operational tools, and processes.
- Server Security Compliance service involves the Account Security Officer reviewing and assessing raw server compliance data to identify areas of potential non-compliance. Exception and mitigation requirements will be documented and communicated to Purchasing Entity, on a regular basis, per the established Governance model.

During Data Breach: To protect data during a data breach, DXC provides the following services:

- DXC experts offers comprehensive, 24x7x365 monitoring delivered from DXC's 12 Security Operations Centers.
- Provides expert analysts that investigate alerts, and validates attacks which trigger investigations
- Offers a Security Portal that provides clients with a granular view of their current security state, and enables clients to conduct their own searches, as well as monitor all open incidents in real-time
- Comprehensive 24x7x365 service to provide rapid response time and minimize breach impact

DXC's Advanced Compromise Assessment (ACA) allows our clients to identify whether adversaries are active within their enterprise, and includes the following:

- Monitors Internet gateways to monitor traffic and scans it against DXC proprietary threat intelligence to identify threat actor communications
- Performs initial investigation of selected end points to search for indicators of compromise
- Identifies actors triggers incident response and/or remediation





- Focuses on abnormal activity by an account, and deviations from the standard activity patterns that allow for quick identifications of hijacked accounts

After Data Breach: DXC provides Incident Response and Digital Forensics following the data breach to make sure that it will not happen again. DXC provides the following services to do so:

- Provides deep-dive analysis to understand the breadth of compromises and then present damage assessments
- Conducts investigations based on evidential standards to support legal actions
- Provides highly trained teams who possess numerous professional and academic credentials
- Provides DXC experts who advise on in-house threat intelligence deployment and optimizations, while providing intelligence assessments, and uses built-in Security Monitoring to identify attacks
- Conducts analysis using DXC proprietary intelligence and methods to identify attackers in the client's environment. These are essential components of any defensive posture to make certain that advanced actors who breach the network are not given time to conduct reconnaissance to enable planning and preparation for a more complex attacks
- Focuses on abnormal activity by an account, and deviations from the standard activity patterns that allow for quick identification of hijacked accounts
- Identifies attackers who have breached enterprise defenses

Security incidents must be reported immediately to the DXC Security Incident Response Coordination Center (SIRCC). Security incidents are assessed by the DXC SIRCC and then categorized in accordance with client-defined procedures (incident management workflow).

Personnel who will be involved at various stages, include detail on how the Contract Manager in Section 7 will be involved;

The DXC security team will collaborate with the Purchasing Entities, as required and engage through DXC's Contract Manager as identified in section 7.1 of this proposal document.

DXC's Contract Manager, Chris Van Vlack, has complete understanding of the contract. Chris will assist the NASPO as a single point of contact for DXC's contract and will work with Purchasing Entities. He has experience working with Purchasing Entities. The DXC team working under Chris will perform a number of tasks in various stages.

During the participating addendum period, the Purchasing Entities can select and define varying levels of dedicated security service, which will be defined based on DXC's managed services offering.

The table that follows under the Processes and Timelines heading shows the DXC security personnel and their role in working with the Purchasing Entities throughout the project management process.





Response times;

When a security incident occurs, DXC will use incident-triggered analysis to help determine the full extent of the breach and what effect it has had on the business. Our incident responders and forensics experts are available 24x7x365 to enable a rapid response and minimize damage. As part of our incident response solution, we quickly locate any compromised device, remove it, and rapidly return to normal operations.

DXC provides 24/7 coverage for incident response, from detection through to resolution and follow-up. All security events are centralized at a SIEM and then reviewed by our analysts. Additionally, we staff a threat intelligence team and work closely with our clients to analyze threats and determine the risk to our clients' systems. Actionable intelligence is acted upon quickly, resulting in security control reconfiguration and additional monitoring rules, as appropriate.

Processes and timelines;

The following steps summarize the life cycle for DXC security event management policies and standards, which guides our response to security incidents and breaches.

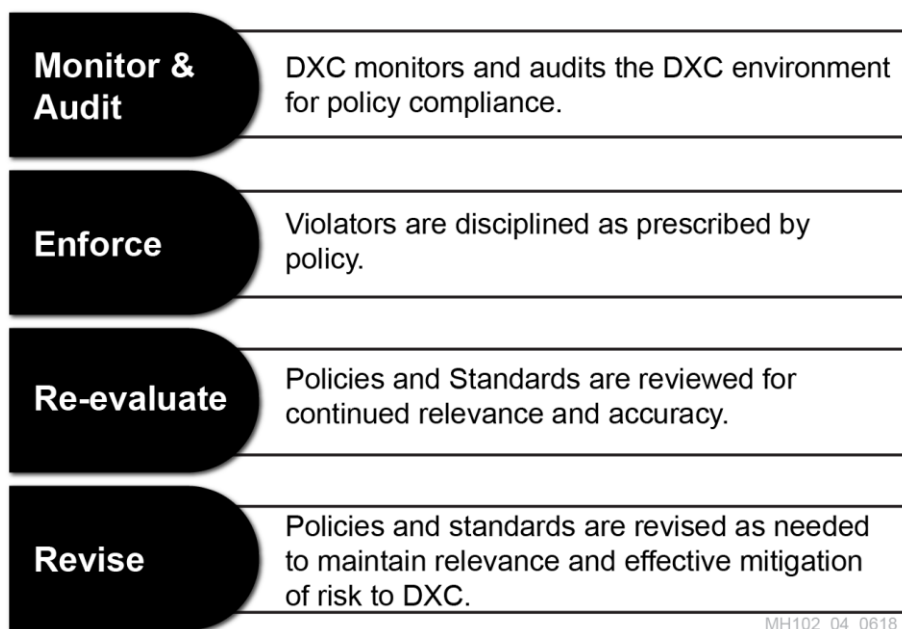


Figure 3: Life Cycle for DXC Security Event Management Policies and Standards

The following are additional DXC SaaS offerings that address data breaches. DXC's Security Incident procedure follows a similar process as other Cloud Support incidents.

Security Monitoring includes the following:

- Offers comprehensive, 24x7x365 monitoring delivered from DXC's 12 Security Operations Centers
- Provides expert analysts that investigate alerts, and validates attacks which trigger investigations





- Offers a Security Portal that provides clients with a granular view of their current security state, and enables clients to conduct their own searches, as well as monitor all open incidents in real-time
- Removes CAPEX costs and SOC infrastructure maintenance overhead

Incident Response and Digital Forensics and includes the following:

- Comprehensive 24x7x365 service to provide rapid response time and minimize breach impact
- Provides deep-dive analysis to understand the breadth of compromises and then present damage assessments
- Provides investigations conducted based on evidential standards to support legal actions
- Provides highly trained teams who possess numerous professional and academic credentials

DXC's Advanced Compromise Assessment (ACA) allows our clients to identify whether adversaries are active within their enterprise, and includes the following:

- Monitors Internet gateways to monitor traffic and scans it against DXC proprietary threat intelligence to identify threat actor communications
- Performs initial investigation of selected end points to search for indicators of compromise
- Identifies actors triggers incident response and/or remediation

Threat intelligence and Threat Hunting includes the following:

- Provides DXC experts who advise on in-house threat intelligence deployment and optimizations, while providing intelligence assessments, and is built into Security Monitoring to identify attacks
- Conducts analysis using DXC proprietary intelligence and methods to identify attackers in the client's environment. These are essential components of any defensive posture to make certain that advanced actors that breach the network are not given time to conduct reconnaissance to enable long-con style attacks

Behavior Analytics includes the following:

- Includes close partnerships with a number of organizations specializing in behavior analytics
- Focuses on abnormal activity by an account, and deviations from the standard activity patterns that allow for quick identifications of hijacked accounts
- Provides the same principle for network components, such as servers and applications
- Identifies attackers that have breached enterprise defenses

Security incidents must be reported immediately to the DXC Security Incident Response Coordination Center (SIRCC). Security incidents are assessed by the DXC SIRCC and then categorized in accordance with client-defined procedures (incident management workflow).

Methods of communication and assistance; and

DXC continuously maintains an open communications channel with our IT incident management team and addresses threats in real-time to determine the security impact. In addition to security





event monitoring and the ongoing relationship with intelligence and incident teams, system/application outages and performance issues are constantly monitored. DXC uses a variety of methods to spot volumetric attacks. We also monitor edge devices, which provide an entry point into enterprise or service provider core networks within the DXC infrastructure.

Other information vital to understanding the service you provide.

DXC's security experts constantly manage real-world incident responses at some of the largest organizations across the globe, giving us unique insights into the decisions that executives will face and making certain that the support accurately reflects the response scenario. We help our clients craft an improvement roadmap to demonstrate that response capabilities improve to meet the next attack.

With a global workforce of highly experienced security professionals, DXC is an industry leader in enterprise security. Our advisory-first approach reduces risk, and our analytics drive advanced detection. Clients can count on DXC to provide comprehensive security services with a flexible consumption model to meet their needs. Here is what sets DXC apart from our competitors:

- Global reach, availability, and scale—DXC managed services provides 24x7x365 support to drive and protect the client's business. DXC has more than 4,000 security advisors and more than 12 Security Operations Centers worldwide.
- Advisory-led approach—Provides clients with access to some of the most experienced security operators in the world, helping to accurately pinpoint optimization opportunities and craft security improvement plans using our proprietary Reference Architecture to help clients achieve best practice and gain significant risk reduction.
- Industry-recognized and NSA-accredited expertise in incident response—DXC advisors offer comprehensive reactive and preemptive incident response services using the latest threat intelligence and leading technology. Expert teams with deep forensic experience deliver cost-effective rapid responses that minimize business disruption and use globally available state-of-the-art forensic laboratories and testing facilities to deliver tailored forensic advice and assistance.
- Intelligence-driven approach—DXC proprietary threat intelligence is gathered from providing security to some of the largest companies in the world and responding to scores of incidents each year. This intelligence is an advantage in identifying the most severe of threats that would otherwise evade detection.
- End-to-end security services—DXC offers a single source for security advisory services, managed services, and third-party technology, enabling delivery of complete remediation plans and security improvement programs.
- Technology independence – DXC's expansive threat intelligence enhances monitoring and detection services, and our technology partnerships with security leaders generate innovative solutions.

8.3.2 Offeror must describe how it will not engage in nor permit its agents to push hardware, software, or marketing not explicitly authorized by the Participating Entity or the Master Agreement.

DXC recognizes that any Master Agreement resulting from this NASPO solicitation is intended as a vehicle to help Participating Entities procure specific Cloud Solutions identified in the





Master Agreement, and does not constitute an open-ended invitation for DXC agents to push or market to Participating Entities hardware, software, or services not identified in the Master Agreement.

All DXC employees are required to annually review and certify to the DXC Code of Business Conduct, which includes strict policies and guidelines for proper and ethical client engagement. All breaches of the DXC Code of Business Conduct by a DXC employee that are reported internally or by clients or third parties are seriously considered, promptly investigated, and addressed appropriately.

8.3.3 Offeror must describe whether its application-hosting environments support a user test/staging environment that is identical to production.

Where required by the Participating Entity and included in the scope of a subsequent contracting vehicle, DXC will create user test/staging environments that are identical to production. This applies to private, hybrid or public clouds (Amazon Web Services and Azure) and in-scope mobile environments. DXC best practices and templates will be used to create these cloud environments.





8.3.4 Offeror must describe whether or not its computer applications and Web sites are accessible to people with disabilities, and must comply with Participating Entity accessibility policies and the Americans with Disability Act, as applicable.

DXC will comply with the Americans with Disabilities Act as applicable, and will comply with the accessibility policies. DXC's Digital User Experience Assessment service under the Test and Digital assurance offering assesses user requirements and compliance with relevant federal and state level policies. In addition, DXC Business and Application Integration service creates the application programming interfaces to integrate our solutions with assistive technologies. DXC Digital Development Services provide user experience (UX) strategy and design.

8.3.5 Offeror must describe whether or not its applications and content delivered through Web browsers are be accessible using current released versions of multiple browser platforms (such as Internet Explorer, Firefox, Chrome, and Safari) at a minimum.

DXC's proposed solution will be accessible with the current released versions of the leading browser platforms. There will also be some degree of "backward compatibilities" for older versions of some of the leading browsers (such as Internet Explorer, Firefox, Chrome and Safari).

8.3.6 Offeror must describe how it will, prior to the execution of a Service Level Agreement, meet with the Purchasing Entity and cooperate and hold a meeting to determine whether any sensitive or personal information will be stored or used by the Offeror that is subject to any law, rule or regulation providing for specific compliance obligations.

For any implementation, DXC performs a rigorous and defined pre-project assessment to determine the appropriate scope of work. As part of this activity, DXC will work with each Purchasing Entity to understand available sensitive or personal information. A plan of action will be included to address any legal, regulatory, or compliance mandates that may impact access to the sensitive information.

8.3.7 Offeror must describe any project schedule plans or work plans that Offerors use in implementing their Solutions with customers. Offerors should include timelines for developing, testing, and implementing Solutions for customers.

DXC uses best practices in implementing solutions in applications development, infrastructure migration and implementation. Our proprietary tools and accelerators reduce the typical transition duration when compared with a traditional transition timeline. Implementation plans are defined during planning and requirements gathering. These are communicated and refined in collaboration with all relevant stakeholders.

The following figure illustrates a sample high-level implementation plan that DXC provided to a client with similar scope. DXC will define specific plans according to the requirements of the Purchasing Entity.



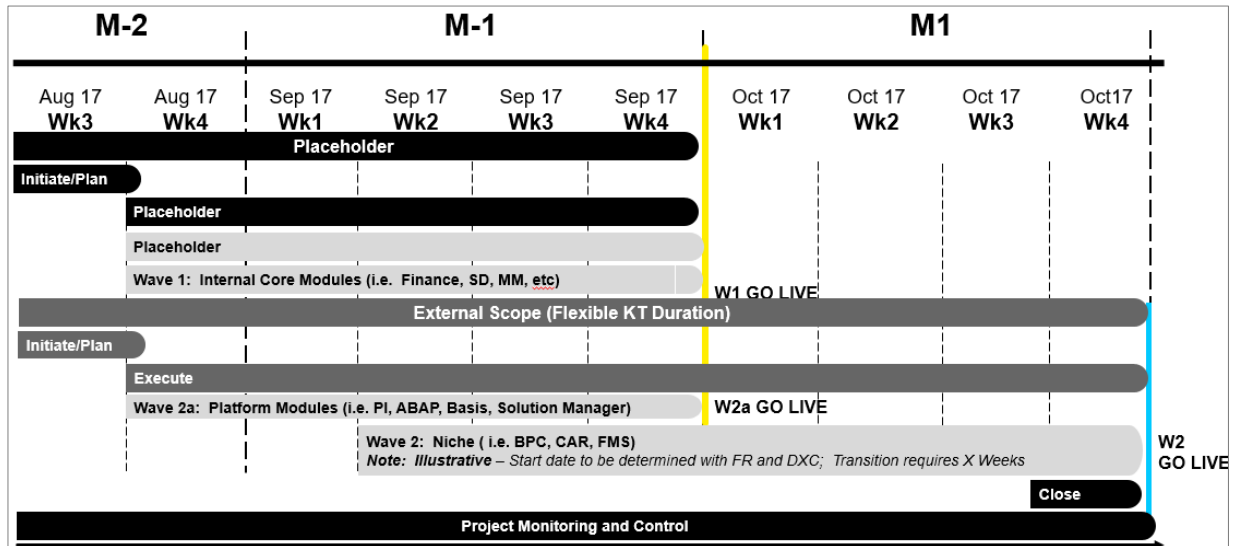


Figure 4: Detailed Transition Plan/Schedule

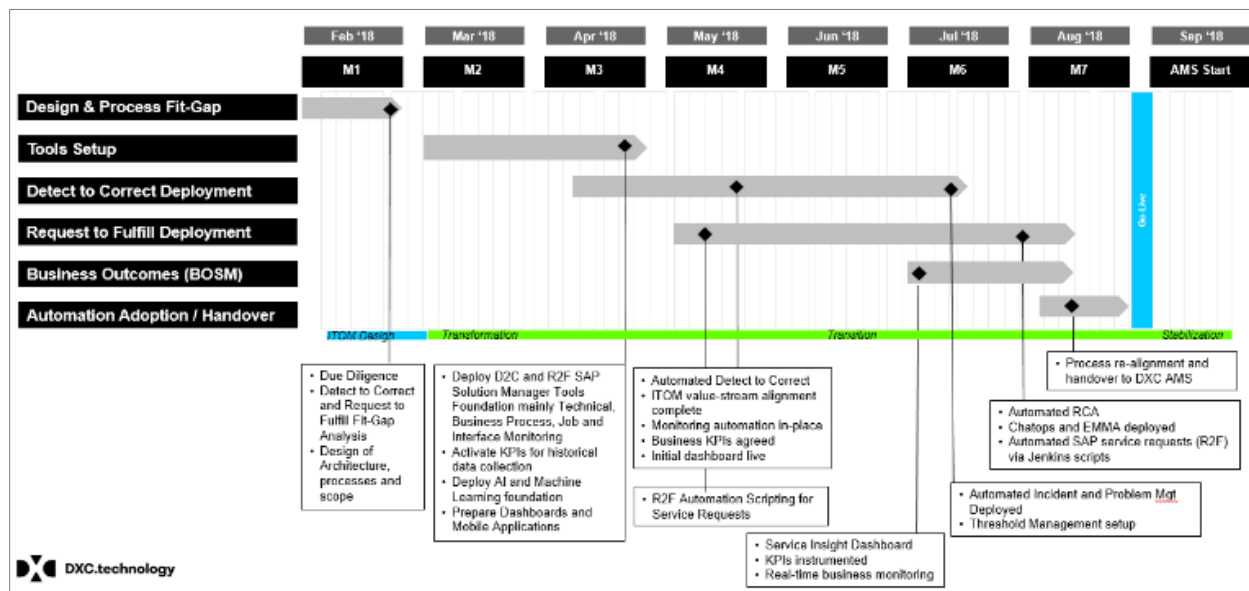


Figure 5: High Level Timeline

DXC provides clients with the capability, scale, and speed to drive business agility and digitalization by developing feature-rich and secure business applications that run on a variety of technology and user platforms. These include on-premises, cloud, mobile, and IoT. Using industrialized and lean delivery, DXC partners with clients to build and manage an applications portfolio to continuously increase value to end users and maximize business outcomes.

DXC uses rapid and continuous delivery leveraging Agile and ITIL principles for implementation, as depicted in the figure that follows.



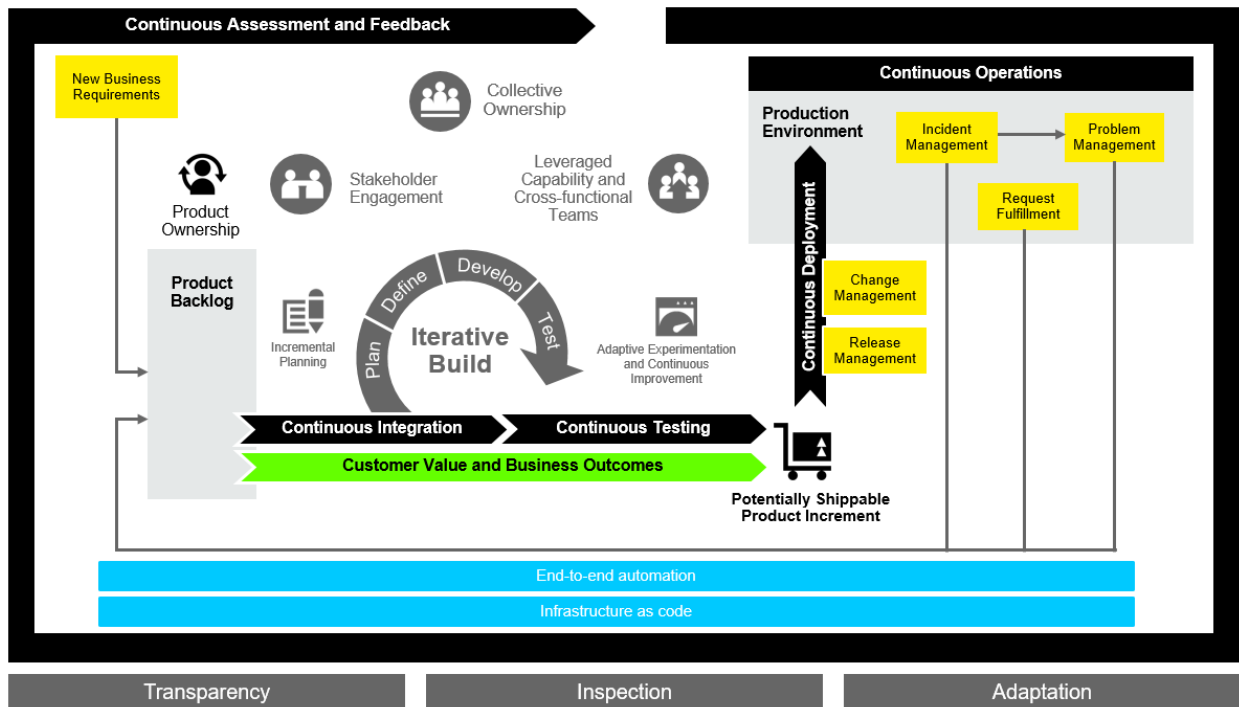


Figure 6: DXC Agile Development Process

To plan and manage the implementation, DXC uses an agile approach to projects using the artifacts in the following list.

- **Product backlogs** - In its simplest form, a Product Backlog could start as a vision of the product we would like to build. These range from well-defined features, to rather vague concepts. This list of ideas must be prioritized, with the most important and valuable at the top. Those at the top tend to be more detailed, well defined, and have a clearer idea of what each will achieve, while those further down may still be quite vague. Each item on the list has a description, an order, and an estimate associated with it.
- **Sprint backlogs** – This is the list of items that have been accepted for a Sprint to create an increment. Just as items in the Product Backlog have a description and an estimate, so do the Sprint Backlog items, with a plan for delivering the work with sufficient detail to make certain that progress can be understood daily.
- **Task boards** - Project teams can customize the task board to depict the status applicable to each task.
- **Burndown charts** – These show the actual and estimated amount of work to be done in a sprint. The horizontal x-axis in a Burndown Chart indicates time, and the vertical y-axis indicates the remaining effort. By interpreting the burndown chart, the team is able to track the total work remaining and the likelihood of achieving the sprint goal on time. Using this information the team can manage its progress and respond accordingly.





8.3.8 The State of Utah expects Offeror to update the services periodically as technology changes. Offer must describe:

How Offeror's services during Service Line Additions and Updates pursuant to section 2.12 will continue to meet the requirements outlined therein.

DXC's Global Product Offering teams manage product lifecycles under a rigorous planning and release process, which includes short- to long-term Plan of Record and Plan of Intent roadmaps. We continuously monitor and evaluate our offerings for alignment with our clients' evolving business needs, technology age, regulatory compliance, and competitiveness, to make certain that they continue to deliver market leading services for our clients.

This means that our clients enjoy the enhanced benefits of DXC's continuously improving capabilities and best practices that evolve and remain evergreen and relevant to industry trends. Occasionally, features that our clients are still actively using may become depreciated, and require a collaborative plan to decommission and/or migrate to a replacement capability or service. DXC will work with the client to define a change management framework to manage changes and updates to service lines and features that have potential to adversely affect the deliverables or continued availability of in-scope services. Some characteristics of this framework include:

- Processing on-request changes that will go through approvals
- Scheduling implementation of approved changes to make certain of minimal disruption to ongoing services
- Providing post implementation monitoring and support, with roll-back processes in place to make certain that business is minimally affected

How Offeror will maintain discounts at the levels set forth in the contract.

DXC will collaborate with the Purchasing Entity to define on an agreed-upon management review process. The processes will review the scope for work and financial landscape of the engagement. Agreed-upon steps will be planned and discussed to manage any agreed discount.

How Offeror will report to the Purchasing Entities, as needed, regarding changes in technology and make recommendations for service updates.

DXC Digital Strategy and Transformation Consulting provides the Purchasing Entity with the expertise and guidance needed to perform the tasks on the following list.

- Develop strategic plans for digital transformation
- Translate strategy into executable transformation flight plans
- Create the business cases
- Manage organizational change
- Architect, design, and execute the transformation program

These consulting activities will be in collaboration with Purchasing Entity and outputs would generally be in the form of recommendations and roadmaps.





How Offeror will provide transition support to any Purchasing Entity whose operations may be negatively impacted by the service change.

Changes to the current technology landscape will be managed through a change management framework. Post implementation monitoring and support will be in place, with a roll-back process that makes certain that business is minimally affected.





8.4 Customer Service

8.4.1 Offeror must describe how it will ensure excellent customer service is provided to Purchasing Entities. Include:

- Quality assurance measures;
- Escalation plan for addressing problems and/or complaints; and
- Service Level Agreement (SLA).

The following pages present DXC's response to making sure we provide excellent customer service to Purchasing Entities. This description includes quality assurance measures, an escalation plan for addressing problems and/or complaints, and use of Service Level Agreement.

Quality assurance measures

DXC's Quality Assurance (QA) program provides the tools, and processes that give our clients' quality services consistent with industry best practices, while being in-line with our clients' standards. The goal of quality assurance is to maintain and gradually improve business-aligned IT service quality. DXC's quality assurance program responsibilities include the following:

- Develop and employ a quality assurance program, subject to client approval, designed to promote a high level of quality service performance while focusing on measuring and improving reliability, speed, cost-effectiveness, and customer satisfaction
- Write and maintain quality assurance procedures and measurements for activities associated with the services
- Confirm compliance with a published quality assurance program, including adequate internal controls and verification activities
- Allow clients to perform audits that focus on DXC's adherence to its quality assurance procedures and standards, metrics gathered to support quality assurance activities, and DXC's efforts to improve overall quality

Escalation plan for addressing problems and/or complaints

Across the globe, DXC teams actively monitor our operations to manage customer service issues that may arise. When an issue arises, the incident and its resolution is documented and shared throughout DXC to benefit our client environments.

Critical or major incidents, also known as Priority 1 and Priority 2 incidents, require additional management attention and oversight because of their potentially significant business effect. In addition to the standard escalation procedures defined in our service level agreements (SLAs) with the client, DXC has developed the Response to Operational Problems (RtOP) process and supporting applications. Our goal is to expedite communicating critical incidents to leaders. This escalation process enables senior leaders to efficiently manage the service restoration of mission-critical production environments.

A detailed escalation process will be mutually agreed upon during the Project Setup for escalations during the implementation project, as well as during the Process Design phase (or escalations during ongoing service delivery).





Global Service Excellence

Service excellence begins with honest communication. We recognize the need for real-time, unfiltered feedback that flows from the client and the DXC account team to DXC executives for immediate awareness, assessment, and action. We create this flow of information through our Voice of the Client (VoC) program, Service Excellence Dashboard, and service excellence metrics.

Voice of the Client (VoC)

DXC's VoC program collects direct client feedback to improve services and deliver timely, innovative, and valued solutions. We gather input from senior executives and key managers, as well as other individuals that the client wishes to participate. This is done through surveys and interviews, with the information gathered used to deploy improvements. After feedback is received, we develop and share a VoC Improvement Plan to verify alignment on the challenges and opportunities to be addressed. The plan execution is governed regularly with periodic progress reports. The goal of this closed-loop program is to foster improved relationships, as well as continuous service delivery improvement.

Service Excellence Dashboard

The Service Excellence Dashboard is a web-enabled, real-time information system that provides information regarding the quality of services we are delivering. The dashboard is the cornerstone of reporting, feedback, and continuous improvement actions.

Client executives have around-the-clock access to the Client Dashboard to check service delivery status, provide online feedback, and report issues. If a situation requires immediate action, the dashboard automatically alerts DXC leaders. The leaders, in turn, notify the client's key stakeholders about the progress toward the resolution. This complete visibility into service delivery operations helps drive service excellence in a real and measurable way.

Service Excellence Metrics

The viewpoint that customers are at the center of everything we do guides DXC's commitment to course-correction and continuous improvement. We manage customer experiences as a business discipline, measuring how effectively we use perception, description, and outcome metrics to provide context and diagnose the why behind the what.

DXC uses three critical measurements to provide Service Excellence:

- The **Service Excellence Client Loyalty Segment** is an internal measure of the general health of the relationship and services delivered based on overall performance, referenceability, renewability, value, competitive advantage, and quality. To provide the positive experience clients expect, we assess and act on specific feedback, and avoid focusing only on aggregate results.
- The **Net Promoter Score (NPS®)** is a customer loyalty metric developed by Fred Reichheld that expresses how satisfied clients are with DXC services and the relationship. The NPS methodology measures how clients feel about their experiences with DXC and the likelihood that they will recommend DXC to business colleagues or friends.
- When clients reach the point that IT services are stable and consistently meet base-level expectations, the client's desire and need for innovation increases. We measure and monitor **client innovation**—the client's perception of DXC innovation—to verify that DXC is delivering continuous improvements in products, services, tools, and processes.





Service Level Agreement (SLA)

DXC Service Level Management (SLM) defines our process for monitoring, reporting, and improving service level performance in alignment with the client's business. Through SLM, we are able to consistently deliver the agreed-upon service level performance commitments in our Service Level Agreement (SLA) with Participating Entities and discover ways to increase those base levels. Skilled delivery teams, reporting tools, and highly visible service level performance reports enable us to incrementally step up the quality of service the client receives.

SLM integrates into our ITIL®-aligned Service framework and provides a consolidated view of all process metrics across IT towers and geographies. This leveraged, global process performs the functions on the following list.

- Enables consistent support
- Documents agreed-on service targets
- Makes certain that service level requirements are relevant and cost-justified
- Monitors and reviews actual service levels against their SLA targets

The SLM process includes the six sub-processes that follow.

1. Define SLA
2. Create SLM business design
3. Monitor, review, and report service levels
4. Perform Service Improvement Program
5. Manage complaints and compliments
6. Update SLAs

The SLM process provides key activities that establish and define the DXC SLM framework; define and consistently update Participating Entity SLA and service catalog; monitor, review and report Participating Entities' SLAs; and execute the service improvement program.

- Establish/Define the DXC SLM framework—DXC's corporate SLM framework makes certain that all offerings adhere to standards for measuring, monitoring, and reporting SLAs. The corporate SLM framework extends across all clients and involves the elements that follow.
 - Planning activities for new or changed service offerings
 - Defining service level criteria for each offering
 - Communicating proposed and final service level criteria to affected stakeholders
 - Establishing operational level agreements
 - Producing and documenting the final SLM standards
- Define and consistently update Participating Entity SLA and Service Catalog—Based on an organization's requirements, we collaborate with the organization to define and continually update Participating Entity and DXC SLAs. If necessary, we review and amend internal DXC operational level agreements and supporting contracts with DXC partners to make sure they support any non-standard services or service levels. Participating Entities and DXC agree on a mutually acceptable service catalog and associated service levels that are aligned with client business needs. DXC publishes the SLAs to affected parties through mutually defined distribution lists (e.g., business units, DXC delivery organizations, and third-party vendors).
- Monitor, Review, and Report Participating Entities' SLAs—In accordance with time triggers in the approved governance procedures, DXC performs periodic service level reviews with Participating Entities to assess the relevance and performance of current Service Levels. As part of the review, Participating Entities and DXC may negotiate appropriate changes to the





SLA, or to the services, so the services and service levels support clients' current business needs. The review may result in signoff on DXC performance, initiation of a service improvement program (SIP), or engagement of financial management to assess appropriate performance credits or penalties.

- Perform Service Improvement Program—If a service level review indicates non-compliant service performance, DXC initiates an SIP to correct the performance. The first step is for the affected stakeholders to determine the SIP objectives. Objectives should be SMART (specific, measurable, achievable, realistic, and time bound), and clearly state the criteria for success to allow signoff. Based on the SIP objectives, DXC defines and executes corrective actions, engaging change management when necessary, and coordinates progress reviews through program and project management for proper implementation. After we implement the corrective actions, DXC measures outcomes against the SIP objectives to make sure all objectives have been met. To close the SIP, DXC obtains appropriate signoff from Participating Entities and our account teams.

The SLA is negotiated between the client and DXC, with a focus on understanding the client's need for service levels related to workloads or applications. DXC's solution design demonstrates a relationship between client workload services needs and designed-in features, such as availability sets, availability zones and disaster recovery solutions.

For scheduled services downtime for regular cloud infrastructure maintenance and DXC managed services, DXC alerts the client five days before the maintenance is to be performed. This is to make certain that the client has enough notice so that their business is not negatively affected. These service maintenance windows may be mitigated by designing availability sets and availability zones as appropriate.

*8.4.2 Offeror must describe its ability to comply with the following customer service requirements:
a. You must have one lead representative for each entity that executes a Participating Addendum.
Contact information shall be kept current.*

DXC will work with the individual Purchasing Entity to assign a dedicated lead representative to execute the participating addendum. We will keep contact information current.

b. Customer Service Representative(s) must be available by phone or email at a minimum, from 7AM to 6PM on Monday through Sunday for the applicable time zones.

DXC has certified professionals and a deep delivery capability across the globe to support ongoing services issues and installation requests from the Purchasing Entity. Our 24x7 support is in place to make certain that all tickets are resolved.

c. Customer Service Representative will respond to inquiries within one business day.

Depending on the priority level of the issue received, the response time will be determined based on the table that follows.





DXC Issue Priority Level Response Time

Priority Level	Response time
Priority 1	15 minutes
Priority 2	30 minutes
Priority 3	4 hours
Priority 4	One business day

d. You must provide design services for the applicable categories.

e. You must provide Installation Services for the applicable categories.

In addition to complying with the requirements in 8.4.2, DXC offers the following services to respond to questions d and e.

DXC Managed Services for AWS provides design, delivery, and daily operational support for native services within the AWS public cloud. This offering consists of monitoring and managing system software, infrastructure configurations, and service consumption using proven native AWS processes and tools. The native services are further augmented with leading tools to enhance security, forensic cost control and analysis, and integration into ITSM tools. Both AWS' and DXC's managed services scale up and down to continually meet a client's changing business needs. This makes certain that IT costs and services continually align to business demand. Designated silver and gold service bundles address client applications ranging from development and testing to a full-scope managed environment.

AWS Consulting and Advisory services helps manage risk and meet compliance requirements. Key activities within consulting and advisory services are identified in the following list.

- Align with key business issues and desired outcomes
- Clarify current state, constraints, and goals
- Define the optimal AWS virtual datacenter to support workload, security and compliance needs
- Provide workload and application transformation services

DXC Managed Services for AWS and Azure provides design, delivery and daily operational support of compute, storage and virtual network infrastructure within the Azure public cloud. The offering consists of monitoring and managing system software, infrastructure configurations and service consumption using proven processes and tools. Financial and governance services mitigate uncontrolled consumption. Both Microsoft Azure and DXC's managed services scale up and down to continually meet a client's changing business needs. This offering makes certain that IT costs and services continually align with business demand. Silver and gold service bundles address client workloads ranging from development and testing to a full-scope managed environment.

Consulting and Advisory services for AWS and Azure help manage risk and meet compliance requirements. Key activities with our consulting and advisory services are noted in the following list.

- Align with key business issues and desired outcomes
- Clarify current state, constraints, and goals
- Define the optimal Azure virtual datacenter to support workload, security and compliance needs
- Provide workload and application transformation services





Operational Management enables business agility for the customer. Key activities within operation management are identified in the list that follows.

- Management of Microsoft Azure-hosted compute, storage and networking infrastructure
- Bundled options to suit the client's needs
- Pricing aligned with the client's AWS spend
- Security management
- Best practices and governance
- Financial management and cost optimization





8.5 Security of Information

8.5.1 Offeror must describe the measures it takes to protect data. Include a description of the method by which you will hold, protect, and dispose of data following completion of any contract services.

DXC collects, uses, stores, and transfers (collectively, processes) personal information to manage its relationship with its customers, employees, business partners and other third parties (covered individuals) and better serve covered individuals by personalizing their experience and interaction with DXC. We process information in compliance with applicable laws, including appropriate notice and consent, and submit required filings with data-protection authorities, where required.

Data Security Measures for (PAAS, SAAS and IAAS)

Data protection measures are based on the criticality of the information to be held. Prior to solutioning/deployment, DXC will work with the client to evaluate the client's categorizations of their data holdings and will then recommend an appropriate environment and data protection measures. The client will always own client data. DXC will recommend a data security and privacy approach based on the local laws, global policy, and the client's industry.

At the end of their useful life and in accordance with DXC's Records Retention Schedule, DXC will securely dispose of the records and information in accordance with the requirements of Records and Information Management Policy, including sections specific to the secure disposal of certain media, such as the Sanitization and Disposal Policy, and the Removable Computer Media Protection and Handling Security Guideline.

DXC provides complete information security solutions from its portfolio offering to protect the enterprise. We deploy market-leading intellectual property to manage information security risk, enable actionable business intelligence, and integrate security operations. DXC's preemptive approach to information security optimizes investment and improves security posture, enabling our clients to achieve desired business results. DXC offers a complete set of security solutions, shown in the inset figure, with key features and benefits further described in the following figure.



Figure 7: DXC Security Solution





DXC Security Solutions Features and Benefits

Security Offering	Features	Benefits
Security Risk Management	• Security Risk Management Advisory Services • PhishEd Advisory Services • Account Security Governance • Client Security Officer • Technology Compliance	• Understand and measure IT security risk • Develop a holistic risk/cyber security strategy and roadmap aligned with business objectives • Build a proven and agile security architecture
Cloud Security	• Cloud Security Advisory Services • Managed Cloud Access Security Broker • On-Demand Workload Protection • File Integrity Monitoring • Cloud Security Monitoring (FY19)	• Understand use of cloud-based applications, user access, and stored data • Provide policy based control of cloud applications • Monitor defined user, device, and data activity of cloud based applications
Data Protection and Privacy	• Data Protection and Privacy Advisory Services • Data Loss Prevention • Managed public-key infrastructure (PKI)	• Align business data handling with business policy and industry regulations • Prevent important data loss or access without appropriate permission • Build a proven asset classification and data protection strategy
Identity & Access Management	• Identity and Access Management Advisory Services • Identity Management as a Service • Identity Governance and Administration • Privileged Account Management • Authentication Broker • Confident ID - Biometric Authentication • Multifactor Authentication • Security Access	• Provide proven solution design and implementation • Provide advisory guidance to define, deliver and manage the best solution, based on client needs • Provide an agile solution that doesn't inhibit users
Intelligent Security Operations	• Intelligent Security Operations Advisory Services • Incident Response Advisory Services • Security Monitoring Managed SIEM • Log Management (FY19) • Dark Web Monitoring (FY19)	• Protect brand and assets from internal and external cyber threats • Detect threats and compromise vectors, regardless of location or device • Respond to security incidents; mitigate damage • Integrate a complete and continuous security event-monitoring solution across endpoints, identity access, perimeter devices, vulnerability scans, and threat intelligence
Threat and Vulnerability Management	• Threat and Vulnerability Management Advisory Services	• Provide real-time notification of identified vulnerabilities and the associated risks





Security Offering	Features	Benefits
	• Vulnerability Scanning • Vulnerability Intelligence • Applications Security	• Perform vulnerability assessment of endpoints, networks and applications for weaknesses • Prioritize hygiene to reduce effort and cost of unnecessary emergency patching
Infrastructure & Endpoint Security	• Infrastructure and Endpoint Security Advisory Services • Managed Endpoint Threat Detection and Response • Managed Endpoint Protection • Managed Advanced Threat Protection • Managed Firewall • Managed Network IDS/IPS • Managed Proxy • Firewall Ruleset Assurance • Distributed Denial of Service Protection	• Effective protection, detection and response solutions with controls specific to their environment • Proven solutions to defend against breaches and data loss with agility and augmented resources to respond to inevitable attacks • Flexible delivery and capital expense/operating expense(CAPEX/OPEX) options
Security Advisory Services	• Cyber Maturity Review • Privileged Account Security Diagnostic • Advanced Compromise Assessment • Cyber Attack Simulation • Ransomware Diagnostic	• Help identify the overall security stage and plan according to business requirement • Conduct an effective organization wide assessment to identify the targeted attack • Help identify the security and control over the privileged account

8.5.2 Offeror must describe how it intends to comply with all applicable laws and related to data privacy and security.

DXC is a global organization that delivers solutions and services in multiple countries, states and industries, such as Healthcare, Fast-Moving Consumer Goods (FMCG), Banking, Financial Services and Insurance (BFSI), Manufacturing, and state government accounts. The DXC Global Privacy and Data Protection Policy helps users apply Privacy-by-Design principles in engineering and implementing systems and processes. The policy governs customer and employee data protection, and influences:

- System implementation standards
- Rulebooks
- Business processes
- Applications
- Web, product, and service developments
- Technology roadmaps

DXC will coordinate with the client to discuss and understand the data security and privacy requirements and will also make certain that DXC's approach is in line with the client domain, local governance policies, and global standards to achieve the desired results.

Applicable Laws

- Applicable laws relating to Privacy include the following:
- UK Data Protection Act (1998)





- US Privacy Act (1978)
- Graham-Leach-Bliley Act
- Health Insurance Portability and Accountability Act (HIPAA)
- German Data Protection Act
- UK Data Protection Act
- Indian IT Act 2008
- General Data Protection Regulation (GDPR)

8.5.3 Offeror must describe how it will not access a Purchasing Entity's user accounts or data, except in the course of data center operations, response to service or technical issues, as required by the express terms of the Master Agreement, the applicable Participating Addendum, and/or the applicable Service Level Agreement.

DXC understands the various requirements in handling and protecting private information and complying with legal and regulatory requirements. Our controls are designed to make certain that we have industry best standards in place to protect data. DXC follows appropriate measures to confirm compliance with current and future changes to international and national data protection and privacy laws.

DXC will safeguard, according to strict standards of security and confidentiality, any sensitive information, Non Public Information (NPI), Personally Identifiable Information (PII), Personally Identifiable Financial Information (PIFI) and Personally Identifiable Health Information (PIHI) that our clients, associates, vendors or other stakeholders share with us. In general all NPIs and client information is considered private information. Additional information and classifications will be obtained from the Purchasing Entity during the initial engagement and the control requirements will be documented as part of the Master Services Agreement (MSA) with the Purchasing Entity.

DXC will permit only authorized associates or contractors, who are trained in the proper handling of sensitive information, to have access to this information. DXC will not reveal such information to any external organization unless we inform the stakeholder in disclosures or agreements, receive authorization by the stakeholder, or are required by law or our regulators. DXC will limit the collection and use of such information to the minimum for delivering superior service to our clients. Access to this information shall be provided on a strict need-to-know basis. Associates or contractors who violate our Privacy Policy will be subject to our disciplinary process.

DXC will immediately inform all stake holders (includes Clients and law enforcement agencies) in case of any impact because of violation of Privacy Policy. DXC will conduct its business in a manner that fulfils this promise in the many nations in which we do business as well as complying with the applicable laws in the geographies that we operate.





8.6 Privacy and Security

8.6.1 Offeror must describe its commitment for its Solutions to comply with NIST, as defined in NIST Special Publication 800-145, and any other relevant industry standards, as it relates to the Scope of Services described in Attachment D, including supporting the different types of data that you may receive.

DXC governs its information security program using policies and standards designed to meet or exceed current industry standards, such as Information Systems Audit and Control Association (ISACA), National Institute of Standards and Technology (NIST), and the Center for Internet Security (CIS) and ISO/IEC 27001 and its predecessor, BS7799-2, as well as compliance with applicable laws.

DXC's Chief Information Security Officer (CISO) establishes these policies and standards. DXC complies with NIST Special Publication 800-145, a special publication that describes flexibility for cloud computing in service models SaaS, PaaS and IaaS and in the cloud-deployment mode (private, public and hybrid), and provides the data security and privacy for the stated services and deployment models.

DXC derives IT security policies and standards from formal risk assessments that analyze risk from a global (broad, general,) DXC perspective. IT security policies and standards will specify the minimum security controls that must be implemented based on the risk to the specific IT environment. DXC then monitors information security controls and continually adjusts them to account for varying security threats, vulnerabilities, and effect on the organization.

The DXC Information Security Policies and Standards govern systems use, electronic mail and messaging, networks, external systems and resources, and Internet use. Key components of the Information Security Policies and Standards include those on the following list.

- Human resources security
- Asset management
- Access control
- Cryptography
- Operations security
- Communications security
- Incident management
- Physical and environmental security

According to the guidelines of FIPS PUB 199, data has been defined in three different categories: Low, moderate, and high. All three categories are based on the loss of confidentiality, integrity, or availability. The DXC security team will take the input on the customer data and will classify the data based on the criticality of data and then implement the security policies based on those data classifications. For low severity data protection, we will use baseline solution such as anti-virus, data loss prevention (DLP), Firewall, Proxy, Email Security, and other traditional security solution based on the requirement. As the data criticality increases, we will implement advance threat protection, such as multifactor Authentication, identity and access management and DDOS. Once the data criticality reaches the maximum category, we implement the SIEM solution behavior monitoring and security monitoring, as well as and other solutions to protect the data.





8.6.2 Offeror must list all government or standards organization security certifications it currently holds that apply specifically to the Offeror's proposal, as well as those in process at time of response. Specifically include HIPAA, FERPA, CJIS Security Policy, PCI Data Security Standards (DSS), IRS Publication 1075, FISMA, NIST 800-53, NIST SP 800-171, and FIPS 200 if they apply.

DXC uses and continuously improves its global quality and security processes, promoting consistency of approach and the deployment of a standard global process set to all of our clients.

DXC's commitment to standards, models, and frameworks that began within EDS and CSC more than three decades ago with our first certification in ISO 9001 (Quality Management). Since then, certification programs have continued to expand and we have built an integrated management system that supports multiple standards, models, and frameworks including:

- ISO 9001 (Quality Management)
- ISO 14001 (Environmental Management)
- ISO 20000 (Service Management)
- ISO 22301 (Business Continuity Management)
- ISO 27001 (Information Security Management)
- CSA STAR (Cloud Certification)
- OHSAS 18001 (Health and Safety Management)
- ISO 50001 (Energy Management)
- SA 8000 (Social Accountability)
- TL 9001 (Quality Management in Telecom)
- ISO 13485 (Quality Management in Medical)
- BS 10012 (Personal Information Management)
- COBIT5
- CMMI-DEV CMMI-SVC
-

Industry specific compliance standards that DXC recognizes and to which we conform include: Sarbanes-Oxley (SOX)

- Health Insurance Portability and Accountability Act (HIPAA)
- Basel II
- Good Automated Manufacturing Practice (GAMP)
- Payment Card Industry Data Security Standard (PCI DSS)
-

DXC provides auditable security certifications— HIPAA, PCI, SOC2, FedRAMP, FIPS, and CJIS — that support regulatory compliance and data sovereignty. DXC makes certain that platforms and services meet ISO 27001, EU model clauses, HIPAA BAA, FISMA and FERPA requirements.

In addition to our certification and assurance strategy, we support client compliance and regulatory obligations by participating in client regulatory compliance programs for Sarbanes Oxley, HIPAA, Good X Practice (GxP), Gramm-Leach-Bliley Act (GLBA), and many others.

8.6.3 Offeror must describe its security practices in place to secure data and applications, including threats from outside the service center as well as other customers co-located within the same service center.





DXC Security Services maintains a comprehensive, detailed list of security requirements encompassing risk assessments, perimeter security, exterior and interior security, computer room security controls and access controls. We implement physical security controls based on the risks identified in the facility risk assessments. These controls include security guards, badge entry system, fencing, man traps, vehicle and pedestrian gate controls and closed-circuit television (CCTV) recording.

The DXC network is constructed with appropriate firewalls and access controls. DXC has an established global network connectivity program that provides the necessary authentication and authorization controls through our firewalls for access to any confidential data. DXC also uses automated auditing tools and scans to maintain application compliance.

The following diagram illustrates how segmentation is accomplished to block access among the compartments within a DXC Data Center:

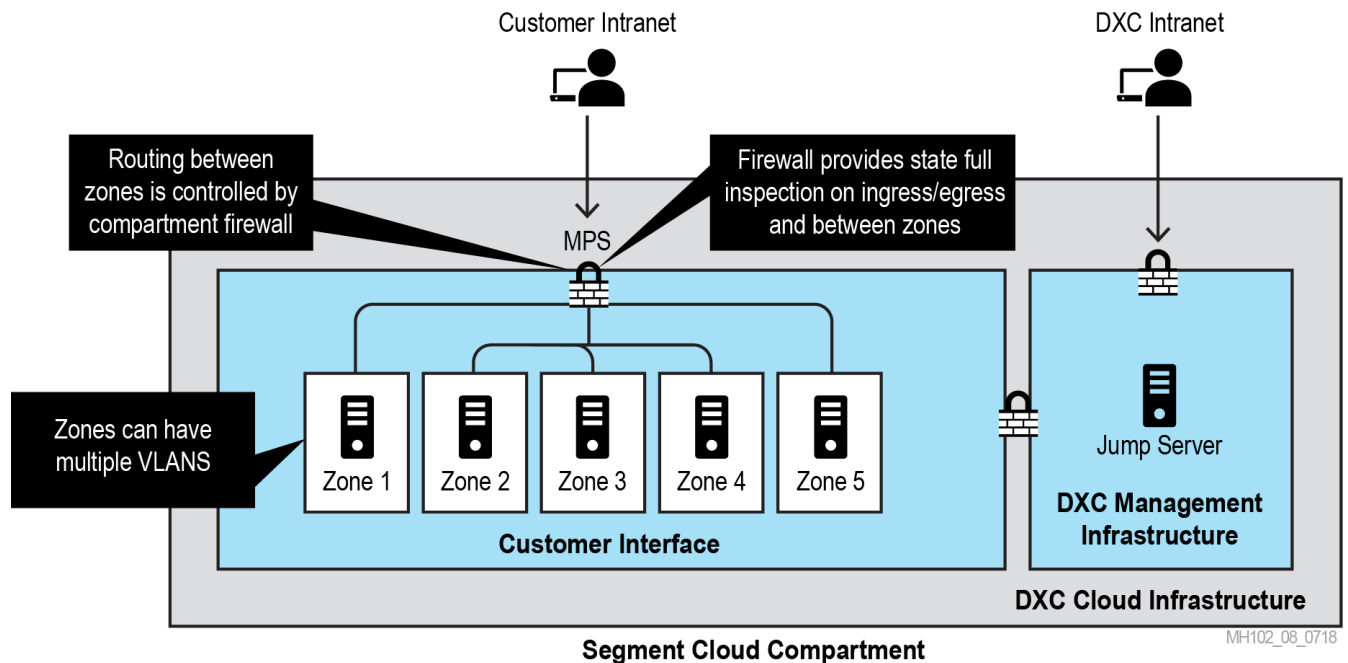


Figure 8: Segment Cloud Compartment within a DXC Data Center

DXC data protection and privacy services provide certified specialists with security and privacy expertise and experience to help you understand risks to business-critical data. First DXC pinpoints weaknesses, and then we help our client develop an enterprise-wide data protection and privacy strategy, build sophisticated data protection and privacy solutions, and maintain the enterprise's security environment. Our consultants deliver projects of all sizes, from advisory workshops, assessments and tactical deployments to enterprise-wide solutions with full turnkey architecture design and technology implementation. DXC services include:

- Advisory and planning services for the General Data Protection Regulation (GDPR) and other regulatory initiatives
- Data governance and classification
- Trust services (PKI, certificate and key management)
- Encryption solutions
- Rights management
- Data loss prevention





Applications Security Services

DXC's industry leadership in security services and solutions benefits our clients by addressing applications' security at the onset of the applications development lifecycle, in the requirements, architecture, and design stages and throughout the entire lifecycle.

DXC delivers the following services that enable our clients to understand the activities necessary to deliver cost-effective application security:

- Applications Security Advisory Service include consulting and diagnostics services to assess the maturity of the current applications security practices, and develop a strategy and roadmap to increase the security resilience of an organization.
- Comprehensive Applications Threat Analysis (CATA) uses a uniquely designed methodology and processes to conduct security requirements gap analysis and architectural design threat analysis.
- Applications Security on Demand delivers convenient, consumption-based applications security Testing as a Service (TaaS) to identify security defects and vulnerabilities in applications using industry-leading technology hosted in our secure DXC cloud.
- Enhanced Applications Security Testing applies comprehensive analysis of the application, including human expert code review to find potential vulnerabilities that can't be identified by automated testing alone.
- Vulnerability Remediation corrects the security defects and vulnerabilities found in applications through our testing and analysis services.
- DXC provides services for ongoing security and regression testing to reduce the risk that security vulnerabilities are introduced as part of break-fix or change requests.

DXC physical security requirements are based on a comprehensive risk assessment, analysis, and implementation of appropriate physical security operational controls based on the associated risks. These controls include guards, badge entry, fencing, barriers, electronic intrusion detection, gate controls and closed circuit television (CCTV) recording.

8.6.4 Offeror must describe its data confidentiality standards and practices that are in place to ensure data confidentiality. This must include not only prevention of exposure to unauthorized personnel, but also managing and reviewing access that administrators have to stored data. Include information on your hardware policies (laptops, mobile etc).

DXC requires the identification of all physical (hardware) and logical (software) IT assets used to manage DXC client, third-party, and internal information throughout their lifecycles, including creation, processing, storage, transmission, deletion, and destruction. They must also be protected, kept confidential, and used only for valid business purposes.

Information security management is of utmost importance to DXC. We take a controlling approach to continuously and effectively manage and improve our information security, including people, infrastructure, and business operations. Our information security risk management program helps reduce risks to manageable levels, based on the business goals and expectations of the contractual engagement. This program is anticipatory, identifying information security risks, establishing physical security, defining information security controls, and implementing risk treatment plans to reduce both inherent and residual risks.





DXC's information security program is governed by policies and standards established by the Chief Information Officer. Such policies and standards are designed to meet or exceed then-current industry standards as well as comply with applicable law.

Operating Systems

Servers in DXC data centers are continuously monitored. This includes operating system and patch level. DXC uses this information to make certain that operating systems and patches are current. DXC deploys encryption protection when warranted.

Network, Firewall and Infrastructure

The DXC network is constructed with appropriate firewalls and access controls. DXC has an established global network connectivity program that provides the necessary authentication and authorization controls through our firewalls for access to any confidential data. DXC also uses automated auditing tools and scans to maintain the application.

Data centers have additional security features and controls that require pre-approval of all people entering the centers. These include pre-approval, escorts, screening, and video coverage.

Each defined work space has separate access-control standards, such as data center, research and development, office space, and business center.

Physical Security

Security personnel guard and monitor the global delivery centers 24x7. Their roles and responsibilities include emergency response, incident reporting and management, investigation, patrolling, preventing unauthorized entry, and implementing loss-prevention programs.

DXC development centers, production floors, and data centers are highly restricted. Multiple levels of physical security controls protect these areas. Only authorized personnel have access to network equipment, computer equipment, storage media, and processing areas. Security card readers protect the doors leading into these areas and provide increasing levels of security and access by job function. Biometric controls can be implemented for facilities housing critical data.

Desktop Security Management

DXC's Consistent Office Environment (COE) is used on all systems connecting to the DXC network. Desktop security, such as patching, AntiVirus, VPN, password authentication etc., are managed through the COE function.

DXC's IT Infrastructure Operations manage desktop operating system patching. DXC has formal patch-management policies and standards, as well as change control policies that are strictly enforced.

Administrative Access Management

Powered by industry-leading technology and expert advisory and managed security services, Privileged Account Management protects organizations' most critical assets by securing, managing, and monitoring privileged accounts and access. This service also helps clients comply with regulatory mandates while lowering administrative costs, consistently defining and enforcing security policies, and effectively protecting their diverse environments. This helps client's gain control of their critical accounts, which leads to increased visibility, accountability, and efficiency, as highlighted in the list that follows.





- **Visibility** - Controls administrative access to a wide range of systems and infrastructures with a single, integrated solution.
- **Accountability** – Makes certain that the right people have access by eliminating anonymous use of credentials across the enterprise and tying people to their actions through auditable controls.
- **Efficiency** - Enforces password policies and provides secure, centralized, and automated password management for administrative, service, and application accounts.

Mobile Device and Authentication Management

With users numbering in the hundreds of millions worldwide, mobile solutions present unprecedented opportunities for increased convenience and accessibility. At the same time, mobile access has introduced new threats from identity theft and fraud as most transactions are conducted with no face-to-face customer contact. DXC provides enterprise-class mobile device management solutions and services to protect the customer identity and data residing on mobile devices by adding security controls, such as encryption, data wipe, password policy, and applications control.

DXC provides an enhanced customer experience solution for mobile user authentication by leveraging software from our partner, Daon's ConfidentialID. A biometric-enabled authentication software product for mobile devices, ConfidentialID uses an in- and out-of-band approach to protect customers from identify theft and fraud. ConfidentialID provides efficient, reliable identity authentication for mobile, online, and other transactions using a combination of passwords, PINs, biometrics and other techniques. The software employs dynamic security levels, allowing the client to customize the level of authentication based on a transaction's value and the client organization's risk management strategies. It can eliminate passwords to truly enhance the customer experience.

Environmental security

DXC has a Corporate Social Responsibility Policy. Global citizenship is one of the DXC corporate objectives that reflect the company's long-standing commitment to making a positive contribution to the global community. DXC is guided by its company values of trust, respect for the individual, and conducting its business with uncompromising integrity. These values are embodied worldwide in the company's Standards of Business Conduct and implemented through rigorous governance practices to make certain that business practices reflect DXC values.

As one of the world's largest providers of information technology (IT) infrastructure, software, services, and solutions, DXC is in a unique position to respond to the environmental challenges that we as individuals as well as enterprises face. To achieve this, we combine the expertise of our people, our innovative technology portfolio, and collaborative partnerships to create environmental solutions that reduce negative effects and expand opportunities for our business, our customers, and the world.

DXC's early environmental initiatives have evolved into a strategic, global effort to drive sustainable growth for our customers and our own business. Over the years we have continually strengthened our commitment to the environment and invested significant resources. Through these efforts, we are improving the efficiency of our portfolio, supply chain, and operations to reduce our environmental impact. At the same time, we are working to improve or replace current energy and resource-intensive processes and behaviors with more efficient alternatives—and help people rethink the ways they have traditionally lived and worked.





8.6.5 Offeror must provide a detailed list of the third-party attestations, reports, security credentials (e.g., FedRamp High, FedRamp Moderate, etc.), and certifications relating to data security, integrity, and other controls.

Global ISO Certifications have been established for ISO 9001, ISO 20000-1, and ISO 27001. These global accreditations for the respective ISO standards enable one certification across DXC facilities, rather than certifying individual sites. More than 400 sites have been certified under this program in one or more of these ISO standards. Every year, surveillance audits are carried out at a central location (Plano, TX) and at selected certified sites, based on the global sampling plans for each of the ISO standards that are in scope. British Standards Institution (BSI) is our registered certification provider. Our organization undergoes recertification every three years. Apart from cost savings, the global certification initiative has resulted in consistency and standardization in the use of terminologies, management system practices, and our internal and external communications.

International Standards for Assurance Engagements (ISAE 3402) is a global assurance standard for reporting on controls at service organizations. DXC has obtained multiple Service Organization Control (SOC1) reports for its data centers worldwide for ISAE 3402. DXC intends to obtain SOC2 reports for facilitating its Cloud Computing Services. DXC's IAAS and PaaS service model authorized by FedRAMP Moderate Level.

DXC conforms to the following Industry-specific compliance standards:

- Sarbanes-Oxley (SOX)
- Health Insurance Portability and Accountability Act (HIPAA)
- Basel II
- Good Automated Manufacturing Practice (GAMP)
- Payment Card Industry Data Security Standard (PCI DSS)

The Net Promoter Score (NPS), developed by Fred Reichheld, is a customer loyalty metric that measures the health of the relationship and the likelihood that a client will recommend a company to others. We use this methodology behind the metric to strengthen our company through positive customer experiences and word-of-mouth.

8.6.6 Offeror must describe its logging process including the types of services and devices logged; the event types logged; and the information fields. You should include detailed response on how you plan to maintain security certifications.

By policy, software must maintain an audit trail of security-related events, including startup/shutdown, account creation/modification/deletion, successful session establishment/termination, and unsuccessful attempts to access data. For network access logging, audit trails of security related operational events must be maintained, including successful and unsuccessful login attempts. For network events logging by policy, logs for the system components must be reviewed daily or with automated alerts as a part of continuous monitoring.

DXC considers it a critical obligation to protect DXC information, client information, and supporting technology assets and make certain they are used only for their intended business purposes. DXC has technical and procedural controls in place to protect its information assets from unauthorized access, destruction, modification and disclosure. But we cannot rely on technology alone.





As an organization, DXC makes certain that all employees are trained and, where required, certified to support applicable regulatory compliances and statutory requirements. To achieve this, DXC schedules regular mandatory training by domain experts, to transfer the knowledge to our employees.

All DXC employees are required to certify annually to the DXC Code of Business Conduct, which includes materials related to key regulatory and compliance topics that broadly affect all DXC staff.

8.6.7 Offeror must describe whether it can restrict visibility of cloud hosted data and documents to specific users or groups.

DXC can restrict visibility of Purchasing Entity cloud-hosted data to specific users and groups and this can be done between tenants and within a single tenant as well. Purchasing Entities gets the flexibility to control the level of access they have to resources while managing users and user permissions wherein each user can have unique security credentials, eliminating the need for shared passwords or keys, and supporting the security best practices of role separation and least privilege. DXC can guide entities in setting proper permissions to specify the users who have access to resources and the actions they can perform in those resources that supports hierarchical multi-tenancy, meaning that tenants are logically separated using firewalls and encryption to prevent access of one tenant's data or applications by any other tenant.

In addition, security whitepapers can be made available to purchasing entities to further illustrate these points or to establish transparency regarding the separation of responsibility between them for compliance programs such as HIPAA or PCI. Subscribers are able to use a VPN connection at multiple layers to maintain data security. For traffic in motion, VPNs can be created for a particular application and also for an entire virtual data center. A site-to-site IPsec-VPN can also be established to securely tunnel the entire virtual data center back to the private data center. For data "at rest", subscribers are provided a role based access control, whereby specified users are not exposed to the entire infrastructure and can be limited to a single or multiple virtual data centers.

Identity and Access Management – Preventing unauthorized access to information resources in the cloud is a major consideration for cloud consumers. One recurring issue is that the organizational identification and authentication framework may not naturally extend into the hybrid cloud environment.

DXC uses identity federation, which allows the Purchasing Entity and DXC to trust and share digital identities and attributes across both domains as well as provides a means for single sign-on. Clear separation of the managed identities of the Purchasing Entity from those of DXC is enforced to protect the Purchasing Entity's resources from DXC-authenticated entities as well as protect DXC-authenticated entities' resources from the Purchasing Entity. DXC manages this using the controls and processes on the list that follows.

- DXC administrative access
- Purchasing Entity administrative access
- Role-based access control
- Password controls
- User access authorization
- User access reviews
- User access revocation





- Accountability
- Multi-factor authentication on the Managed Services Portal

8.6.8 Offeror must describe its notification process in the event of a security incident, including relating to timing, incident levels. Offeror should take into consideration that Purchasing Entities may have different notification requirements based on applicable laws and the categorization type of the data being processed or stored.

DXC's policy is to report customer security incidents based on the requirements in the specific client contract, along with the relevant security incident or breach laws and regulations in cooperation with our client and law enforcement officials. DXC incorporates cross-functional, multidisciplinary escalation processes to manage security incidents. The timelines can be mutually agreed upon between client and DXC in due diligence or during contract negotiations.

DXC's post-breach review procedure includes the analysis of system weaknesses, procedure weaknesses, or both to make certain that appropriate remedial and longer-term root-cause elimination efforts are taken.

8.6.9 Offeror must describe and identify whether or not it has any security controls, both physical and virtual Zones of Control Architectures (ZOCA), used to isolate hosted servers.

By policy, internal spaces that are shared by third parties are required to implement physical controls to prevent unauthorized access to DXC spaces. DXC restricts access to virtual zones through client specific network access controls that isolate and restrict traffic between public or private IP ranges, or between specific servers. This includes firewall and port access rules which monitor critical perimeters with intrusion prevention technologies that are logged to SIEM.

8.6.10 Provide Security Technical Reference Architectures that support Infrastructure as a Service (IaaS), Software as a Service (SaaS) & Platform as a Service (PaaS).

DXC's security reference architecture, illustrated in the diagram below, is tailored according to the client's requirements, environment and scope:



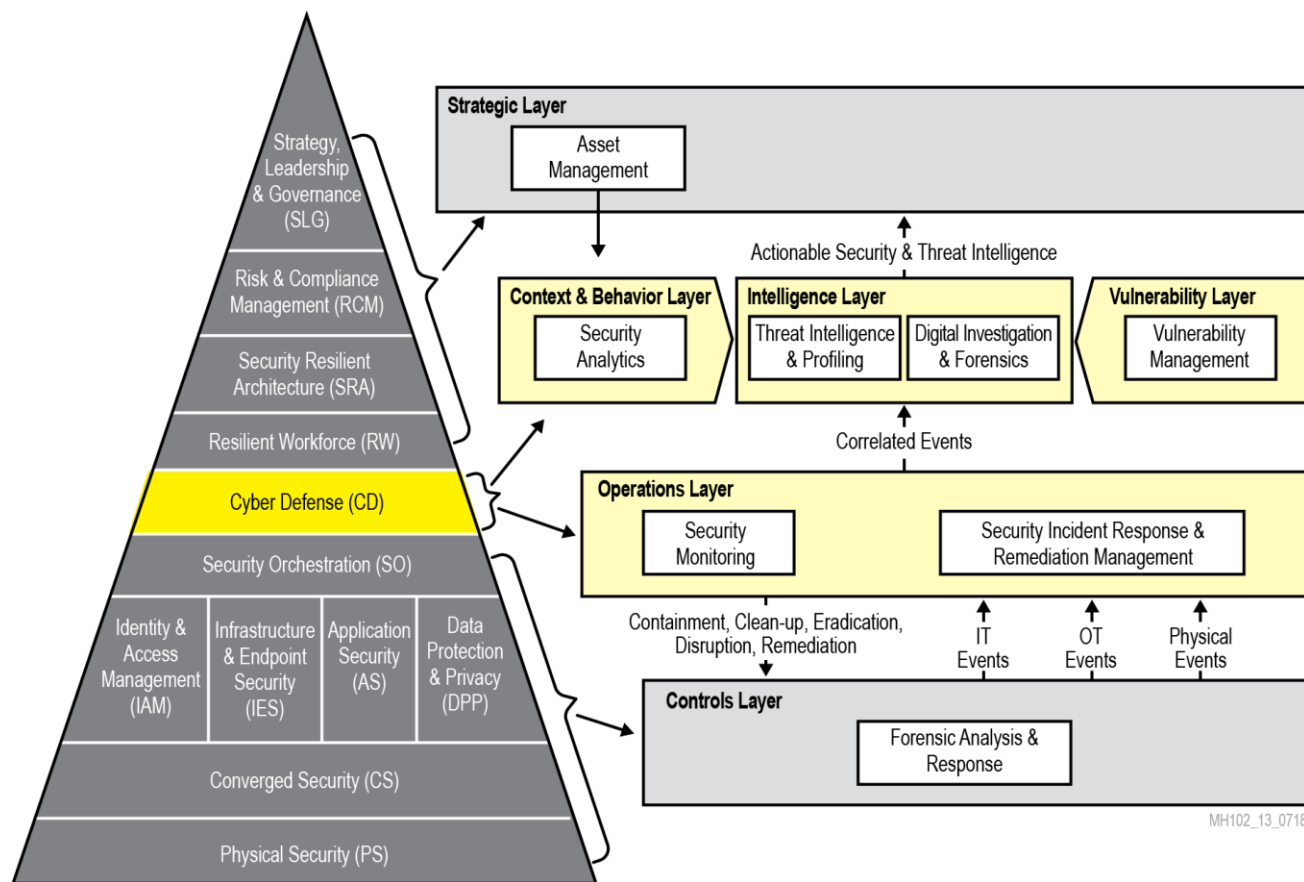


Figure 9: DXC's Security Reference Architecture

DXC has a layered approach for its security reference model which is applicable to Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS) environments.

DXC has segregated the security controls in six layers as depicted in this illustration. It provides a robust security resilience framework to detect, protect and respond to security threats and attacks, along with a continuous monitoring and threat hunting approach to respond proactively.

8.6.11 Describe security procedures (background checks, foot printing logging, etc.) which are in place regarding Offeror's employees who have access to sensitive data.

New DXC employees are required to complete a pre-employment background investigation. DXC standard pre-employment background checks will meet the following minimum criteria for all regular and part-time employees on DXC's payroll, where legally permissible and culturally acceptable.

- National identification check
- Five-year criminal check (felony and misdemeanor)
- Employment history - confirmation of last two jobs
- Education - confirmation of highest degree





For those employees working with more sensitive information or government contracts, more extensive background checks, security clearances, and/or drug screenings may apply.

Additionally, U.S. and Canadian customer-facing service employees are required to complete a multi-year criminal background investigation that includes county, state, provincial, and federal criminal records, as appropriate. This screening is recertified periodically.

DXC employees are expected to conduct business in a manner consistent with the DXC Standards of Business Conduct (SBC). The SBC integrates security into business processes and establishes security goals and objectives to support the organization and its customers. DXC employees are required to participate in the DXC Standards of Excellence training program. This program includes modules addressing data privacy and security. For those employees identified as having a role related to systems administration, information security, and/or application development, additional cyber security training courses are required. Annual refresher training keeps employees' knowledge up to date.

8.6.12 Describe the security measures and standards (i.e. NIST) which the Offeror has in place to secure the confidentiality of data at rest and in transit.

DXC requires the use of cryptography in transit and at rest as follows:

- In Transit – Cryptography must be used when sensitive information is transmitted over external, unsecured networks or wirelessly. This includes email, instant messaging and Web traffic. Sensitive information stored on portable or removable devices in transit between a DXC or supplier facility and another physical location must be encrypted.
- At Rest- Cryptography must be used when sensitive information is removed from secured DXC or DXC supplier facilities. This includes information stored on laptops, memory cards/sticks, flash drives, smart devices, CDs, DVDs and compact flash (CF) cards.

To maintain system interoperability and help preserve the availability of sensitive information assets, DXC implemented policies and standards to define the selection, use and parameterization of cryptographic algorithms and protocols. DXC uses industry-standard cryptographic and hashing algorithms, including:

- AES
- DES
- Two-Fish
- Blowfish
- RC4 (stream)
- SHA
- MD5
-

Unless prohibited by law, symmetric ciphers must have a minimal effective length of 112 bits, and all RSA ciphers used for authentication or digital signature must have a minimal effective length of 1024 bits.

8.6.13 Describe policies and procedures regarding notification to both the State and the Cardholders of a data breach, as defined in this RFP, and the mitigation of such a breach.





DXC maintains an incident-response plan for privacy related issues. While our internal programs for incident response are considered confidential, the following is a high-level overview of what they include.

Security incidents must be reported immediately to the DXC Security Incident Response Coordination Center (SIRCC). Security incidents are assessed by the DXC SIRCC and categorized in accordance with client approved Workflow. All instances of data breach are reported to DXC Security through a 24x7 online supported process and managed by the Corporate IT Security Incident Response Team (CITSIRT). DXC's Global Cyber Security then leads the incident investigation to determine if any unauthorized access has occurred. If such a breach is determined, the DXC Privacy Office and the Office of the General Counsel are consulted.

In accordance with DXC standards and policies, outsourcing client data breach incidents are handled in conjunction with the client's data breach response requirements as mutually agreed and documented per contractual obligations. DXC will incorporate the required policies to support the compliance requirements for notification of both the State and effected cardholders, in the case of a data breach. Our incident-response plan includes industry-wide best practices, knowledge of and adherence to applicable legal requirements in the event of data loss, and communication plans that focus on limiting risk exposure.

The DXC Privacy Team, along with other key organizations, handle corporate-level privacy related incidents. The team maintains a robust incident-response program that includes handling of sensitive data and data-loss procedures.





8.7 Migration and Redeployment Plan

8.7.1 Offeror must describe how it manages the end of life activities of closing down a service to a Purchasing Entity and safely deprovisioning it before the Offeror is no longer contractually obligated to maintain the service, include planned and unplanned activities. An Offeror's response should include detail on how an Offeror maintains security of the data during this phase of an SLA, if the Offeror provides for redundancy during migration, and how portable the data is during migration.

DXC has a long and successful record of performing efficient and effective transition-out services at end of contract or service termination. Our mature methodologies have been proven over numerous transition-out projects to actively engage with the client and, where applicable, the incoming service provider, in performing the migration, managing operations, and managing end-of-life activities to fulfill migration and redeployment responsibilities. DXC's Migration and Redeployment Plan minimizes risk through data security, data portability, and effective knowledge transfer. We deploy our mature tools, which include a comprehensive collection of processes, activities and checklists to facilitate plan execution.

End of Life

Activities to decommission an application (including data migration or archiving, application shutdown, server redeployment, or other activities deemed necessary to eliminate the billable components of an application) or to transition the support of the application because of insourcing or termination of a service, are categorized as end-of-life activities.

- **Migration** – As part of assessment and transition, we will provide knowledge transfer and access to data and documentation as defined the contract or provisioned through time and materials, enhancing receiving team readiness to support the client's in-scope applications portfolio.
- **Operations** – Leading up to migration and through to the final day of our contracted delivery term, or until each service is transitioned and cut-over to the future delivery entity (whichever comes first), we continue to deliver and manage the services in line with the SLAs.
- **End-of-life** – DXC requires at least 30 days' written notice to remove an application from Applications Management Services. Migration from DXC to new provider is generally the responsibility of the new provider; DXC facilitates migration with knowledge transfer and access to data and documentation as defined in the contract, or provisioned through time and materials.

Data Security

The security procedures and user/groups access rights defined by the account are still in effect while activities are in being executed during service termination. User/group access to the applications and data is terminated/revoked according to timeline of activities of a service termination plan (See section 8.7.2 below).

Data Portability

DXC works with the client and the incoming service provider to determine and execute, as applicable, the access to client's data for export and transfer to the designated future delivery platforms. This can include both logical and physical media access and data transfers, as best enables the efficient and secured delivery of the data.





Knowledge Transfer

DXC defines and executes a knowledge transfer approach for transitioning the service back to the client or new service provider. We monitor knowledge transfer and obtain sign-off to certify that it is complete. Our overall knowledge transfer approach typically includes classroom training, job shadowing, and remote knowledge transfer. DXC's knowledge transfer plan lists the activities necessary to transfer knowledge from the subject matter expert (SME) to the recipient for each area. It includes current and target proficiency levels for each activity. The SME/recipient/domain lead assess the target proficiency level.

Tools

DXC's Technology Separation Checklist is a list of technology elements that should be considered as part of a separation. DXC also uses a Transition Deliverables Responsibility Matrix to identify, document, and monitor performance of our organization's and the UNHCR time-bound contractual obligations and commitments. The matrix includes the relevant contract references, the dates by which delivery/achievement is required, overall responsibility for completion, and the current status on progress toward timely performance.

We use Transfer Readiness Criteria and map a number of specific and agreed-upon deliverables against each criterion. These deliverables provide the proof that the readiness criteria have been achieved. At transfer readiness review meetings this file is reviewed with UNHCR and the outsourcer.

Other Transition Elements

As part of our Migration and Redeployment Plan, DXC will conduct activities related to a number of other transition elements. Examples of these follow.

- **Manage people and communications** – DXC will transfer in-scope employees out of the terminated service unit
- **Manage communications** – DXC will manage the communications to employees, staff, the client, and vendors regarding the termination of a service
- **Implement financial updates** – DXC will provide new or amended financial forecasts, plans, and reports to reflect the effect of the terminated service.

Data Redundancy

Data redundancy is also integrated in the data migration plan. Back-ups of the data are created by the business continuity process agreed between DXC and the client as part of the support services. The back-up data are, in agreement with the client, transferred or destroyed upon completion of the migration of the product or latest data to the incoming service provider or back to the Purchasing entity.

8.7.2 Offeror must describe how it intends to provide an orderly return of data back to the Purchasing Entity, include any description in your SLA that describes the return of data to a customer.

DXC will make sure that Purchasing Entities' data is securely returned as part of the process of services termination defined in the previous section. As part of the termination, DXC will plan, execute, and close, performing the activities on the following list.

- **Plan** – identify the data to be returned and define data format (i.e., physical format or access rights on the cloud). This includes the controlled removal of DXC access to the data and handoff to the Purchasing Entity





- **Execute** – implement the agreed handover activities related to the data transfer
- **Close** – perform tasks to review and make certain that the data transferred is complete, and that access is now with the Purchasing Entity; verify that sign-off documents are signed by the Purchasing Entity to acknowledge the transfer completion

8.8 Service or Data Recovery

8.8.1 *Describe how you would respond to the following situations; include any contingency plan or policy.*

a. Extended downtime.

Extended downtime is an extremely rare situation because of the robust operational processes and redundancy measures that are embedded in our offerings and services. DXC, in such cases, communicates to the client through ITIL-based escalation processes. Issue escalation includes proper identification of escalation time frames, paths, procedures, and contacts. We base incident level 1 through 5 assignment on priority, with 1 being the highest priority, and we align resources to address incidents accordingly. Customer representatives receive frequent updates and are included in discussions of options and resolution plans as appropriate and necessary.

Extended downtime situations are closely tied to disaster recovery and business continuity plans. In the event that a disaster is declared, we follow tested procedures for orderly failover and preparation for resumption of operations at the alternate target site. As part of shutdown, we activate operations at the alternate site, which supports operations until resumption at the primary site.

b. Suffers an unrecoverable loss of data

DXC works with every client to be sure that the client's data is fully protected against corruption or loss using technologies such as data backup, cloning, replication, offsite retention using tape/cloud. Depending on the chosen technology, recovery point objective (RPO) and recovery time objective (RTO) vary. By making the solution redundant at various levels, we can prevent unrecoverable loss of data. Depending on the specific service in question and the applicable data loss prevention measures that are employed, data durability for the catalog of proposed services can be as high as 16-nines, i.e., 99.99999999999999%. As a result, most true data losses are the result of human error or application software bugs.

In the rare event that data is irretrievably lost despite the data-loss-prevention measures that are in place, DXC works with the client to restore the system to the most recent known valid recovery point, which is typically no earlier than the RPO defined in the applicable SLA.

c. Offeror experiences a system failure.

DXC uses a combination of reactive and preemptive measures to handle a system failure. Both are described in the subsections that follow.





Reactive measures

DXC uses the Incident Management process to manage IT service disruptions such as those resulting from system failures, and to restore normal service operation as quickly as possible. The overall goal is to minimize adverse effects on the client's business operations.

Incident Management includes the following seven sub processes:

- Incident Identification
- Incident Logging, Categorization, and Prioritization
- Incident Diagnosis
- Investigation and Diagnosis
- Resolution and Recovery
- Management Review
- Incident Closure

The first step in Incident Management is acknowledging and accepting ownership of the incident, then documenting critical information in the incident tracking tool. Conducting an initial investigation validates and classifies the incident, determines the level of priority, and assigns it to the appropriate support team for resolution.

After an initial diagnosis, incidents associated with known errors are quickly resolved by applying approved solutions or workarounds. Incidents associated with an existing or parent incident that has not yet been resolved are assigned to the technical support team already working on that incident's resolution. Technical support teams perform additional diagnostics, as necessary, to identify and implement an appropriate solution or workaround. Finally, the affected users verify and confirm the solution or workaround.

While an incident remains open, the service desk function within ITIL monitors and reviews incident status, communicates to affected users, and updates incident records as necessary. Based on severity, we manage the defined escalation procedures to facilitate resolution by establishing bridge lines with our technical support team; alliance partners and vendors; Participating Entity technical support teams; and Participating Entity/DXC business leaders. The focus of Incident Management is restoration of normal service operations as quickly as possible, minimizing adverse effects on the business and users.

Preemptive measures

The contingency plan that DXC offers the client to recover from a system failure is replicating data and operating systems on storage devices in a DXC Recovery Center. Clients can enable the plans on the following list to prevent a system failure.

- Host-based (software) asynchronous replication
- Replicating local and array-based storage (storage vendor agnostic)
- Replicating both data and operating systems simultaneously, to be sure that both the operating system and the application context are copied

The DXC Continuity Services Recovery Center has a cloud server infrastructure that can offer the client the capabilities on the following list.

- The storage capacity is dedicated to that customer (but hosted on a shared array)
- Server blades running as VMware ESX clusters provide the compute capability for customers
Customers can invoke or rehearse
All compute capability is provided as virtual servers





DXC can include comprehensive tools and processes that perform the functions noted in the list that follows.

- Support recovery processes and invocations
- Support noninvasive rehearsals
- Support fallback to the original environment

d. Ability to recover and restore data within 4 business hours in the event of a severe system outage.

Managed Continuity Service *powered by* Microsoft provides data-replication-based Disaster Recovery services for customers looking for a service to recover their traditional IT or cloud environment to a cloud-based environment. It is a cost-effective cloud solution that provides disaster recovery using a shared infrastructure, also known as Cloud Disaster Recovery or Cloud DR. The service allows recovery of a customer's infrastructure environment (for infrastructures of up to 200 systems) within four to six hours following a major IT interruption (when recovering to latest replication time) while relying on the service's data replication feature to typically achieve a recovery point objective that represents no more than 15 minutes of data loss.

Depending on the complexity of the customer's environment, additional steps may be required to restore full functioning, such as redirection of network circuits for user connectivity, enablement of applications and other factors required to provide user logon. The time to complete these additional steps must be considered when calculating the recovery time objective (RTO).

The customer has the option to choose to recover servers to a point in time (recovery tag), representing a system and data state that is different from at the time of failure. This option allows recovery from a data-corruption event by restoring data to a time before the corruption occurred. Note that this recovery option will require additional time.

Additionally, the Managed Continuity Service powered by Microsoft provides for testing the customer's recovery environment with a minimum of 14 days' notice, which is a significantly shorter notification period than normally experienced with traditional DR services.

DXC's standard recovery targets are noted in the following list.

- Target RPO < 15 minutes.
- Target RTO: typically 4 to 6 hours for environments of 200 servers (150 physical servers, 75 TB storage), using "latest time" option for data recovery. Larger environments could take significantly longer and require prioritizing the servers being recovered.

e. Describe your Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

Managed Continuity Service powered by Microsoft offers flexible and highly cost effective Recovery-as-a-Service that offers a broad range of tiered services for resumption of normal business processes, allowing DXC to tailor the service to be commensurate with the criticality of each client application or system environment. The table that follows outlines a range of RTO/RPO SLAs that is supported by DXC, depending on the type of service and associated continuity technologies being contracted by the Participating Entity.





RTO/RPO Service Levels

Capability	RPO	RTO	Price	Comments
Data Center Recovery Services (core) Customer backup tapes recovering onto leveraged DXC servers (Infrastructure Avail in 24 Hours)	Up to 24 hours	36-72 hours	x1	If equipment in center, systems available immediately
Data Center Recovery Services (critical) Customer backup tapes recovering onto leveraged DXC servers (Infrastructure Avail in 7 Hours)	Up to 24 hours	12-48 hours	x1.2	If equipment in center, systems available immediately
Managed Continuity Services (powered by Microsoft) Cloud solution with dedicated storage and leveraged servers (Infrastructure Avail in 4 Hours)	Up to 15 minutes	Up to 4 hours	x1.6	Linux / Windows
Managed Resiliency Services (leveraged servers) Dedicated storage service recovering onto leveraged servers (Depends on which Core/Critical)	1-30 minutes	1-12 hours	x2.5	Same storage infrastructure on both sites

DXC's Recovery Point Objective (RPO) solution is designed to contain data loss to 15 minutes or less. Depending on available bandwidth, amount of data queueing and other factors external to DXC's hosted recovery environment, the RPO could exceed 15 minutes of transactional data loss. In addition, use of the Continuous Data Protection (CDP) option to select earlier recovery points will affect the achievable RTO.

8.8.2 Describe your methodologies for the following backup and restore services:

The following subsections describe DXCs methodologies for data backups, server image backups, digital location of backup storage, and alternate data center strategies for primary data centers.

a. Method of data backups

DXC Backup as a Service (BUaaS) provides a cost-effective managed service for backup and recovery of all types of data. The Participating Entity chooses whether the data is hosted in their data centers and remote offices, DXC datacenters, or public cloud environments. DXC then manages the purchase, configuration, protection, and management of the backup data aligned to the business impact of the data. Service options include high-performance backup and rapid recovery for critical workloads. We leverage data deduplication technology to optimize performance and cost and to segregate extended retention data to object store for further cost reduction.

Regardless of the type or location of a Purchasing Entity's data assets, DXC BUaaS protects and recovers data where it is needed while observing national data sovereignty rules with locally deployed assets and in-country support. Purchasing Entity may choose offshore support options for data not affected by data sovereignty rules.

DXC BUaaS provides a reliable, managed and centralized backup solution for your corporate data and requires minimal infrastructure buildout. Service options include:

- Operational backup with next generation data protection storage
- Offsite replication
- Remote office protection
- Support for industry-leading private, hybrid and public cloud storage
- APIs for integration and automation





The following DXC BUaaS list includes two primary offerings and one sub-offering.

- Standard Data Protection
- Extended Data Protection
- Cloud Data Protection

BUaaS – Standard Data Protection provides general data protection to private-hosted environments for unstructured and structured data assets. It delivers a reliable managed data protection service and managed backup infrastructure storage services along with options including replication, remote site data protection, long term retention, and encryption of backup data at rest and in motion. BUaaS Standard Data Protection is targeted to deliver reliable and efficient operational backup and restore services for hosted environments located in DXC data centers and client on-premise data centers.

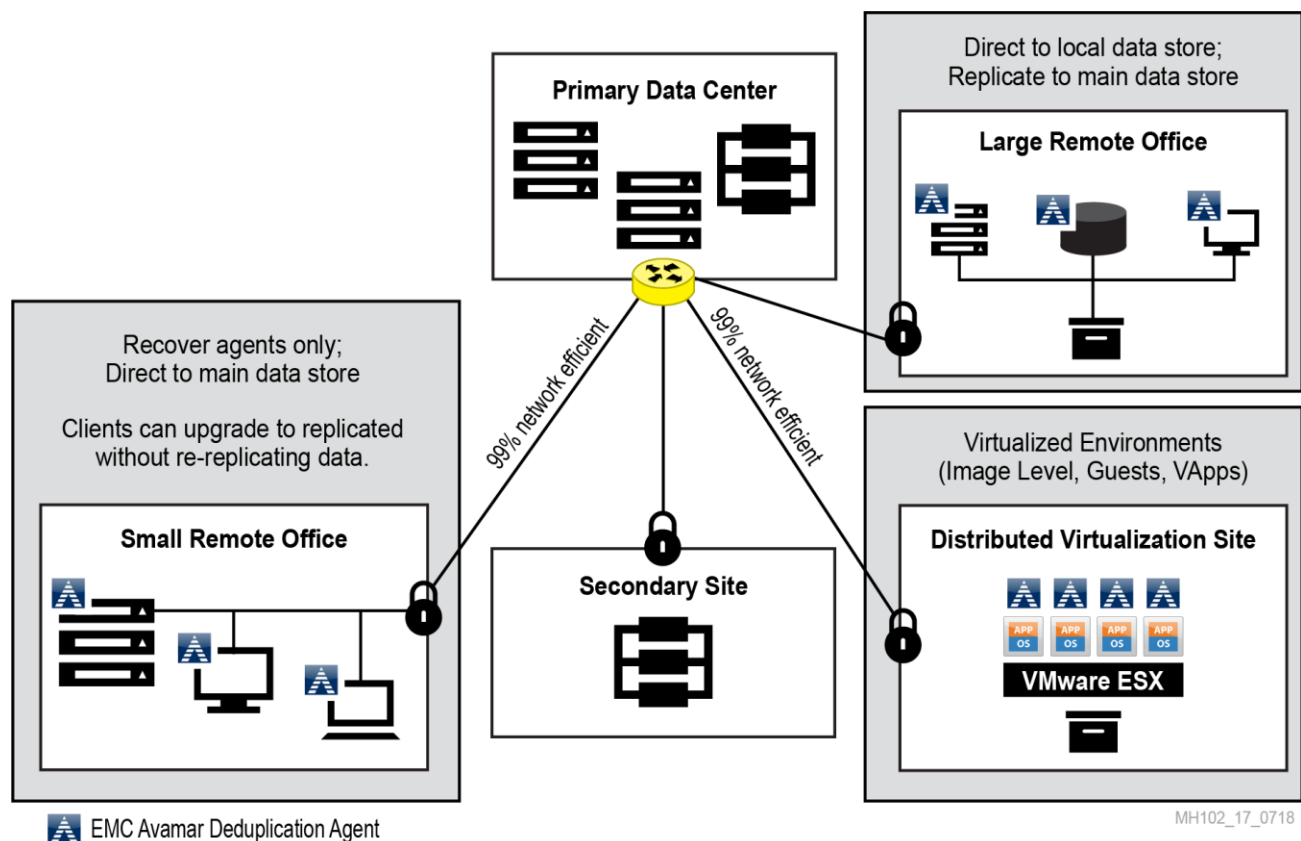


Figure 10: BUaaS Standard Data Protection deployment options

BUaaS Standard Data Protection provides a managed data protection service and managed backup infrastructure storage services along with options that include replication, remote site data protection, long term retention, and encryption of backup data at rest and in motion.

This offering is provided as either a shared or a dedicated service. The dedicated infrastructure can be hosted in either a Purchasing Entity data center or a DXC data center.

The service is offered using a leading and established data protection portfolio from vendors such as Dell EMC and Veritas. DXC leverages its partnership with these vendors to provide services that bring out the best of these technologies for customers to meet their data protection requirements.





BUaaS is primarily a disk based backup and recovery service with options to store data on tape or to object storage for longer retention to meet a customer's compliance and regulatory requirements.

BUaaS – Extended Retention is a sub-offering of BUaaS Standard data Protection, which provides solutions for clients' long-term retention requirements. This sub offering uses object storage to store data for long term retention. The object storage can be hosted in a DXC or a Participating Entity data center. It can also be provisioned on object storage solutions on public cloud vendors such as AWS. The service is offered using products from vendors such as Dell EMC (Elastic Cloud Storage) and AWS (S3). DXC leverages its partnerships with these vendors to provide services that bring out the best of these technologies for our clients to meet their Extended Retention requirements.

The BUaaS Extended Retention offering uses data protection optimization options such as compression and deduplication. The service can store reduplicated back up data in on-premises object storage or public cloud object storage. The offering allows data to be natively tiered to object storage without the need to setup cloud gateways. This offering also provides security options such as encryption for clients sensitive to data security and to meet industry standards to secure backup data.

BUaaS Cloud Data Protection provides a Public-Cloud-based Backup and Restore service as well as further options as defined in the Offering Description. BUaaS Cloud Data Protection is based on Dell EMC data protection product portfolio using NetWorker, CloudBoost and S3 object storage (AWS). It is offered mainly to customers who have elected a Public Cloud BUaaS Data Protection Solution.

BUaaS Cloud Data Protection is primarily a cloud based backup and recovery service with options to store data onto object storage for longer retention to meet clients' compliance and regulatory requirements. The offering uses data protection optimization options including deduplication, capacity and availability management, security, data Integrity, performance, and scalability and manageability to meet the backup window requirements. The service can also back up data on-premises, using Internet for Cloud Object Storage. Additionally, the offering can be used to backup data on disk-based devices on-premises or on cloud object retention to accommodate customers' distributed data complexity.

BUaaS Cloud Data Protection uses NetWorker with CloudBoost using AWS S3 (Object Storage) technologies to protect backup data for a client, and has the characteristics on the following list.

- Deployed with NetWorker, CloudBoost and installed automatically as part of NetWorker client package
- Performs backup data compression, deduplication and encryption at the point in the data flow
- AWS cross region replication is optional
- Extends retention to Public cloud object storage (AWS)
- Supports backup types: File backup, database, application
- Supports Client Direct features for Linux
- Creates CloudBoost metadata, which is sent to the CloudBoost appliance
- CloudBoost Appliance will have its own dedicated Object Storage bucket





The following figure is a conceptual view of BUaaS CloudData Protection.

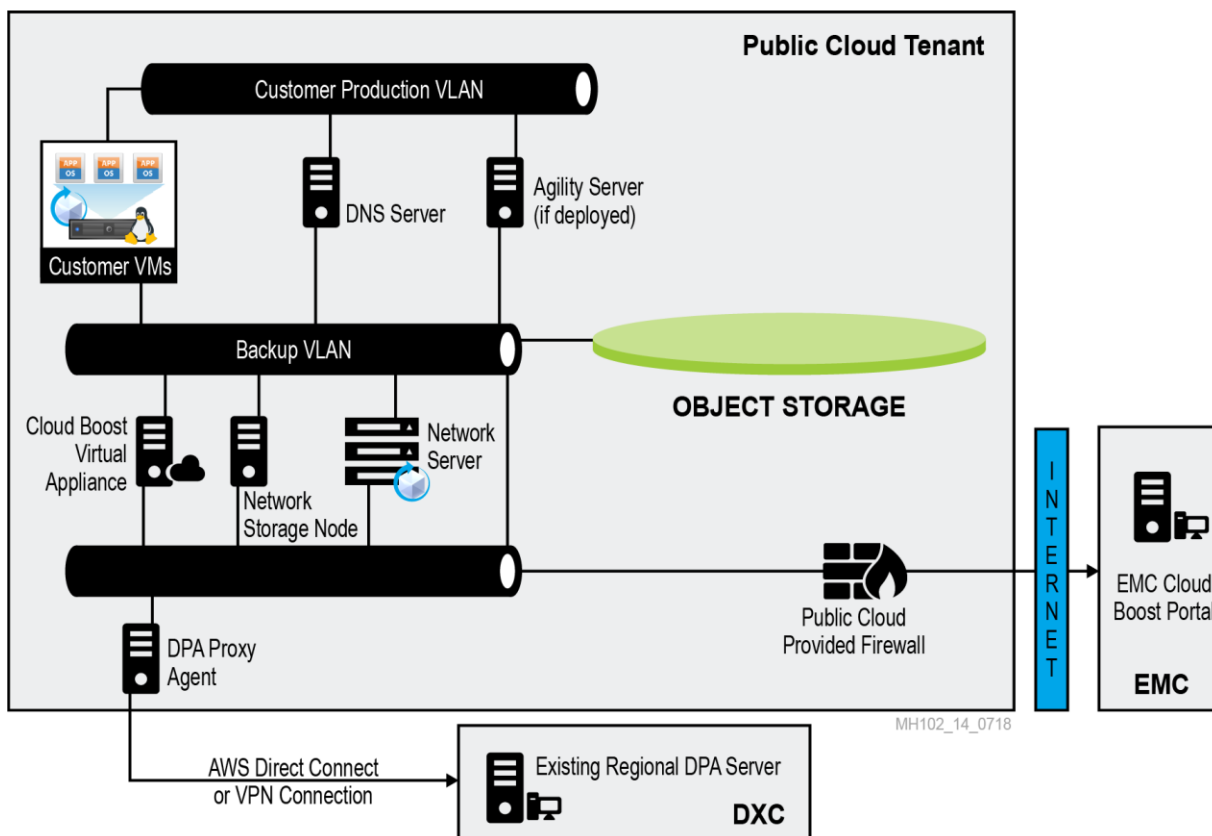


Figure 11: BUaaS Cloud Data Protection conceptual view

b. Method of server image backups

DXC Backup as a Service (BUaaS) offerings support the following three functional approaches for backups

- Snapshot backup, sometimes called image level backup, is a point in time copy of the host that preserves the state of data at an instant in time, by storing only those blocks that are different from an already existing full copy of the data. After the initial full copy is taken, there is no dependency on the original data.
 - Data can be complete machine images, LUNS or file systems but not individual files.
 - Enables easier and faster full VM recovery than an agent based backup approach
 - The level and ease of use for file level recovery is very dependent on the hypervisor, with VMware being the simplest to recover, most advanced and functionally rich.
- File level backup, which is Agent based and backs up the files and folders specified
 - Does not enable easy full VM or physical host recovery, you need to rebuild the host and then restore the data from backup
 - Ideal for file servers where file level restore is a common requirement





- Application or Database integrated backup,
 - Agent based, which integrates into the application or database to give advanced granular recovery options
 - Usually used in conjunction with file level backup

BUaaS can be used to configure any of the backup types discussed above to an expansive list of supported platforms and databases.

c. Digital location of backup storage (secondary storage, tape, etc.)

Digital location of backup storage, as described below, can involve replication to a secondary data center, backup to tape, extended online retention, or extended retention using ECS storage.

Replication of Your Backup Data to a Secondary Data Center Option

We will provide this option for replicating the client's backup data to a secondary data center only if specified by the client in the Transaction Document. If the client elects to purchase the option for replicating the client's backup data to a secondary data center, the backup data stored in the primary data center will be replicated to a secondary data center identified in the Transaction Document. Replication will occur asynchronously, where the backup data is transferred at point in time, as part of a schedule, after the backup completes.

Backup to Tape Option

Backup to tape means a proportion of client's backup data, elected by the client, is additionally committed to tape media monthly using standard Linear Tape-Open (LTO) tape drives. This option is inclusive of the tape drive use, but excludes the provision of LTO tape media. This option is not available in all installation locations. Unless the client elects to order the tape management service, the tapes used for backup to tape will be made available to the client for collection at the installation location during the next working day after the backup is taken, and the client must collect the tapes within one working day.

Extended Online Retention

Under this option client may nominate a certain image or group of images within the backup data to be retained for an extended time period of up to 370 days, using online disk storage only. The nomination of images for extended retention under this option is performed using the Service Request process. Use of this option will increase the volume of consumed storage. Selecting the backup storage and/or replication target options, means it is solely the client's responsibility to implement and manage the data retention policy, manual backup, and recovery tasks and to make sure that adequate backup storage and/or replication target is ordered to meet the requirement of that policy.

Extended Retention (ECS Storage)

BUaaS uses one of the Backup software platforms, EMC NetWorker or Veritas NetBackup or Avamar with EMC Data Domain (DD) to store the backup data. Extended retention provides an internal tiering approach that enables cost-effective, long-term retention of backup data on a DD system. The internal two-tiered file system of a DD Extended Retention-enabled DD system consists of an active tier and a retention tier.

Cloud Tier feature of DD enables moving inactive data from an active tier of a DD system to a low-cost and a high-capacity object storage such as a public, private, or hybrid cloud.





Conceptually, the cloud storage is treated as an additional storage tier (DD Cloud Tier) attached to the DD system, and data is moved between tiers as needed.

d. Alternate data center strategies for primary data centers within the continental United States.

DXC offers numerous options for Purchasing Entities seeking alternate or secondary data center target locations in the continental U.S. for securing backup data sourced from their primary data centers also located in the U.S. Within the continental United States, DXC has 10 leveraged data centers that Purchasing Entities can use to support either primary or secondary hosting and/or backup target site operations. Similarly, each of these U.S.-based data centers could also be configured as the target backup site for backup data originating from a Purchasing Entity's own on-premise data center.

In addition to leveraging DXC data centers as backup target sites, Purchasing Entities can also leverage DXC's BUaaS Extended Data Protection and BUaaS Cloud Data Protection offerings to seamlessly integrate public cloud storage as alternate targets for their backup data, by selecting one or more AWS Regions located in the continental U.S. as their BUaaS target sites.

In the USA, Participating Entities can take advantage of DXC Cloud Recovery instances in our Continuity Services Recovery Centers located in Alpharetta, Georgia; Colorado Springs, Colorado; and Littleton, Massachusetts.

Some of the benefits of the Continuity Services offering are listed below:

- Minimized business interruption and downtime -Limit number of clients on same HW platform/geographic region
- Delivery model-Continuity options aligned to business criticality of workloads
- Billing - As-a-Service pricing achieving 15% ~ 40% cost reduction over an equivalent in-house solution
- Security features, audit compliance, and risk management
- Support for compliance with industry regulations (ISO frameworks. SOC2, and IL3)
- Advisory and Continuity Program Management services
- Advisory services offered to create, validate, audit, run continuity plans





8.9 Data Protection

8.9.1 Specify standard encryption technologies and options to protect sensitive data, depending on the particular service model that you intend to provide under this Master Agreement, while in transit or at rest.

DXC will protect data in select cloud applications with gateway encryption or tokenization solutions offered in conjunction with Managed Cloud Gateway Solutions

DXC's security approach spans across all layers of the cloud stack, ranging from physical security to application security. The solution leverages current industry practices, including the National Institute of Standards and Technology (NIST).

Security and Privacy Requirements for Cloud Services

Item	Description
• Personnel requirements, including clearances roles, and responsibilities • Regulatory requirements • Service availability • Problem reporting review and resolution • Information handling and disclosure • Physical and logical access control • Incident reporting, handling and response • Assurance levels	• Data protection • System configuration and patch management • Backup and recovery • Data retention and sanitization • Security and vulnerability scanning • Risk management • Continuity of operations • Certification and accreditation • Independent auditing of services

Specific to the public cloud offerings in our proposed services catalog, DXC supports the encryption features described below for our Microsoft Azure, AWS, and Oracle partners.

Azure encryption

Azure supports various encryption models, including server-side encryption that uses service-managed keys, customer-managed keys in Key Vault, or customer-managed keys on customer-controlled hardware. With client-side encryption, a Purchasing Entity can manage and store keys on-premises or in another secure location.

Client-side encryption

Client-side encryption is performed outside of Azure. It includes two types of encrypted data.

- Data encrypted by an application that is running in the customer's data center or by a service application
- Data that is already encrypted when Azure receives it.

With client-side encryption, cloud service providers don't have access to the encryption keys and cannot decrypt this data. You maintain complete control of the keys.





Server-side encryption

The three server-side encryption models in the following list offer different key management characteristics, which you can choose according to your requirements:

- Service-managed keys: Provide a combination of control and convenience with low overhead.
- Customer-managed keys: Give the Purchasing Entity control over the keys, including Bring Your Own Keys (BYOK) support, or allows the Purchasing Entity to generate new ones.
- Service-managed keys in customer-controlled hardware: Enable the Purchasing Entity to manage keys in a proprietary repository, outside of Microsoft control, a concept called Host Your Own Key (HYOK) that involves a complex configuration and a model that most Azure services don't support.

Azure disk encryption

Purchasing Entities can protect Windows and Linux virtual machines using Azure disk encryption, which uses Windows BitLocker technology and Linux DM-Crypt to protect both operating system disks and data disks with full volume encryption. Encryption keys and secrets are safeguarded in the Purchasing Entity's Azure Key Vault subscription. By using the Azure Backup service, a Purchasing Entity can back up and restore encrypted Virtual Machines (VMs) that use Key Encryption Key (KEK) configuration.

Azure Storage Service Encryption

Data at rest in Azure Blob storage and Azure file shares can be encrypted in both server-side and client-side scenarios.

Azure Storage Service Encryption (SSE) can automatically encrypt data before it is stored, and it automatically decrypts the data when the Purchasing Entity retrieves it. The process is completely transparent to users. SSE uses 256-bit Advanced Encryption Standard (AES) encryption, which is one of the strongest block ciphers available. AES handles encryption, decryption, and key management transparently.

AWS Cloud encryption

AWS Cloud encryption includes security groups, network access-control lists, data security (optional), data at rest, and data in transit.

Security Groups

AWS Security Groups will be used to act as a virtual firewall for an instance (e.g., EC2, RDS, and Redshift). Inbound traffic is denied by default. Security Groups will be configured to only allow the traffic required for the instance. Source and destination objects, along with protocol and ports, will be used in Security Groups' rulesets to provide the minimal access required for the instance to operate.

Network Access-control Lists (NACLs)

AWS NACLs act as a virtual firewall at the network layer to control traffic into and out of a subnet. NACLs are stateless, permitting both allow and deny rules. NACLs will be created for each VPC and for each subnet. NACLs will be configured with 'ALLOW ALL' rules, unless a specific requirement to restrict access to a VPC or subnet exists that cannot be achieved by means of Security Groups.





Data Security (Optional)

A Purchasing Entity will have (at an additional cost) the option to encrypt data at rest. If this option is applicable, the AWS Key Management Service (KMS) will be used to create and control the encryption keys used to encrypt data at rest. Any requirement to encrypt data in transit will use SSL or a VPN-based solution.

Data at Rest

Data at rest will use encryption keys managed by the AWS Key Management Service (KMS). Keys will be automatically rotated (by AWS) annually. Unused keys incur a charge, so unused keys will be deleted periodically. Up to 1000 customer master keys can be created for each account for each region. The limit increase for customer master keys can be done through the AWS Support center.

Note: KMS will not be used for encryption in AMIs.

Data in Transit

A solution will be defined on a client-by-client basis. The following list of best practices recommended by AWS to protect data in transit would be applicable.

- SSL-enabled AWS APIs are used appropriately
- SSL or equivalent is used for communication
- Solution is VPN based
- Private connectivity (e.g., AWS Direct Connect) is used
- AWS Marketplace solution is being used

Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). Purchasing Entities can protect data in transit using SSL or client-side encryption. Purchasing Entities have the three mutually exclusive options on the following list for protecting data at rest in Amazon S3, depending on how the Purchasing Entity chooses to manage the encryption keys.

1. Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3) – Each object is encrypted with a unique key employing strong multi-factor encryption. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data. For more information, see Protecting Data Using Server-Side Encryption with Amazon S3-Managed Encryption Keys (SSE-S3).
2. Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS) – Similar to SSE-S3, but with some additional benefits along with some additional charges for using this service. There are separate permissions for using an envelope key (a key that protects your data's encryption key) that provides added protection against unauthorized access of the Purchasing Entity's objects in S3. SSE-KMS also provides the Purchasing Entity with an audit trail of when the Purchasing Entity's key was used and by whom. Additionally, the Purchasing Entity has the option to create and manage encryption keys itself, or use a default key that is unique to the Purchasing Entity, the service it is using, and the region in which it is working.
3. Use Server-Side Encryption with Customer-Provided Keys (SSE-C) – Purchasing Entities manage the encryption keys and Amazon S3 manages the encryption as it writes to disks, and decryption, at the time the Purchasing Entity accesses its objects.





Oracle Cloud Encryption

Oracle's mission is to bring its leading enterprise technology and business applications software to customers anywhere in the world through the Internet. Oracle Cloud is a broad set of industry-standards-based, integrated services that provides customers with subscription-based access to Oracle platform services, application services, and social services, all completely managed, hosted, and supported by Oracle. The technology includes robust, layered defenses that span IaaS, PaaS, and SaaS, extending security to the network, hardware, chip, operating system, storage, and application layers, bolstered by new security cloud services.

Purchasing Entity data is secured with Transparent Data Encryption (TDE), encryption at rest, and an isolated Virtual Cloud Network the Purchasing Entity has the option to control. Control access and security uses the same database policies in the cloud as in the Purchasing Entity's own data center. TDE prevents attackers from bypassing the database and reading sensitive information from storage by encrypting data in the database layer. Applications and users authenticated to the database continue to have access to application data transparently, while unauthenticated users attempting to circumvent the database are denied access to clear text data. The high level of protection provided by TDE follows common standards for strong encryption as described in the figure that follows. With Oracle 18c, TDE supports operation with a FIPS 140-2 Level 1 cryptographic module, using approved encryption suites for SSL/TLS and TDE encryption.

TDE's Common Standards for Strong Encryption

Encryption Algorithms	Hashing Algorithms (optional)
Advanced Encryption Standard (AES) Key length: 128, 192, 256 bits	Secure Hash Algorithm (SHA-1)
Triple Data Encryption Standard (TDES) Key length: 168 bits	
Regional encryption algorithms ARIA and SEED GOST	

Built-In Key Management- Key management is critical to the encryption solution security. Oracle Advanced Security TDE provides an out-of-the-box, two-tier key management architecture consisting of data encryption keys and a master encryption key. The database automatically manages the data-encryption keys, which are themselves encrypted by the master encryption key. The master encryption key is stored and managed outside of the database within an Oracle Wallet, a standards-based PKCS12 file that protects keys, or in Oracle Key Vault, a centralized key management platform.

8.9.2 Describe whether or not it is willing to sign relevant and applicable Business Associate Agreement or any other agreement that may be necessary to protect data with a Purchasing Entity.

DXC is willing to negotiate specific agreements with individual Purchasing Entities as relevant and applicable to mutual business requirements related to data protection.

.





8.9.3 Offeror must describe how it will only use data for purposes defined in the Master Agreement, participating addendum, or related service level agreement. Offeror shall not use the government data or government related data for any other purpose including but not limited to data mining. Offeror or its subcontractors shall not resell nor otherwise redistribute information gained from its access to the data received as a result of this RFP.

As the custodian of our clients' critical and proprietary data, DXC exercises the highest degree of care and discretion in the manner in which this data is handled. Client data is never used or accessed for purposes other than as expressly contracted, prescribed, or requested by our clients. This policy is strictly enforced through the DXC Code of Business Conduct, to which every DXC employee must annually certify. Failure by any employee to comply with the policies under the Code of Business Conduct are subject to disciplinary action, up to and including termination.

DXC protects against resale and redistribution of information gained from our access to client data in a number of ways. We begin with personnel screening and training, and also protect against data access through physical, procedural, and software access controls. We hold our subcontractors to the same level of security we uphold.

Personnel screening and training

DXC protects information through our personnel screening and training. We conduct background investigations for applicants before finalizing employment offers, verifying employment application data, testing for drug use, and checking for convictions.

DXC operates a security and confidentiality training program designed for each level of staffing, specific to the role the staff member holds. Training is mandatory for each staff member who has responsibility for the system or access to the data it contains.

DXC staff who handle Protected Health Information (PHI) must complete the HPE training course "HIPAA Privacy and Security Awareness" at initial hire and annually thereafter.

Our security and confidentiality training program also includes the topics on the list that follows.

- Federal and state laws about security and confidentiality that are applicable to the work, including Health Insurance Portability and Accountability Act (HIPAA), Information Practices Act; Welfare and Institutions Code section 14100.2, and National Institute of Standards and Technology (NIST)
- Client security and confidentiality policies and procedures developed to comply with the applicable state and federal laws, including acceptable use, access, and data protection
- Classes of sensitive information, such as PHI, PII, and proprietary information, as well as public information and information that is exempt from disclosure under public record laws
- Staff's roles and responsibilities in maintaining the security and confidentiality of sensitive information and preventing unauthorized disclosure by practicing formal security and confidentiality procedures, such as proper password use, including creating, changing, and safeguarding passwords
- Education on how security and confidentiality breaches can occur in everyday work practices and what steps can be taken both by individuals and by automated processes to minimize or prevent these breaches; steps include taking measures to prevent attempts at social engineering by not opening email attachments from unknown sources, reporting attempted phishing, and not forwarding emails suspected of containing viruses





- Review of the manual and automated processes and the policies and procedures put in place to protect these processes
- Physical safeguards for the building, including fire safety training

DXC regularly reviews the training files of staff members to verify that they are current with training requirements.

In addition to this list, DXC requires annual Standards of Business Conduct training to keep these standards foremost in employees' minds and to be sure the resources for related questions and incident reporting are regularly communicated.

Physical controls

DXC designs our facilities to limit access to authorized personnel only. Our facilities are monitored using security personnel and cameras. We lock unmanned entrances to prevent unauthorized access and make sure facility exterior and the surrounding grounds are well lit.

Inside DXC facilities, we physically separate various zones and require different permissions with varying access card credentials, door codes, or combinations to gain access to more restricted areas. Control points include the main entrance, service entrances, loading platform or garage entrances, inside facility entrance, and secondary entrances. An authorized person must accompany unauthorized personnel, such as maintenance or cleaning personnel, network providers, or visitors.

DXC controls physical access using a key card system. The key card system controls the days and times the cardholder can be on the premises or in designated areas, depending on the person's job responsibilities.

Procedural controls

An example of DXC's procedural controls is our entry monitoring. Visitors, including messengers, are required to sign a Visitor Log before receiving a temporary key card. At minimum, the log includes the elements on the following list.

- Visitor name
- Agency/company the visitor represents
- Visit purpose, including name of individual to whom the visit is made
- Arrival date and time
- Departure date and time

We require visitors to have identification or credentials to enter the facility, and to be escorted to their destination. When leaving, the visitor must surrender the visitor key card.

Another procedural control is separation of duties, so that approvals cannot be given by the same employee who performs an action.

Marking sensitive data

Marking sensitive data is another procedural control. DXC handles client the information within the system, whether paper or electronic, in accordance with the DXC Information Handling Security Standards. This includes the areas of information handling on the following list.

- Standards for restricting access to output products based on content and classification
- Standards and controls used for transporting or mailing media or printed output
- Internal and external labeling based on content and classification





- External labels and special handling instructions, including inventory identifiers, controlled access, special storage instructions, and release or destruction dates
- Standards for shredding or other destructive measures for hardcopy media that is no longer required
- Access, retrieval, duplication, disclosure

DXC only permits staff to use the information they create, maintain, or collect for a customer for the specific business purpose that the written terms of our agreement define. DXC staff follow the Minimum Necessary rule when accessing, using, or disclosing confidential or sensitive information, including PHI/PII or other sensitive information. By both technical controls, such as role-based access, and non-technical controls, such as policies and training, our staff's use and disclosure of confidential information is limited to only what is necessary to perform their jobs.

DXC prevents unauthorized individuals from accessing system information or reading, copying, altering, or stealing printed or electronic information through the mechanisms on the following list.

- The files must have appropriate, restrictive access control lists and permissions applied
- No anonymous user IDs are allowed except on public access systems that do not contain confidential information or PHI
- Microsoft Windows-based computer systems must have current anti-virus software installed and functioning.
- Data requests from within the DXC organization must have audit trails showing who accessed, what they accessed, and when, as pertinent to the request.
- Data requests by individuals from outside the DXC organization must follow the procedures established by the customer Privacy Officer.
- Log files, audit trails, and system access requests must be maintained for an appropriate time period

DXC staff members will not disclose, except as otherwise specifically permitted by the agreement or authorized by the person who is the subject of customer sensitive or confidential information, any customer sensitive or confidential information to anyone other than customer without prior written authorization from the customer program contract manager, except if state or federal law require disclosure. DXC staff will promptly transmit to the customer program contract manager the requests for disclosure of any customer sensitive or confidential information, including PHI/PII or other sensitive information not emanating from the person who is the subject of the information.

Software controls

Access to computer systems and applications requires an identification (ID) and an associated password. At the network level, we use the ID and password to identify the users and authenticate that the user has access to a personal computer, a network, or an application. At the application level, the ID and password are used to not only identify the user and authenticate what data the user can access, but also to determine whether the user can only view the data or can also change or delete the data.

At a minimum, DXC implements the user ID and password controls on the following list.

- The users must be issued a unique user name for accessing personal and confidential information





- Passwords are not to be shared
- Passwords must be at least eight characters
- Passwords must not be a dictionary word
- Passwords must not be stored in readable format on the computer and must be changed every 60 days
- Passwords must be changed if revealed or compromised
- Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:
 - Upper case letters (A-Z)
 - Lower case letters (a-z)
 - Arabic numerals (0-9)
 - Non-alphanumeric characters (punctuation symbols)

Another aspect of security is access by location—facility and virtual local area network (VLAN)—and access methods (direct local area network (LAN), wide area network (WAN), and virtual private network (VPN)). Using third-party security mechanisms, if an individual is only allowed to access the system from a specific office (IP range) or using a certain connection method, the individual's user ID can be blocked when attempts originate from a different location or using a different connection method. DXC also uses rules related to unsuccessful logon attempts, password timeouts, session timeouts, activity timeouts, and other security items, as appropriate.

Additional protection from unintentional disclosure of data to an unauthorized party will include software designed to prevent or report the transmittal of specific data elements that violate policies for that specific data type. We configure computer operating systems, based on policy, to recognize specific types of devices and only perform actions specific to that type of device. DXC follows redaction policies before printing reports or displaying data.

Security audits

In addition to examining access audits, security event logs, and security incident tracking reports, DXC schedules internal and external audits. We carefully examine audit reports and promptly initiate follow-up, such as procedural changes, as indicated.





8.10 Service Level Agreements

8.10.1 Offeror must describe whether your sample Service Level Agreement is negotiable. If not describe how it benefits purchasing entity's not to negotiate your Service Level Agreement.

Some service levels are negotiable, where DXC is fully responsible for the end-to-end services, such as environments that are hosted in a DXC data center. Examples include Virtual Private Cloud, Service Desk, and VDA. SLA information is provided in our response to question 8.10.2.

Other service levels are pre-defined by our IaaS, PaaS, and SaaS partners, based on their standard service offerings, and are not negotiable. It is vital to understand the Purchasing Entity's need for service levels related to the workload or application, which will drive DXC's solution design. This will align Purchasing Entity workload service level needs with designed-in features such as availability sets, availability zones and disaster recovery solutions.

DXC leverages our strong relationships with global IaaS and SaaS partners to deliver services to our customers and ensure high availability of cloud resources. We collaborate with these partners in securing high availability of the platforms and applications. Please refer to the URLs in the following figure that show our partners' service level commitments for their respective platforms.

DXC Partner Service-level Commitments

Partner	Site
IBM Cloud	https://www-03.ibm.com/software/sla/sladb.nsf/sla/bm
AWS	https://aws.amazon.com/legal/service-level-agreements/
Azure	https://azure.microsoft.com/en-us/support/legal/sla/summary/
Oracle	https://cloud.oracle.com/iaas/sla
SAP	https://www.sap.com/about/cloud-trust-center/cloud-service-level-agreements.html
ServiceNow	https://www.servicenow.com/content/dam/servicenow/other-documents/schedules/ServiceNow_Subscription_Service_Guide_111214.pdf
Salesforce	https://trust.salesforce.com/en/
Workday	http://www.erpsearch.com/workday-price.php

8.10.2 Offeror, as part of its proposal, must provide a sample of its Service Level Agreement, which should define the performance and other operating parameters within which the infrastructure must operate to meet IT System and Purchasing Entity's requirements.

Azure

The overall service levels provided to the client comprise the following suite of service layers:

Azure Service Layers Suite

Layer	Service SLA	Notes
Infrastructure	Microsoft (typically 99.95%)	Applies regardless of whether Enterprise Agreement (EA) or Cloud Service Provider (CSP). Service levels can be changed, depending upon the design availability sets or availability zones. If no availability set is configured, the base Microsoft availability may not be available.





Layer	Service SLA	Notes
Infrastructure support	Microsoft – dependent on the level of support taken out	If the client has an EA, their support contract should accompany this SLA, and we will raise tickets into Microsoft based on their support contract. If the client is CSP, the support request is raised to Microsoft based upon DXC's support contract with Microsoft. For all EA clients, DXC recommends opening a case directly with Microsoft
Managed Service	SLOs added into the Solution pack for Managed Service (will be future SLAs)	This is the service level that DXC commits to for managed services.

AWS

DXC, as the reseller of the AWS services, will provide the support for both the CS for AWS service and for the AWS environments that DXC is reselling to the Purchasing Entity. The Purchasing Entity will not contact AWS directly for support.

Response Time SLA

- If DXC fails to respond to a Priority 1 or Priority 2 incident within the Response Time SLAs, DXC will pay to the Purchasing Entity a service credit of \$250 U.S. for each incident for which the Response Time SLA was not met ("Response Service Credit"). Multiple, related incidents will count as a single incident for the purposes of measuring Response Time SLAs.
- DXC will pay a maximum of three Response Service Credits in any given month.
- DXC will not pay Response Service Credits for Priority 3 and Priority 4 incidents or for incidents that are incorrectly classified as Priority 1 or Priority 2 by the Purchasing Entity.
- "Respond" means DXC will begin working on the incident reported by the Purchasing Entity as evidenced by documentation in the CS for AWS Portal - for example, by hot hand-off, by calling the user to clarify the issue, or by starting a technical investigation. Responding does not mean that DXC will resolve an incident within the Response Time SLAs.

Severity Descriptions

The following priority levels are used to classify incidents for the CS for AWS service that are reported by the Purchasing Entity to DXC using the methods set out in function ID SD5:

- Priority 1: Complete loss of function so that Purchasing Entity is unable to access the CS for AWS portal, or application(s) located within the AWS environment; or a critical security event. Incidents reported by email may not be classified as Priority 1.
- Priority 2: Degradation of CS for AWS Portal and/or service performance that has a material adverse effect on either the CS for AWS Portal or AWS environment based applications performance, but does not result in an outage; or a circumstance that, in DXC's reasonable discretion, if not corrected, could result in an outage or loss of Purchasing Entity data; or a major security event that degrades or could degrade service.





3. Priority 3: No impact on end users or any degradation of service; or no material degradation or loss of a noncritical business function; or services are functioning normally, but an individual experiences a problem; or a noncritical security event that does not impact performance of the services.
4. Priority 4: A service request that is not a problem with the CS for AWS Service or the AWS environment (e.g., Purchasing Entity seeking advice on the best use of AWS features or functions).

Response Time SLA and Support Process

The following table sets out the Response Times SLAs for the CS for AWS service:

CS for AWS Service Response Times SLAs

Priority Level	Process of Purchasing Entity Submission and DXC Response	Response Time SLA
1	If a Purchasing Entity representative calls the DXC Service Desk, the ticket is logged real-time in the CS for AWS Portal and DXC will respond by a hot hand-off to the appropriate technician while Purchasing Entity representative is still on the phone. If DXC has received notice through a monitoring alert or Purchasing Entity has opened the ticket by any means other than calling the DXC Service Desk or by email, DXC will send a notification to the Purchasing Entity's contact person/mailbox.	<15 minutes
2	If a Purchasing Entity representative calls the DXC Service Desk, the ticket is logged real-time and DXC will respond by a hot hand-off to the appropriate technician while Purchasing Entity representative is still on the phone. If DXC has received notice through a monitoring alert or Purchasing Entity has opened the ticket by any means other than calling the DXC Service Desk, DXC will send a notification to the Purchasing Entity's contact person/mailbox	<75 minutes
3	Upon Purchasing Entity's contact to the DXC Service Desk, the ticket is logged real-time and DXC will respond by forwarding to an appropriate technician for follow up.	<4.25 hours
4	Upon Purchasing Entity's contact to the DXC Service Desk, the ticket is logged real-time and DXC will respond by forwarding to an appropriate technician to follow up.	<1 business day

VPC Service Level Agreements

Managed VPC provides Service Level Agreement (SLA) from 99.0% to 99.95% across the Service Environment for Tier 2 to Tier 4. Availability is measured monthly.

NOTE: Only the Tier-2, Tier-3 (option B) and the Tier-4 (option C) are available in the current version of the NextGen Portal.





VPC Service Level Agreement Tiers

	Tier 2 (Option A)	Tier 2 (Option B)	Tier 3 (Option A)	Tier 3 (Option B)	Tier 4 (Option A)	Tier 4 (Option B)	Tier 4 (Option C)
Data Center Type	Single	Single	Single	Single	Dual	Dual	Dual
Server Type	1 Physical Server	1 Virtual Server	2 or more Physical Servers	1 Virtual Server	2 or 3 Physical Servers	4 or more Physical Servers	1 Virtual Server
Cluster Type	None	Hypervisor Cluster	OS Cluster	Hypervisor Cluster	OS Cluster	OS Cluster	Hypervisor Cluster
Server Management	Managed or Unmanaged Server	Managed or Unmanaged Server	Managed Server	Managed or Unmanaged Server	Managed Server	Managed Server	Managed or Unmanaged Server
SLA Applies to:	Physical Server	Virtual Server	OS Cluster	Virtual Server	OS Cluster	OS Cluster	Virtual Server
Service Level	99.0%	99.90%	99.95%	99.95%	99.99%	99.999%	99.95%

Oracle Cloud SLA

Oracle Cloud is the only service to offer end-to-end SLAs covering availability, manageability and performance services.

- **Availability** -Purchasing Entity cloud workloads will be in continual operation because of Oracle's commitment to uptime and connectivity.
- **Manageability** - The elasticity and configurability of infrastructure is one reason why organizations move applications to the cloud. Purchasing Entity services need to be continuously manageable to deliver this benefit. Oracle is the first cloud vendor to offer manageability SLAs, enabling Purchasing Entities to manage, monitor and modify their resources.
- **Performance** - IaaS resources should be accessible and consistently perform as customers expect. Oracle is the first cloud vendor to guarantee performance, which means Purchasing Entities can rely on the infrastructure for enterprise applications.

Enterprises demand more than just availability from their cloud infrastructure. Mission-critical workloads also require consistent performance, and the ability to manage, monitor and modify resources running in the cloud at any time.

The following graphics further describe availability, manageability and performance services:





Availability

Service/Resource	Measurement	Monthly SLA Percentage	Oracle service credit if SLA breached
Compute	Region Unavailability	Greater than or equal to 99.99% uptime	10%
		Greater than or equal to 99% uptime	25%
Block Volumes	Region Unavailability	Greater than or equal to 99.99% uptime	10%
		Greater than or equal to 99% uptime	25%
Object Storage	API error rate	Greater than or equal to 99.99% uptime	10%
		Greater than or equal to 99% uptime	25%
FastConnect	Private Connectivity	Greater than or equal to 99.99% uptime	10%
		Greater than or equal to 99% uptime	25%

Manageability

Service/Resource	Measurement	Monthly SLA Percentage	Oracle service credit if SLA breached
Compute	API Error rate	Greater than or equal to 99.99% uptime	10%
		Greater than or equal to 99% uptime	25%
Block Volumes	API Error rate	Greater than or equal to 99.99% uptime	10%
		Greater than or equal to 99% uptime	25%
Database	API Error rate	Greater than or equal to 99.99% uptime	10%
		Greater than or equal to 99% uptime	25%

Performance

Service/Resource	Measurement	Monthly SLA Percentage	Oracle service credit if SLA breached
Compute local NVMe drive	Disk IOPS	Resource performance greater than 90% of published performance 99.9% of the time	10%
		Resource performance greater than 90% of published performance 99% of the time	25%
Block Volumes	Disk IOPS	Resource performance greater than 90% of published performance 99.9% of the time	10%
		Resource performance greater than 90% of published performance 99% of the time	25%
Network	Network Performance	Resource performance greater than 90% of published performance 99.9% of the time	10%
		Resource performance greater than 90% of published performance 99% of the time	25%

Service Desk - Contact Channels and SLA

A Service Desk contact is a client-initiated communication, submitted through one of four contact channels - telephone, web-based Portal interface, email form, or chat - which reports an incident or requests a service and requires an agent to record or read, research, find a resolution, and then respond to the client request. The contacts are recorded and tracked for Service Desk billing and service performance reporting purposes. There is not necessarily a one-to-one correlation between a submitted communication and a Contact, because a single





submission may contain multiple requests for assistance. In this case, each item is logged as a Contact and becomes a billable unit of work.

The standard volume of contacts to a Service Desk is one contact per month. This may be adjusted based on client data and complexity. There is no standard division of contacts among the four channels as this is dependent on client's industry, user maturity, and other factors.

The Service Desk Offering provides various standard SLAs for the contact channels, as shown in the following figure:

Service Desk Offering Channel SLAs

Channel	Primary SLA	Secondary SLA(s)
Voice	80% in 60 seconds	80% in 30 seconds
Email	95% in 80 seconds	Multiple
Chat	80% in 120 seconds	80% in 60 seconds 80% in 45 seconds
Portal	95% in 12 hours	Multiple

VDA Service Availability (in a DXC-managed Data Center)

The Target Availability Service Level for the VDA Services hosted at a DXC service location or at a customer site is 99.85% availability during the total minutes in each measurement period of one calendar month starting on the first day of the month following the start of user onboarding.

Availability is defined as the services being available for and capable of delivering the virtual desktops and hosted shared applications to users. Availability is calculated as a percentage (rounded to two decimal places) where the measurement period in the following list applies:

$$\frac{((Actual\ Services\ Available\ Minutes) + (Permitted\ Outage\ Minutes))}{(Total\ Minutes)} \times 100$$
 and where:

1. Actual Services Available Minutes is calculated as 24 x 60 x the number of days in the measurement period minus total outage time in that measurement period
2. Permitted Outage Minutes means the period in minutes for all permitted outages during a measurement period
3. Total Minutes is calculated as 24 x 60 x the number of days in the measurement period
4. Outage means the services are unavailable to more than 10% of the active users attempting to access them. Following resolution of an incident, DXC will calculate the total number of possible active users attempting to access the services based upon the timing and location of an outage.

Outage Time means the time in minutes between the start time logged for an incident and the time that incident is resolved or a workaround implemented as documented in the unavailability record for Priority 1 or Priority 2 incidents.

Availability measurements relate only to availability of the services, and do not include availability of the network connecting the user to the services.





8.11 Data Disposal

Specify your data disposal procedures and policies and destruction confirmation process.

DXC uses industry-standard data disposal methodologies, and we maintain a complete chain of custody for all sensitive data and equipment. We can provide an audit trail on request and as required by Purchasing Entities for regulatory requirements.

Media storage devices used to store purchasing entities data are classified as Critical and treated accordingly throughout their life-cycles. DXC's solutions has standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, media is decommissioned using techniques detailed in NIST 800-88. Media that stored purchasing entities data is not removed from its control until it has been securely decommissioned.

Disk-disposal process that complies with NIST SP 800-88 R1, *Guidelines for Media Sanitization* is been used. Disks are physically destroyed to render recovery of data impossible. Records of the destruction are retained and reviewed as part of the audit and compliance process. Cloud services use approved media storage and disposal-management services.

Data-destruction techniques vary, depending on the type of data object being destroyed, whether it be whole subscriptions themselves, storage, virtual machines, or databases. In a multi-tenant environment, careful attention will be taken to be sure that one Purchasing Entity's data is not allowed to either leak into another Purchasing Entity's data, or when a Purchasing Entity deletes data, no other Purchasing Entity (including, in most cases, Purchasing Entity who once owned the data) can gain access to that deleted data.

Below stated are some of the disposal procedures and policies adhered to incorporate best practices and recommended approach via it's different cloud solution's and offerings made available to purchasing entities.

1. If a storage account is deleted within an existing subscription (or when a subscription deletion has reached its timeout), the storage account is not actually deleted for two weeks to allow recovery from mistakes. Once a storage account is finally deleted, or when blob or table data is deleted outside the context of a storage account deletion, the data is no longer available. To make storage data unrecoverable faster, the Purchasing Entity should delete tables and blobs individually before deleting the storage account or subscription.
2. Instead of allocating log files directly from disk sectors, log files are created in a file system running New Technology File System (NTFS). A background thread running on Cloud Storage nodes frees space by going through the oldest log file, copying blocks that are still referenced from that oldest log file to the current log file (and updating all pointers as it goes). It then deletes the oldest log file. So there are two categories of free space on the disk: space that NTFS knows is free, where it allocates new log files from this pool, and space within those log files that Cloud Storage knows is free since there are no current pointers to it.
3. Database implementation is designed to be sure user data is never leaked by disallowing access to the underlying storage except by means of the related Database API. That API allows users to read, write, and delete data, but does not have a way to express the reading of data that the user has not previously written.
4. When services are terminated or at a Purchasing Entity's request, DXC will delete environments or data in a manner designed to make certain that the environments can't





reasonably be accessed or read, unless there is a legal obligation imposed that prevents from deleting all or part of the environments or data.

DXC Virtual Private Cloud (VPC)

In accordance with DXC policy, Purchasing Entity data will be handled and protected as DXC Confidential data. Purchasing Entity data will never be copied to, or stored on a VPC management server (a server that is part of the VPC management infrastructure). VPC Security makes the determination that none of the data stored on the local disks of the VPC management servers is considered DXC Confidential.

VPC Customer Data Disposition

Customer data in VPC can reside on any of the following sites:

- VPC customer physical server local disk
- VPC SAN storage array
- VPC virtual tape library (used for on-site backups)
- VPC physical tape (used for off-site backups)
- VPC file storage (NAS)

VPC Customer Physical Server Local Disk

When a customer terminates a VPC physical server, the physical server's local disks are automatically wiped using a multi-pass overwrite approach.

VPC SAN Storage Array

When a customer terminates a VPC server, with any VPC SAN storage attached to the server, the following situations could occur:

- If the SAN storage was provisioned from an EVA storage array and attached to a physical server, VPC Delivery will perform a multi-pass overwrite disk wipe of the SAN LUNs released by the Purchasing Entity.
- If the SAN storage was provisioned from a 3PAR storage array and attached to a physical server, the SAN LUNs released by the Purchasing Entity will be deleted. Based on the technology used by the 3PAR arrays, VPC Security considers this is sufficient to prevent any subsequent access.
- If the SAN storage was provisioned from a VPC SAN storage array and attached to a virtual server, the virtual disks released by the Purchasing Entity will be deleted. Based on the virtualization technology used, VPC Security considers this is sufficient to prevent any subsequent access

VPC Virtual Tape Library

When a customer requests onsite backup service, the data backed up from the Purchasing Entity servers is stored on a VPC virtual tape library. Upon receipt of a Purchasing Entity release of disk space on the virtual tape library and after the retention period requested by the Purchasing Entity has expired, the backups will be deleted. Based on the virtual tape technology used, VPC Security considers this is sufficient to prevent any subsequent access.

VPC Physical Tape

When a Purchasing Entity requests off-site backup service, then a pool of physical tapes is dedicated to this Purchasing Entity. The data backed up to a physical tape is encrypted by DXC. VPC Security considers the use of encryption sufficient to prevent any subsequent access if physical tapes are later reused for other purposes. Data disposition using physical tape destruction is also available at the Purchasing Entity's request.





VPC File Storage

When a Purchasing Entity requests file storage, then it is provisioned from a NAS device. Upon a customer release of file storage, the file shares are deleted. Based on the technology used for file storage, VPC Security considers this is sufficient to prevent any subsequent access.





8.12 Performance Measures and Reporting

8.12.1 Describe your ability to guarantee reliability and uptime greater than 99.5%. Additional points will be awarded for 99.9% or greater availability.

As a Cloud Service Provider, DXC partners with cloud product vendors to deliver a bundled service to our clients. As such, our SLAs are aligned with the cloud partners' offerings, with uptime reliability varying between 99.5 to 99.95%, depending on the partner product and the design proposed to the Purchasing Entities. For example, in Azure cloud, the Internet-facing virtual machines that have two or more instances deployed in the same availability set, DXC provides an SLA of 99.95%.

DXC leverages various tools to manage the agreed SLAs. DXC leverages key tools such as Operations Management Suite (OMS), which is a collection of cloud-based services for managing client on-premises and cloud environments.

This core function of OMS is provided by a set of services, and each service provides a specific management function. It is possible to combine services to achieve different management scenarios. Some examples are shown in the following table:

	Service	Description
	Log Analytics	Monitor and analyze the availability and performance of different resources including physical and virtual machines.
	Automation	Automate manual processes and enforce configurations for physical and virtual machines.
	Backup	Backup and restore critical data.
	Site Recovery	Provide high availability for critical applications.

MH102_12_0718

Figure 12: OMS Examples

One of the key features of OMS is log analytics, which collect the data stored in the OMS repository, and is hosted on cloud. Connected sources generate data collected into the OMS repository.

As part of DXC managed services gold offering, ServiceNow is closely integrated with the OMS engine so that alerts are notified and converted into tickets. With the help of a 24x7 DXC CloudOps team, we have ability to secure reliability and higher uptime as per the SLA.

Oracle Cloud

Enterprises demand more than availability from their cloud infrastructure. Mission-critical workloads also require consistent performance and the ability to manage, monitor, and modify resources running in the cloud at any time. Only Oracle offers end-to-end SLAs covering availability, manageability and performance of services.





Availability

Service/Resource	Measurement	Monthly SLA Percentage	Oracle service credit if SLA breached
Compute	Region Unavailability	Greater than or equal to 99.99% uptime	10%
		Greater than or equal to 99% uptime	25%
Block Volumes	Region Unavailability	Greater than or equal to 99.99% uptime	10%
		Greater than or equal to 99% uptime	25%
Object Storage	API error rate	Greater than or equal to 99.99% uptime	10%
		Greater than or equal to 99% uptime	25%
FastConnect	Private Connectivity	Greater than or equal to 99.99% uptime	10%
		Greater than or equal to 99% uptime	25%

Manageability

Service/Resource	Measurement	Monthly SLA Percentage	Oracle service credit if SLA breached
Compute	API Error rate	Greater than or equal to 99.99% uptime	10%
		Greater than or equal to 99% uptime	25%
Block Volumes	API Error rate	Greater than or equal to 99.99% uptime	10%
		Greater than or equal to 99% uptime	25%
Database	API Error rate	Greater than or equal to 99.99% uptime	10%
		Greater than or equal to 99% uptime	25%

Performance

Service/Resource	Measurement	Monthly SLA Percentage	Oracle service credit if SLA breached
Compute local NVMe drive	Disk IOPS	Resource performance greater than 90% of published performance 99.9% of the time	10%
		Resource performance greater than 90% of published performance 99% of the time	25%
Block Volumes	Disk IOPS	Resource performance greater than 90% of published performance 99.9% of the time	10%
		Resource performance greater than 90% of published performance 99% of the time	25%
Network	Network Performance	Resource performance greater than 90% of published performance 99.9% of the time	10%
		Resource performance greater than 90% of published performance 99% of the time	25%





8.12.2 Provide your standard uptime service and related Service Level Agreement (SLA) criteria.

DXC is committed to secure the maximum availability of the infrastructure. DXC will provide standard uptime based on the offerings being delivered. The below table is an example of server availability managed by DXC. Additional uptime SLAs for some of our cloud offerings are described above in sections 8.10.2 and 8.12.1.

Server Availability

Server availability applies to DXC Server Management Services. DXC will provide monthly image availability statistics that measure the average time expressed as a percentage that an image is available. Server availability is limited OS availability and hardware issues only.

Description	Service Level Objective
Server Availability (Remote Server Support)	99% server availability
Server Availability (Default)	99.5% server availability for servers located in a DXC Data Center
VMware Specific	99.7% Conditions – Service location must be a DXC Data Center and managed storage boot from SAN used. Environment must also be using VMware vMotion, HA, and DRS technologies.
Server Availability (with Cluster Management and Performance and Capacity Management Uplifts)	99.95% server availability for servers in a DXC Data Center with cluster management and performance and capacity management uplifts selected. System configuration also is to be validated by DXC for high availability design

Server availability percentage will be calculated as follows: (Total Uptime divided by (Maximum Uptime minus Excluded Downtime)) times 100 where: Total Uptime = the maximum uptime minus all downtime.

Maximum Uptime = the maximum number of minutes available in a month is the number of days in the month x 24 hours x 60 minutes = maximum uptime.

Excluded Downtime = the number of minutes of any planned or schedule downtime, plus the number of minutes of any downtime resulting from non DXC-supported hardware or software that would be considered outside the control of DXC.

The following tables show the calculations for months with 28, 29, 30, and 31 days.

Maximum Uptime and Availability Metrics

Maximum Uptime				Availability Metric		
Days	Hours	Minutes	Total Min.	99.00%	99.50%	99.95%
28	24	60	40,320	403.2	201.6	20.2
29	24	60	41,760	417.6	208.8	20.9
30	24	60	43,200	432	216	21.6
31	24	60	44,640	446.4	223.2	22.3

Server Availability Alerts





DXC will detect and respond to up/down availability faults generated by monitored Server Management Services.

Description	Service Level
System Down Alerts	Detect and respond within 15 minutes

The following table depicts the DXC's standard SLA offering. DXC will discuss SLAs with the Purchasing Entity to finalize them.

Offering Service Level Targets

Offering	Service Level Name	Target
Configuration Management	Back End Infrastructure Configuration Items Accuracy	98%
Incident Management	Response Goal	Resolution Goal
	Priority 1: Response 15 Minutes	Priority 1: Resolution 4 Hours
	Priority 2: Response 30 Minutes	Priority 2: Resolution 8 Hours
	Priority 3: Response 4 Hours	Priority 3: Resolution 3 Days
	Priority 4: Response 1 Day	Priority 4: Resolution 5 Days
Problem Management	DXC to create a Problem Record within 2 Business Days of Critical Incident Restoration	100%
Change Management	Standard DXC Monthly Change Report highlighting DXC's adherence to the Change Management Process	100%
Monthly Service Report Delivery	Monthly Service Management Draft Report within 10 Business Days	100%
	Monthly Service Management Final Report within 15 Business Days	100%

8.12.3 Specify and provide the process to be used for the participating entity to call/contact you for support, who will be providing the support, and describe the basis of availability.

DXC Global Service Desk solutions use our Global Delivery Center capabilities to deliver services across the globe. DXC's Service Desk provides a Single Point of Contact (SPoC) for our clients' user community, as well as serving as the key interface between clients and DXC delivery teams.

DXC will provide multiple interfaces to Purchasing Entities to call/contact DXC for support. Purchasing Entities can contact DXC service desk to request services or support. DXC will publish service catalogs in DXC's ServiceNow tool for each contracted service or offering. Purchasing Entities can access DXC's service catalog to request services through a self-service interface. Purchasing Entities can also contact DXC's critical-incident manager directly in case of a business outage. The following table follows DXC's hours of operation:





DXC Support Availability

Hours of Operations			
Team	Incident Management	Change Management	General Support (EST)
NOC	24*7 incl Holidays	As scheduled	Business Days 06:00 – 18:00
Cloud Ops	24*7 incl Holidays	As scheduled	Business Days 06:00 – 18:00
Level 3	Business Days 06:00 – 18:00	As scheduled	Business Days 06:00 – 18:00
Monitoring	24*7 incl Holidays	As scheduled	Business Days 06:00 – 18:00
Tools	24*7 incl Holidays	As scheduled	Business Days 06:00 – 18:00
Storage	24*7 incl Holidays	As scheduled	Business Days 06:00 – 18:00
Backup/Recovery	24*7 incl Holidays	As scheduled	Business Days 06:00 – 18:00
Middleware	24*7 incl Holidays	As scheduled	Business Days 06:00 – 18:00
Database	24*7 incl Holidays	As scheduled	Business Days 06:00 – 18:00
Security	24*7 incl Holidays	As scheduled	Business Days 06:00 – 18:00
Mainframe Support	24*7 incl Holidays	As scheduled	Business Days 06:00 – 18:00
Servers	24*7 incl Holidays	As scheduled	Business Days 06:00 – 18:00
Network	24*7 incl Holidays	As scheduled	Business Days 06:00 – 18:00

8.12.4 Describe the consequences/SLA remedies if the Respondent fails to meet incident response time and incident fix time.

The DXC Service Level Manager will host internal daily service reviews, engaging the DXC work streams to monitor service performance, taking into account the effect of outages or planned changes on service stability. This allows us to improve the overall service performance through preventive review of critical service levels and service-improvement plans.

If potential KPI breaches are identified, these will be escalated to DXC's delivery management team, where mitigation plans to resolve service issues will be created and worked through to resolution. Also, the Continual Service Improvement (CSI) practices will be used to improve the efficiency and effectiveness of Service Level Management and offerings, which support achieving the business objectives and meeting or exceeding the Purchasing Entity requirements.

Performance Service Improvement Program (SIP) – If a service level review indicates non-compliant service performance, we initiate a SIP to correct the performance. The first step is for the affected stakeholders to determine the SIP objectives. Objectives should be S.M.A.R.T. (specific, measurable, achievable, realistic, with a timeline), and they should clearly state the criteria for success to allow for signoff. Based on the SIP objectives, DXC defines and executes corrective actions, engaging change management when necessary, and coordinating progress reviews through program and project management for proper implementation. After DXC implements the corrective actions, we measure outcomes against the SIP objectives to make sure we meet the objectives. DXC obtains appropriate signoff from Purchasing Entity prior to closing the SIP.

8.12.5 Describe the firm's procedures and schedules for any planned downtime.

DXC's procedure for any planned downtime will be tightly coupled with its change management process. For any planned downtime, DXC will work with appropriate stakeholders to get the appropriate approvals. After a planned downtime change is approved, DXC will communicate specific information to all areas affected by the planned downtime. By providing stakeholders





with advance notification in accordance with agreed timelines, stakeholders are able to make necessary preparations to minimize or avoid downtime-related adverse business effects. DXC's change management policies require that communications regarding planned downtime include the following information:

- IT system or application that will be down and the department/service areas that will be affected
- Time that the downtime will begin and the expected length of time the system or application will be unavailable
- Reason for the downtime and what changes can be expected once the planned downtime is completed, such as regular maintenance, where no changes are expected, and enhancements to the system

8.12.6 Describe the consequences/SLA remedies if disaster recovery metrics are not met.

DXC typically contracts disaster recovery commitments as Service Level Objectives rather than SLAs due to the high degree of variability, inter-dependencies across parties and stakeholders, and inability to predict the circumstances surrounding possible disaster recovery scenarios. Therefore, any associated remedies in the agreement would be treated as SLO remedies.

If failures occur during DR exercises, such as inability to recover applications or data, or not meeting the defined RPO or RTO, the DXC Continuity Services Team will register an associated problem management case which will then initiate the following activities:

1. Assign the required subject matter experts listed in the support matrix to resolve the problem
2. Escalate according to the escalation matrix
3. Trigger root cause analysis once the problem is resolved
4. Identify the Root Cause and document in a formal root cause report
5. Conduct an account team and Purchasing Entity discussion of the root cause
6. Generate an account team for recommendations for possible remedies to the disaster recovery solution, processes, or policies to address the root cause. Any associated remedies will be implemented based on mutual agreement between the client and DXC, through the defined Request Management and Change Management processes.

8.12.7 Provide a sample of performance reports and specify if they are available over the Web and if they are real-time statistics or batch statistics.

DXC believes that Performance Management is not only about effectively using best-in-class tools, but also utilizing experts and processes to reduce risk in today's complex operating environments. Our value-added service orchestrates performance management across both the technical and business domains, integrating Service, Incident, and Problem Management functions.

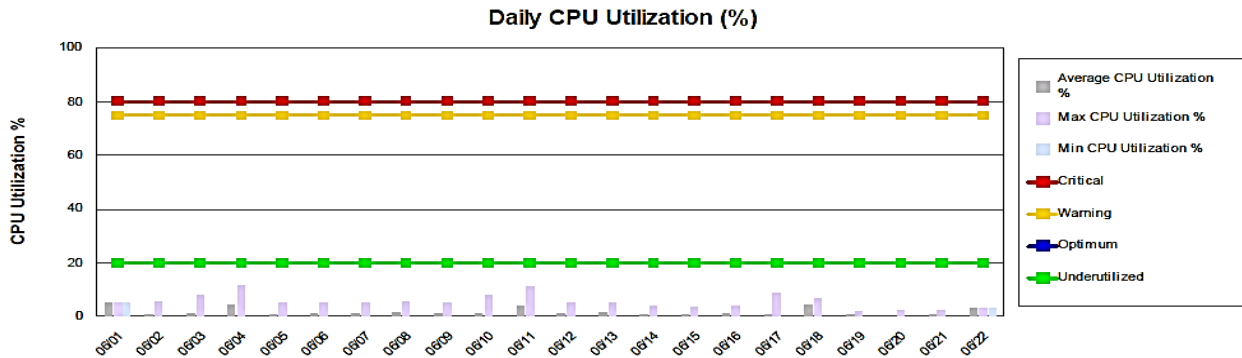
Purchasing Entities can access performance reports over the Web that include a combination of both real-time report interfaces and scheduled batch reports, depending on the services being provided and on Purchasing Entity's requirements.





Sample performance reports are provided below:

Sample Server CPU performance reports:



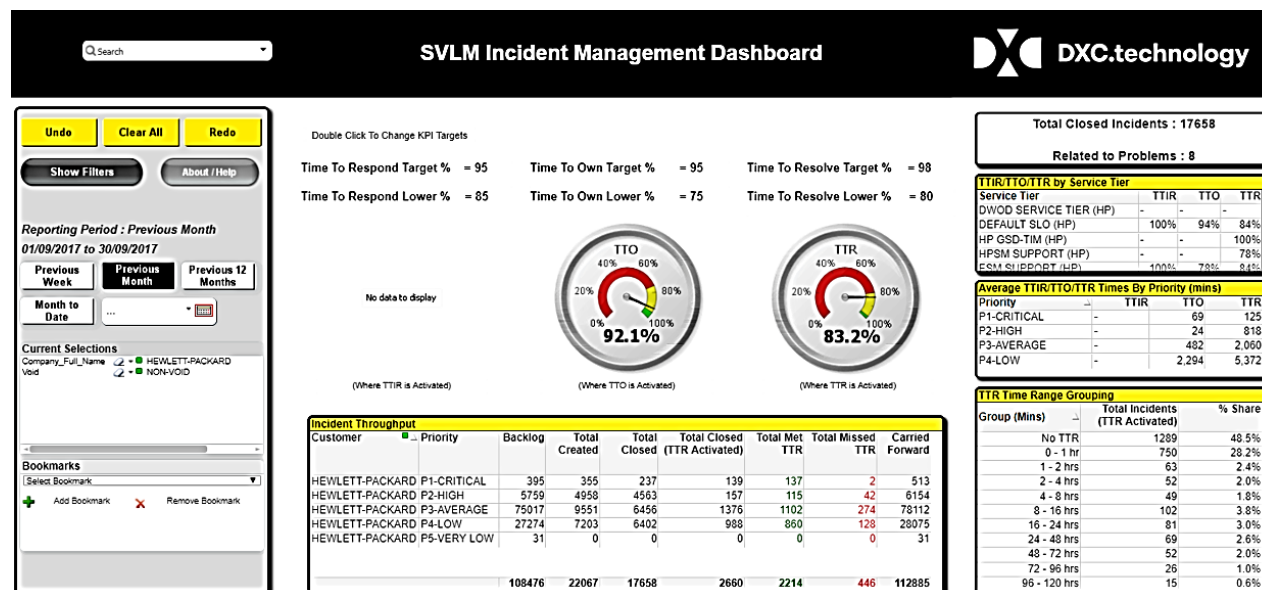
Server Performance Management Trending Summary

		2016/06	2016/07	2016/08	2016/09	2016/10	2016/11	2016/12	2017/01	2017/02	2017/03	2017/04	2017/05
crmpm1s.corp.drreddys.com	Average CPU % Use	35.10	9.41	22.31	11.32	7.40	6.50	7.55	5.76	4.06	3.34	1.99	3.93
	90th CPU % Use	53.97	14.66	50.85	18.27	11.96	9.16	11.95	7.49	8.02	6.39	3.18	7.88
	Average Disk_IO Utilization	88.99	67.01	59.89	59.11	57.65	33.50	38.38	54.95	49.07	37.28	18.68	46.36
	90th Disk_IO Utilization	98.34	83.86	79.80	71.86	70.42	54.73	56.14	63.63	68.48	58.05	30.66	71.93
	Average Memory Bottleneck	39.75	40.00	39.81	40.00	40.00	40.00	40.00	36.29	13.09	10.01	10.03	29.92
	90th Memory Bottleneck	40.00	40.00	40.00	40.00	40.00	40.00	40.00	40.00	32.00	24.00	19.50	40.00
cto2app.empowerscto2.com	Average CPU % Use	1.49	1.95	1.71	2.74	2.60	2.23	1.82	2.16	1.22	2.00	1.04	2.10
	90th CPU % Use	5.45	6.70	6.34	7.75	8.02	7.96	7.85	6.60	5.30	6.40	6.16	7.69
	Average Disk_IO Utilization	55.51	57.58	56.84	80.19	87.19	76.66	27.65	23.47	13.97	17.83	8.14	12.39
	90th Disk_IO Utilization	61.82	70.87	64.25	90.68	92.17	92.73	31.56	36.86	17.12	36.16	19.33	26.85
	Average Memory Bottleneck	6.33	6.32	14.17	17.53	10.70	3.30	3.33	4.89	6.88	9.99	5.47	5.00
	90th Memory Bottleneck	11.42	10.50	22.00	21.50	19.17	5.75	6.83	11.20	11.70	16.00	10.00	14.67
cto2db.empowerscto2.com	Average CPU % Use	1.63	1.56	1.48	1.79	1.46	1.51	1.26	1.37	0.86	1.36	0.70	1.47
	90th CPU % Use	2.63	2.16	2.70	2.42	2.17	2.39	2.95	2.66	1.93	2.68	1.96	3.22
	Average Disk_IO Utilization	15.27	13.78	13.47	15.88	14.13	15.91	16.95	16.82	11.99	15.75	8.90	20.90
	90th Disk_IO Utilization	20.97	18.32	17.20	16.47	17.09	21.99	33.24	30.55	21.66	25.64	16.66	46.03
	Average Memory Bottleneck	9.33	8.66	7.31	8.92	8.05	8.22	7.53	8.25	5.13	7.59	3.00	10.11
	90th Memory Bottleneck	12.42	11.50	8.33	10.75	9.75	11.80	10.53	14.80	8.03	16.00	9.80	20.00
dbserver.fto3empower2.com	Average CPU % Use	0.87	1.03	0.53	0.36	0.34	0.35	0.41	0.41	0.44	0.40	0.29	0.49
	90th CPU % Use	1.12	1.25	0.92	0.43	0.40	0.48	0.59	0.59	0.63	0.62	0.57	0.66
	Average Disk_IO Utilization	4.77	4.91	4.28	3.80	2.75	3.25	5.06	4.76	5.69	4.32	1.99	7.42
	90th Disk_IO Utilization	5.42	5.72	6.34	5.31	4.95	7.07	9.14	9.16	11.07	8.96	9.41	11.27
	Average Memory Bottleneck	4.26	3.87	2.15	2.31	1.56	2.17	3.97	3.88	3.71	3.55	0.92	6.13
	90th Memory Bottleneck	13.08	8.00	3.33	1.67	2.42	4.00	8.00	8.00	8.00	8.00	5.00	10.00
dbserver.fto6empower2.com	Average CPU % Use	0.00	0.00	0.00	6.38	6.57	5.99	1.35	0.56	0.47	0.59	0.97	0.52
	90th CPU % Use	0.00	0.00	0.00	10.11	9.35	10.11	2.51	0.81	0.72	0.98	1.50	0.99
	Average Disk_IO Utilization	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	90th Disk_IO Utilization	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	Average Memory Bottleneck	0.00	0.00	0.00	8.00	7.10	10.80	3.74	3.22	2.48	3.57	8.78	3.47
	90th Memory Bottleneck	0.00	0.00	0.00	10.83	9.17	21.33	5.83	8.00	5.00	8.40	14.70	10.00
dmshps1s.corp.drreddys.com	Average CPU % Use	2.55	2.75	2.04	1.50	0.90	1.20	1.06	1.12	1.25	0.83	0.49	1.74
	90th CPU % Use	2.94	3.28	2.77	2.48	1.26	1.77	1.81	2.09	2.83	1.44	0.98	3.23
	Average Disk_IO Utilization	9.69	8.95	6.07	11.67	8.96	15.29	17.19	16.41	16.52	9.13	3.95	21.21
	90th Disk_IO Utilization	10.95	10.29	10.87	16.04	14.81	24.33	29.39	28.51	44.01	21.87	9.10	40.68
	Average Memory Bottleneck	1.06	0.83	0.83	1.14	0.84	0.67	0.44	0.69	0.63	0.54	0.60	0.35
	90th Memory Bottleneck	1.67	1.67	0.83	2.50	0.83	1.58	1.22	2.33	1.75	0.99	4.00	0.83





Sample Dashboard



8.12.8 Ability to print historical, statistical, and usage reports locally.

DXC will provide access to its reporting console where a Purchasing Entity can access the current reports. Historical reports can be printed locally as well.

8.12.9 Offeror must describe whether or not its on-demand deployment is supported 24x365.

DXC's delivery and onboarding team, present across multiple locations, can address rapid and on-demand deployment requests with support 24x365. We rely on automation tools and enhanced web portals which will help us achieve quick onboarding and seamless operations.

The DXC Agility Platform is an enterprise-grade cloud management platform for implementing DevOps and on-demand, self-service IT operating models supported 24x365 within large enterprises. A Purchasing Entity can select the DXC Agility Platform to automate deploying and managing enterprise applications and platforms across private, public, and hybrid clouds.

Key differentiators include the following:

- Provides a single, integrated control point for governance, compliance, and security across an organization's cloud applications and environments, empowering development teams by providing fully governed, self-service access to the applications, platforms, and services. This enables a Purchasing Entity's central IT function to transform its role into that of a hybrid cloud service broker and allows Purchasing Entity development and IT operations teams to increase the speed and frequency of software releases without sacrificing software quality in production.
- Allows enterprises to establish cloud vendor contestability, and simplifies the operational complexities of DevOps and hybrid cloud management.
- Emphasizes policy-based governance and security both for risk mitigation and as an enabler of end-to-end, fully automated self-service IT models





- Provides a broad range of application-centric policy controls can be rapidly enforced across SDLC stages and hierarchical organizational models.
- Provides application blueprints that are infrastructure independent, and automate orchestrating and deploying complex, multi-tier platforms and applications. Blueprints help automate enforcement of governance and security standards across SDLC stages.
- Provides DXC Agility Platform's Release Manager, which is a visual dashboard, promotes application code and complete deployment environments across SDLC stages for software release automation. Release Manager provides an end-to-end view of the release pipeline, integrates into existing SDLC tool chains, and provides customizable approval processes and quality gates.

Also from the DXC VPC offering, we have a VPC NextGen self-service client portal that enables authorized users to have secure, role-based 24x365 access to add, delete and manage cloud services in real time. This VPC portal is a web-based customer interface to order and manage Managed Cloud services with unified access to billing and support services. The portal acts as a presentation layer for a number of capabilities that improve the customer experience by making it self-service. It also provides a dashboard which contains access to a number of different pages. Each page provides different set of features or services which the customer uses as required to build and maintain their Virtual Private Cloud. The portal dashboard provides options such as Marketplace, Orders, VSCAN, Activity history, Services.

Marketplace displays customer specific catalog services based on the range of DXC Virtual Private Cloud services that the customer can choose to make available in their cloud. The Marketplace section of the portal improves the user experience by offering a more intuitive user interface that makes it easier for the customer to order the assets needed to provide a solution that meets their needs.

Services allows users to initiate service actions and configure service settings for a provisioned service, including the following:

- Starting, stopping, suspending, resuming and rebooting servers
- Mounting and unmounting storage volumes, resizing storage and attaching storage to servers
- Creating\deleting\resetting password of Local OS User Accounts
- Resizing virtual machines
- Unsubscribing from a service in the page

8.12.10 Offeror must describe its scale-up and scale-down, and whether it is available 24x365.

The DXC solution also has the capability to enable applications to automatically scale up and down, 24x365, without human interaction and based on a predefined policy and workloads.

DXC's offerings enable dynamic scalability, rapid elasticity, on-demand resizing of resources, and scale-up or scale-down for peak workloads. Scale-up is achieved by resizing to a larger VM size, scale-down involves resizing to a smaller VM size. The actual resizing of a VM is fully automated with no one-time charge (OTC) for the VM resize operation. The customer billing will be adjusted to reflect the new VM size. VM disks are not changed in the process - a VM resize operation only changes the number of virtual CPUs (vCPUs) and the amount of virtual memory assigned to the VM.





8.13 Cloud Security Alliance

Describe and provide your level of disclosure with CSA Star Registry for each Solution offered.

- a. Completion of a CSA STAR Self-Assessment. (3 points)*
- b. Completion of Exhibits 1 and 2 to Attachment B. (3 points)*
- c. Completion of a CSA STAR Attestation, Certification, or Assessment. (4 points)*
- d. Completion CSA STAR Continuous Monitoring. (5 points)*

The value we bring to all clients and Purchasing Entities goes far beyond our discrete DXC Security offerings. DXC offer core security capabilities that differentiate DXC as a leading Security Advisory Services (SAS) and Managed Security Services (MSS) provider. DXC Technology helps clients harness the power of innovation to thrive on change. For more than 60 years, we have successfully guided the world's largest enterprises and government agencies through successful change cycles. We take pride in our technology independence and our role as a trusted advisor. Our deep experience gives us a clear and confident vision to help clients navigate the future.

DXC proposes Microsoft Azure, AWS, VPC and Oracle offering from Public cloud. Our solutions are compliant with Level 1 CSA STAR Registry Self-Assessment. DXC has provided the following CSA STAR Self-Assessment attachments along with this Technical Response. As per RFP Instructions, all attachments have be uploaded in SciQuest as separate files.

- Consensus Assessments Initiative Questionnaire (CAIQ), Exhibit 1 to Attachment B
- Amazon Web Services - STAR Self-Assessment
- Microsoft Azure
 - Microsoft Azure - STAR Self-Assessment
 - MS Azure Attestation
 - MS Azure Certification
 - MS Dynamics CRM Self-Assessment
 - MS Office 365 Self-Assessment
- ServiceNow - STAR Self-Assessment





8.14 Service Provisioning

8.14.1 Describe in detail how your firm processes emergency or rush services implementation requests by a Purchasing Entity.

Outside of approved project deployments, services that are requested by a Purchasing Entity for implementation are generally handled through the mutually defined ITIL Change Management process. Change Management is designed to minimize the impact, risk, and probability of introducing unexpected results when implementing changes to the environment, by employing a structured, controlled set of procedures. The primary goal and value of the Change Management process is to maximize the stability of the environment.

Under the Change Management process, all changes are categorized into one of three types: Normal, Standard and Emergency, the latter of which would be used to address emergency or rush services implementation requests by a Purchasing Entity. Emergency changes are the only change type that is reactive, not proactive, and represent those changes that are required to be applied resulting from (or to prevent) sudden loss or reduction of service. As such, Emergency Changes are typically derived from business-critical incidents.

To support the rapid and reliable deployment of Emergency Changes, the DXC CloudOps team employs a certified team of highly skilled cloud technology resources, who will closely work with the Purchase Entity to understand the client requirement and validate or refine the solution to meet client requirements and best practice standards. The DXC CloudOps team makes optimal use of cloud native features (i.e. Cloud formation/ ARM templates) and industry leading Automation tools to accelerate deployments.

8.14.2 Describe in detail the standard lead-time for provisioning your Solutions.

DXC leverages best-in-class and cloud native tools to deliver a set of flexible services that are designed to enable Purchasing Entities to reliably and rapidly procure the Cloud Services as defined in the Master Agreement. The lead time for the provisioning of the DXC's cloud solutions can vary significantly, as determined by the needs and project timeline of the Purchasing Entity. Once DXC and the Purchasing Entity execute an agreement to implement the DXC's provided solution, DXC operations team can quickly provision and prepare an environment in alignment with the project schedule.





8.15 Back Up and Disaster Plan

8.15.1 Ability to apply legal retention periods and disposition by agency per purchasing entity policy and/or legal requirements.

DXC provides backup retention policies for our clients based on their unique requirements. DXC approves specific retention schedules, based on designs, to meet the client's business requirements. These may include multiple retention periods and various methods of storage, such as disk, tape, and cloud.

By default, DXC's retention policy is 28 days for the daily backup, and multiples of seven for weekly, full backups. We can set extended, online retention for up to 370 days, and offline retention extended for any duration required by the Purchasing Entities for regulatory or other business requirements. These legal retention policies will be discussed and mutually agreed upon with the Purchasing Entity during contract signature.

8.15.2 Describe any known inherent disaster recovery risks and provide potential mitigation strategies.

DXC's advisors and consultants help our clients assess and analyze their current continuity plans, and develop a roadmap to make certain that they have the protection they need. We make certain of a low risk of capacity constraints in our Continuity Recovery Centers by maintaining strict limits on the number of clients assigned to the same leveraged asset (15-to-1), versus other providers who are often unlimited-to-one, with enforcement of exclusion zones). DXC offers 41 robust recovery facilities in 21 countries, including seven DRaaS facilities that help mitigate risk.

Our offerings support industry regulation compliance and security best practices, including ISO frameworks, SOC 2 and IL3. DXC is one of the few global continuity services providers with deep experience in integrating comprehensive continuity solutions for complex, hybrid environments.

DXC has helped numerous clients improve recovery, reduce data loss and increase efficiency. Two examples include:

- Effective cost-saving recovery - A U.S. public sector agency reduced IT costs by 20 percent, improved system availability and reliability, with no Severity 1 or Severity 2 outages, and improved system redundancy to provide nearly 100 percent network uptime.
- Optimized recovery times - A manufacturer of water-heating systems implemented a cost-effective DXC disaster recovery solution to protect its IT-enabled business processes and significantly improve metrics. The company now maintains a recovery time objective of 7.5 hours, instead of five days, and a recovery point objective of 15 minutes, compared to the previous 24 hours timeframe, while requiring only one disaster recovery rehearsal per year.

DXC provides the following benefits to the Purchasing Entities:

- Experience — Providing continuity services since 1984
- Leadership — Named "Leader" by Forrester in four consecutive Disaster Recovery Services Providers Wave industry reports
- Success — Handled more than 966 disaster declarations managed with a 100 percent success rate





- Client focus — Made certain that the ratio of clients to hardware is 15:1 (25:1 in North America)
- Compliance — Supported key industry regulations, including ISO frameworks, SOC 2 and IL3

8.15.3 Describe the infrastructure that supports multiple data centers within the United States, each of which supports redundancy, failover capability, and the ability to run large scale applications independently in case one data center is lost.

DXC Cloud Recovery instances are deployed in three U.S. Continuity Services Recovery Centers in Alpharetta, GA, Colorado Springs, CO, and Littleton, MA.

The Continuity Services Recovery Cloud is deployed in a Continuity Services Recovery Center, built using an architecture similar to that of our Managed Virtual Private Cloud environment. For each contracted customer, we install a host-based asynchronous data replication agent into their environment and use it to facilitate real-time application data replication, operating system data replication and system state information replication into storage resources allocated in the Continuity Services Recovery Cloud.

During standard production, replication occurs from the production environment to the recovery center. All data on production servers is duplicated and routed to an on-site appliance. On-site appliance encrypts data and sends it to the DXC Recovery Center as shown in the following figure:

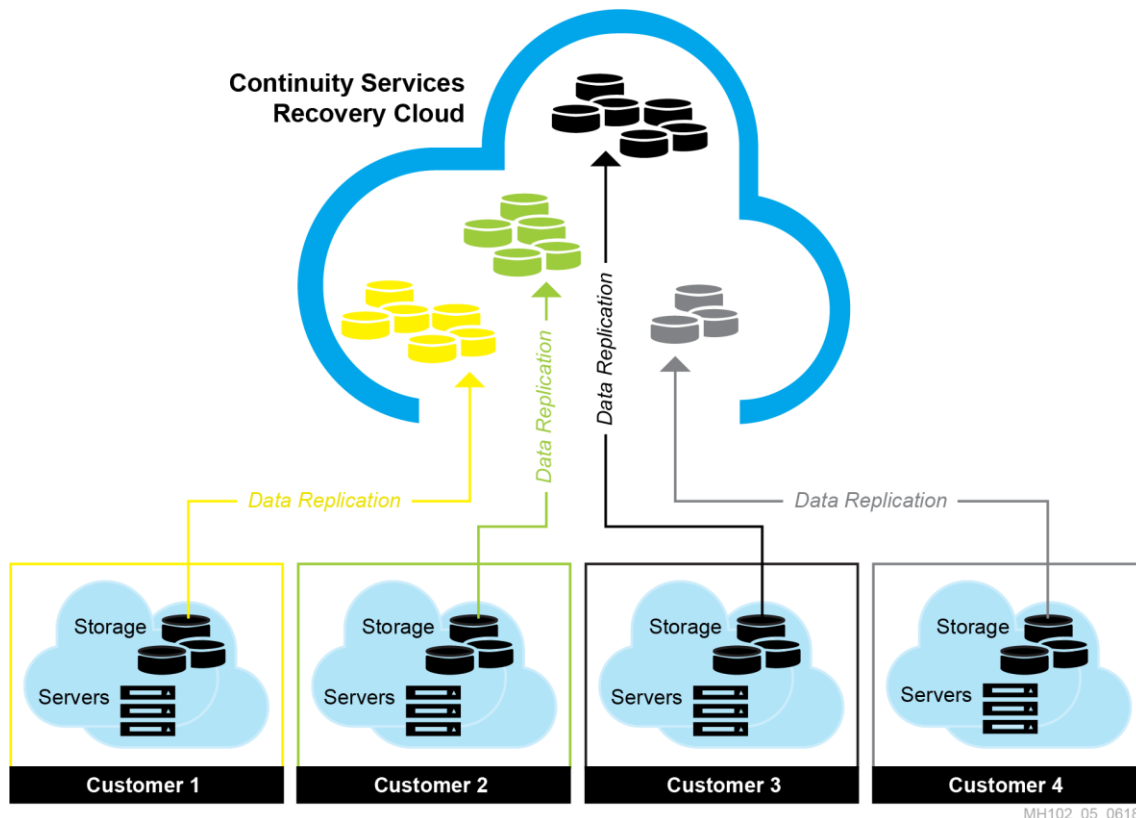


Figure 13: Managed Continuity Service powered by Microsoft - Steady State

If a disaster declaration occurs, DXC will create virtual machines for the customer's protected servers in the Continuity Services Recovery Cloud and will connect to the replicated copies of





the data allowing for rapid resumption of operation. The following diagram shows a single customer making use of this service for recovery after a site failure.

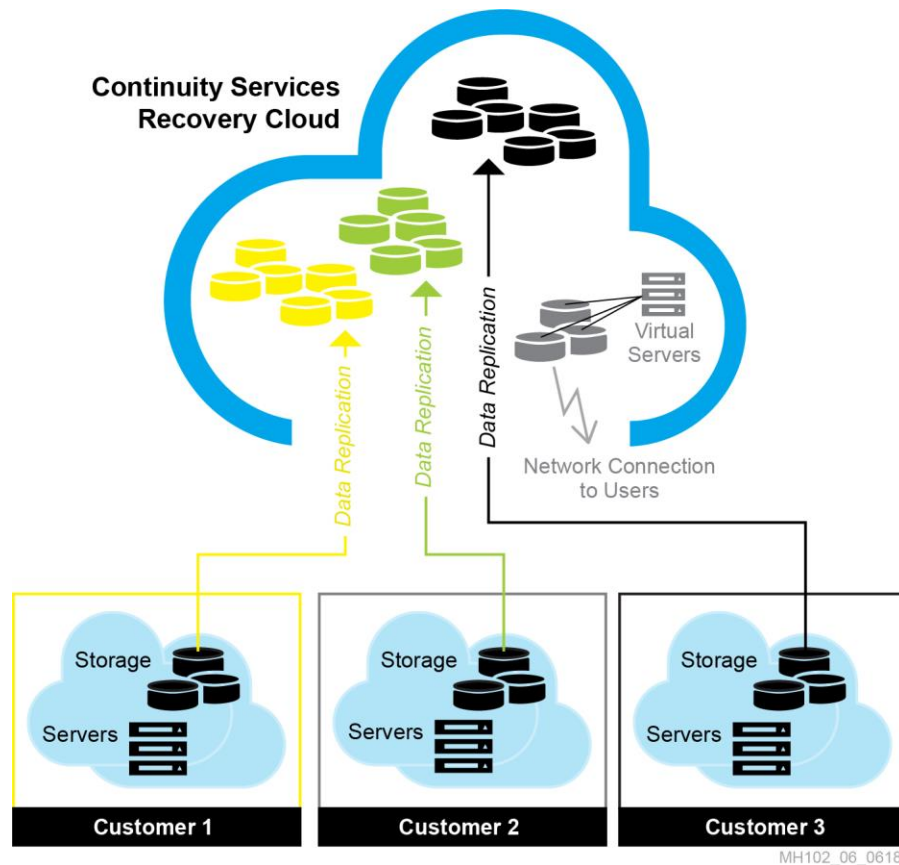


Figure 14: Managed Continuity Service powered by Microsoft Overview - Single Customer Invocation

Managed Continuity Service powered by Microsoft includes data replication, recovery infrastructure, and recovery targets features.

Data Replication

Data replication includes the following:

- For supported configurations, replication of customer data is at a DXC Recovery Center, subject to infrastructure capacity and network bandwidth
- Data replication on a LUN (storage Logical Unit Number) basis
- Replication will operate in asynchronous mode, giving a crash-consistent copy of the customer's data at the DXC Recovery Center
- Replication via an IP, dedicated network, or leveraged connection is based on the customer's requirements. For larger workloads, the recommended connection is a separate circuit for replication, either 1g or 10g, depending on the customer's bandwidth and RPO requirements.





Recovery Infrastructure

Recovery infrastructure includes the following:

- Controlled server fail-over and fail-back
- Customer DNS and Active Directory servers usually hosted in the Managed Continuity Cloud, but, in some limited cases, these services may be replicated using the Microsoft Azure Site Recovery (ASR) software
- Ability to complement Managed Continuity Service by Microsoft with additional Continuity Services offerings, as in a hybrid solution combining traditional disaster recovery with DRaaS
- Full lifecycle support for replication and recovery processes, including monitoring, fail-over, fail-back, rehearsal processes, and support for rehearsal tests
- Additional Storage Option with the ability for customers to specify that additional storage be added to recovered servers at invocation and rehearsal time (e.g., temporary data storage)
- Allocated Hypervisor Option that provides the ability for customers to specify the characteristics of the server hosting their recovered server

Recovery Targets

Recovery targets include the following:

- Target RPO is typically less than 15 minutes
- Target RTO is typically 4 to 6 hours for environments with 200 servers (150 physical servers, 75 TB storage), using "latest time" option for data recovery; larger environments could take significantly longer and require prioritization of the servers being recovered





8.16 Hosting and Provisioning

8.16.1 Documented cloud hosting provisioning processes, and your defined/standard cloud provisioning stack.

DXC cloud hosting provisioning processes includes a complete set of activities, such as deciding server resources, preparing resources, implementing policies, and loading service and supporting tools to make them operational. With Agility at the forefront, it encompasses the way we employ DevOps processes of continuous testing, continuous integration and continuous deployment to speed up the time to delivery for new apps or improvements to existing apps in a multi-cloud environment. With well-defined and documented self provisioning, dynamic provisioning and advanced provisioning processes, purchasing entities receive complete flexibility, cost efficient, fully managed resources with quick return on investment (ROI).

8.16.2 Provide tool sets at minimum for:

1. Deploying new servers (determining configuration for both stand alone or part of an existing server farm, etc.)

DXC provides a set of management tools which includes services such as BeanStalk, CodeDeploy, Cloud Formation, and Resource Manager that allow purchasing entities to deploy new servers and determine configurations for both standalone and part of an existing server farm. With BeanStalk, developers simply upload their applications and the deployment details, such as capacity provisioning, load balancing, auto scaling, and application health monitoring are automatically handled by elastic BeanStalk.

CodeDeploy automates software deployments to a variety of compute services and makes it easier for purchasing entities to rapidly release new features. It helps to avoid downtime during application deployment, and handles the complexity of updating the deployed applications. Purchasing entities can use CodeDeploy service to automate software deployments, and eliminate the need for error-prone manual operations since it scales to match deployment needs.

Cloud Formation provides a common language for purchasing entities to describe and provision all infrastructure resources in cloud environment. Cloud Formation allows purchasing entities to use a simple text file to model and provision, in an automated and secure manner, all the resources needed for applications across all regions and accounts. This file serves as the "single source of truth" for your cloud environment.

DXC leverages Resource Groups (RG) and Resource Manager (RM), which not only simplifies cloud deployment, but also gives purchasing entities a common foundation for its public and private cloud requirements and solutions to standard deployment solutions.

2. Creating and storing server images for future multiple deployments

While DXC helps Purchasing Entities build scalable, highly available, and fault tolerant systems, it also provides consistency, predictability, and integrity across multiple environments. This leads to continuous and more rapid deployment, lower failure and error rates, and faster recovery. Deployment and configuration management tools such as Chef and Puppet are part of the DXC ecosystem.

To fulfill purchasing entities requirement for a simple and consistent multi-region deployment, along with scalability performance and even higher availability, DXC uses machine images that help to achieve these goals.





To create and store server images, DXC follows best practices so that images can be recreated and easily updated in adherence with Purchasing Entities' standards. Best Practices include the following:

- Avoids embedding passwords, private keys, or other sensitive information in machine images.
- Leverages configuration management tools to document and automate images creation and updates
- Creates a library of reusable, modular templates that can be programmatically assembled to create and stores different type of server images for future multiple deployments
- Instruments server images with a standard bootstrapping capability that allows the instance to reference runtime information at launch
- Develops a consistent strategy for tagging to allow for the easy organization and identification of images and their contents

3. Securing additional storage space

DXC provides end-to-end security expertise to protect purchasing entities data, offering three levels of data protection, from replication to full disaster recovery. Purchasing Entities receive secure cloud storage that protects their data infrastructure while they build apps and create better services for their customers. With DXC's standard offerings and solutions, purchasing entities can integrate their on-premises data with their cloud data to form crucial insights, scale globally, and run most demanding workloads while meeting compliance and privacy requirements. Requests for additional storage resources can be made through the DXC-provided self-service portal made available to Purchasing Entities via its diverse offerings and solutions. By using firewalls, authentication, hard zoning and logical unit masking, DXC makes certain that data is safe even in shared storage scenarios, so that only allocated servers and individuals can access your data.

DXC's Storage as a Service (SaaS) is a fully managed service that hosts data in a way that best fits Purchasing Entities' changing business requirements, whether it is in their data center or ours, and in a shared or dedicated environment. SaaS helps Purchasing Entities consume next-generation storage on a gigabyte basis. They can allocate data in different performance and availability tiers depending on usage or value, enabling them to pick the capacity and service levels required.

Instead of a traditional CAPEX model that forces to buy storage capacity in large segments, DXC's SaaS allows you to move to an operating expense (OPEX) procurement model. Paying only for the storage Purchasing Entities use frees up capital to support other business needs.

DXC also offer Backup as a Service (BaaS), which adds protection to storage in a tapeless environment. By adding Object Storage capabilities to storage environment, Purchasing Entities can store multiple data types with universal access at an optimal price.





4. Monitoring tools for use by each jurisdiction's authorized personnel – and this should ideally cover components of a public (respondent hosted) or hybrid cloud (including Participating entity resources).

DXC provides a complete picture of health of the entire cloud infrastructure giving full visibility across all cloud and on-premise tiers, including OS-level and crucial network metrics. Irrespective of purchasing entities running in a public, private, or hybrid cloud, DXC helps to auto-detect & monitoring of cloud components, keeps up with any changes of the dynamic environments and provides complete insights across all cloud and on-premise tiers with a real-time map of dependencies between applications, services, processes, and cloud components. No matter where the purchasing entities are in their cloud journey, below listed are some of the modern monitoring solutions (tools) that DXC leverages enabling different teams - Devops, operations and management and more to begin speaking the same language.

CrowdStrike

As element of the Managed Services, DXC ensures OS-level security of systems with End point protection solution – CrowdStrike Falcon Host. It is SaaS-based and provides advanced detection, prevention, monitoring and search capabilities, allowing users to defend against sophisticated threats and adversaries. It offers remote visibility across endpoints throughout a client's environment, enabling instant access to the "who, what, when, where, and how" of an attack.

What?

- SaaS solution with agents installed on VMs during VM provisioning
 - For existing VMs installed manually by DXC Managed Services with shell/PowerShell
 - Versioned installers stored in a central DXC controlled Storage Account in DXC tenant.
 - Agent updates are performed automatically as soon as agent connects to the CrowdStrike SaaS solution without reboots.
 - There are no 'signatures' updates, since CrowdStrike doesn't use signatures to detect security issues
- VM Endpoint protection – anti-virus, anti-malware, attack detection and response, managed threat identification, and endpoint and application hygiene
- Current the following modules are available – Prevent and Insights
- Monitoring of ports and protocols use (what systems is the end point talking to and what ports are they using)
- Impact on CPU and memory of VM – 25 MB on HDD, ~ 25 MB of RAM, <1% of CPU on average

How?

- Data transfer
 - HTTPS/TLS (AES-128), certificate signed by CrowdStrike (managed with AWS KMS)
 - AES-256 for the payload
- Data deletion upon contract termination - Specific customer identifiable information is purged immediately after contract termination, but certain summary information related to indicators of attack (IOA) may be retained based on the data retention period selected by the customer.
- Any file can be whitelisted by hash in the CrowdStrike management portal





- Data retention – configurable by the customer
- Data export – Falcon Data Replicator will be used to extract raw data to CrowdStrike for which Customer will have access (through API keys). Information about files delivery will be provided through queue.

Who?

- CrowdStrike portal is accessible on ongoing basis only to DXC Managed Services for Azure agents to:
 - Investigate security alerts and incidents
 - Generate reports on Customer environment
- Data access
 - DXC and CrowdStrike Overwatch team have access to the data
 - Access secured with MFA, complex passwords are required
 - CrowdStrike employees are subject to access justification and authentication processes, audit logs, and monitoring as they analyse Indicators of Attack to protect customers
- CrowdStrike alerts are sent to Customer Log Analytics Workspace
- CrowdStrike security events data will be loaded into Customer US Log Analytics Workspace
- General NDA between DXC and CrowdStrike and between Customer and CrowdStrike.

Data collection in CrowdStrike Cloud

CrowdStrike events from sensors monitoring VMs in a client's subscription are collected and analysed in the CrowdStrike Cloud. Every client is assigned a unique Customer ID (CID) by CrowdStrike. This is a security boundary used by CrowdStrike to associate sensor data to an organization for billing and invoicing purposes.

Endpoint protection Telemetry

CrowdStrike collects a large amount of telemetry from endpoints such as dates and times of file execution, failed user logins.

DXC ServiceNow

DXC ServiceNow instance is used for management of all operational activities by DXC Managed Services.

What?

- Multitenant service management SaaS solution
- Resource discovery in CMDB
- Cost blended into the DXC Ongoing Service cost

How?

- Data collected
 - Service management – information required by DXC Managed Service for cloud agents to handle the request
 - Resource discovery/CMDB – Cloud resource information – TLS (HTTPS) is used over internet for DXC ServiceNow to connect to cloud with reader role on service principal to discover resources.





- Data transfer
 - All communication is encrypted, TLS (HTTPS) is used
- Data deletion upon contract termination – data is deleted within 2 weeks from placing the request
- Data export – within 2 weeks from the request placement
- Data retention – data is stored for the duration of the contract
- ServiceNow compliance information is available on their website.

Who?

- DXC ServiceNow is accessible by DXC Managed Service for cloud agents and selected Customer employees (approved by Customer IT Service Owners)
- IOM driven swivel chair mechanism enhanced with Robotic Process Automation is used to synchronize data about requests and incidents that were manually opened in Customer ServiceNow into DXC ServiceNow
- The following type of tickets are synchronized through the same process from DXC ServiceNow into Customer ServiceNow:
 - Security incidents – excluding alerts that were qualified as false-positives
 - Any incident that requires PIM privileges elevation activation to be handled
- Standard global contract between DXC and ServiceNow in place

Log Analytics ITSM Connector

DXC uses the IT Service Management Connector (ITSMC) in OMS Log Analytics to integrate with DXC ServiceNow environments. The connector imports data such as incidents and change requests from ITSM solution into Log Analytics.

With IT Service Management Connector, DXC can:

- Centrally monitor and manage work items for ITSM products/services used across the organization.
- Create ITSM work items (like alert, event, incident) in ITSM from Log Analytics alerts and through log search.
- Read incidents and change requests from the DXC ITSM solution and correlate with relevant log data in Log Analytics workspace.
- Find any unexpected and unusual events and resolve them, even before the end users call and report them to the helpdesk.
- View curated dashboards for deeper insights on incidents, change requests and impacted systems.
- Troubleshoot faster by correlating with other management solutions in the Log Analytics workspace.

At the time of writing, DXC is only using the ITSM connector to inject OMS events into the ServiceNow event management table. The bi-directional synchronization is not currently used although this may change in future DXC Managed Services for Microsoft Azure releases.





Customer Data handling inside DXC ServiceNow

DXC employs ServiceNow's 'Domain Separation' feature. Using this feature, DXC is able to separate data into logically-defined domains. Each DXC customer is setup as a separate domain within DXC's leveraged Service Now instance.

Domain separation allows for data separation and administration (workflow, policy and UI definition) separation.

Members of a domain **only** see the data contained within their domain or the child domains that are lower in the domain hierarchy. This guarantees Customer will not have any visibility into the data of other DXC customers and vice versa, other DXC customers will have no visibility of Customer data.

CloudChecker

CloudChecker is used for billing purposes and for best-practices adherence analysis of Customer cloud environment.

What?

- SaaS solution
- Billing analysis on the per-tag level
- Azure and AWS technical and security best practices compliance reporting – selected best practices checking can be disabled (e.g. so that security best practices are not validated and reported on) (if resource information is ingested)
- Analyze and report on Azure and AWS utilization and cost optimization (if resource information is ingested)
- Azure and AWS resources inventory and configuration reporting (if resource information is ingested)
- Presents discounted prices on the reporting and dashboards
- Cost blended into the DXC Ongoing Service cost

How?

- Data collected:
 - Cost of resources through EA portal
 - Data ingestion can be limited to specific subscriptions
 - Data ingest includes also tags for resources (which will allow for filtering on SupportVendor tag)
 - Resources information (optional, not required for billing) via REST API (TLS/HTTPS), service principal with Azure AD Reader role is required
 - Cloud AD can be used for authentication, RBAC roles are not used for authorization
 - User privileges are managed within the CloudCheckr tool
- Data deletion upon contract termination – data is deleted in 2 weeks from the contract termination
- Data retention – customer data is stored for minimum 180 days and is not configurable by customer
 - Data export – reports can be exported, raw data isn't exportable since CloudCheckr isn't the primary source of data, which originates in Microsoft Azure
 - CloudCheckr compliance information is available on their website.





Who?

- CloudCheckr portal is accessed by DXC Managed Services for team's agents and by Customer. For that purpose Customer is granted with 5 accounts as baseline, for additional accounts, a service request should be raised.
 - Static reports provided to Customer IT and CyberSec team (if resource information is ingested)
- Data access
 - Hosting in AWS and Azure
 - Each user accessing the data has a unique username and password
 - CloudCheckr actively employs a policy of least provisioning, where employees are only granted the minimum system access to perform their assigned job function.
 - CloudCheckr employees cannot decrypt encrypted account data.
- General NDA between DXC and CrowdStrike in place

Symantec CCS-SM

Symantec CCS-SM (Control Compliance Suite – Standards Manager) is used for checking OS compliance for cloud workloads.

What?

- Agents installed on DXC Managed VMs (servers)
- Compliance reporting based on OS configuration data collection
- Cost covered by Customer

How?

- Data collected
 - OS configuration data from VMs managed by DXC (through CCS-SM agent)
- Data transfer
 - All communication is done over cloud backbone and dedicated connection, not through public internet
 - All communication is encrypted, TLS (HTTPS) is used
- Integration method:
 - CCS-SM agents – push
- Data backup/retention – compliance data is captured at the compliance host reporting database

Who?

- Server OS Compliance data accessible by DXC Managed Services (on-prem)
- Reports will be published using standard service reporting process and repositories

Security Center

Security Center is a solution used by DXC Managed Services to deliver ongoing vulnerability monitoring capabilities on the Core Platform level.

What?





- Agents installed on the VM (the same as the OMS agent) for IaaS resources
- Ongoing monitoring of IaaS and PaaS resources for potential security issues

How?

- Security Center dashboard availability
- Integration of security events into Log Analytics Workspace possible (single workspace per subscription)
- Ability to run custom code in response to a security event through security playbooks
- Pure PaaS service, no direct access to the raw data
- Enabled on the subscription level

Who?

- DXC operation & maintenance team agents, Customer IT and Customer CyberSec have access to Security Center and Log Analytic Workspaces used to store and analyze generated data.





8.17 Trial and Testing Periods (Pre- and Post- Purchase)

8.17.1 Describe your testing and training periods that your offer for your service offerings.

DXC Approach to Testing

DXC leverages Best Practices through its Testing Center of Excellence (CoE) framework. The framework, shown below, addresses the various testing services components included in DXC's Best Practices. The DXC project team will collaborate with the Purchasing Entities' Business Leads to finalize their testing needs, along with determining the use of their tools and processes.

DXC will also work closely with the business and testing teams to develop two plans: the initial System Integration Test (SIT) and User Acceptance Test (UAT). DXC will leverage the tools, templates and processes from its Testing CoE, where relevant, to develop the overall UAT test planning and execution.

DXC's pre-configured solution approach offers a ready to use solution pack that includes standard test cases and test scripts to expedite and deliver test types and test cycles.

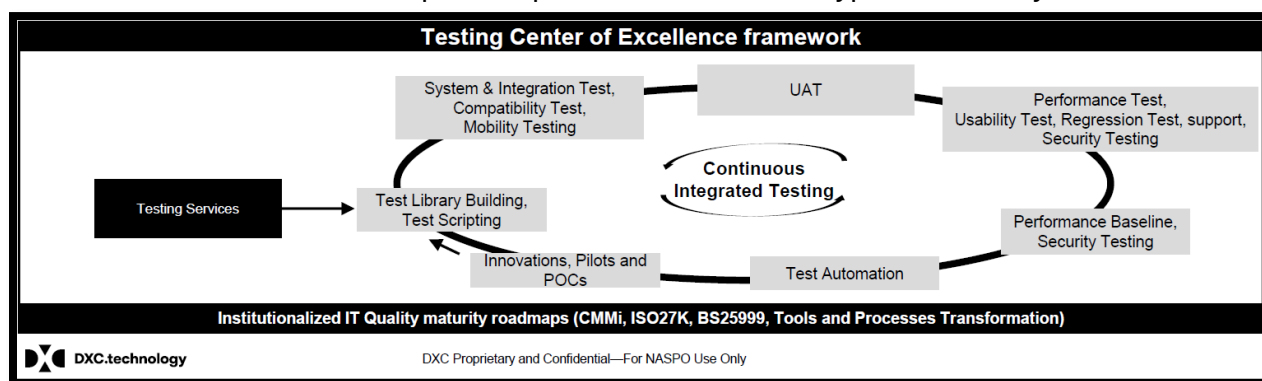


Figure 15: Testing Center of Excellence Framework

DXC Testing and Digital Assurance delivers end-to-end testing services and quality management solutions that help our clients achieve seamless technology transformation, from a traditional to a digital enterprise. DXC's unique IP, Testing as a Service (TaaS) models, advanced test automation assets (frameworks and acceleration tools), and strong partner ecosystem helps deliver faster and optimum solutions. Benefits such as a 50 percent reduction in testing effort through automation frees up resources and assets for other initiatives.

The following figure highlights DXC's testing services offering which is further described below:



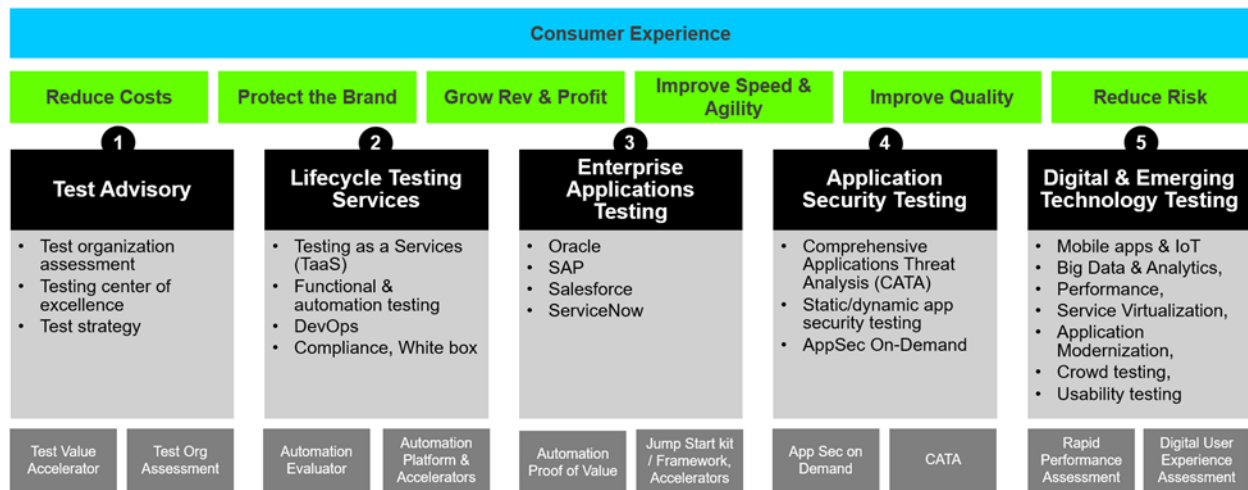


Figure 16: DXC's testing services offering

- DXC's Test Advisory service helps clients determine their testing maturity level. DXC also supports the establishment of a Testing CoE by applying our wealth of knowledge and best practices in the testing space.
- Lifecycle Testing Services provides functional and life cycle testing for various applications to improve the product quality by implementing traditional, agile and DevOps testing methodologies. This helps reduce the cost of testing, using a TaaS model, which speeds up time-to-market through test automation and adhering to standards using compliance testing.
- Enterprise Applications Testing provides functional and non-functional testing services across the life cycle of ERP and COTS projects: implementation, roll-out, upgrade, production support and maintenance through IP, and pre-packaged solutions, tools and accelerators.
- Applications Security Testing provides static/dynamic, mobile application security testing to identify security issues during development, vulnerabilities in deployed apps and data leakage issues. DXC's cloud-based Security-as-a-Service (SaaS) solution enables customers to move from CapEx to OpEx, quickly and accurately evaluates the security of the software.
- Digital and Emerging Technology Testing helps customers roll out quality products and applications leveraging our matured testing services for digital experience and emerging technologies: Mobile, Application modernization, Internet of Things (IoT), Big Data and Analytics, and crowd testing space.

DXC leverages its expansive partner ecosystem to provide the appropriate solutions for its customers based on technology and the specific requirements. DXC utilizes its tool- and vendor-agnostic approach and open source tools, along with other services as appropriate.

Training programs are designed with the Purchasing Entities based on DXC's analysis of the requirements, such as increasing the testing capabilities from the products and services implemented. Training includes the following methods:

- Classroom based – provided in a DXC facility, client site or third-party venue
- Remote instructor-led – led by DXC or our partner vendors
- Online/Computer – scheduled around the customer's availability
- Shadowing/reverse-shadowing – held during transition or user acceptance test periods during the project implementation.





8.17.2 Describe how you intend to provide a test and/or proof of concept environment for evaluation that verifies your ability to meet mandatory requirements.

In collaboration with NASPO and its Purchasing Entities, DXC will establish Proof of Concept (PoC) cloud environments as required or requested by the Purchasing Entities. These activities will be managed as projects where business case are defined, requirements are gathered and duration timeline for the PoC are agreed upon.

Led by DXC certified professionals, our strong partnerships with cloud vendors such as AWS, Microsoft, Oracle and SAP will then create and configure the environments based on the defined requirements of the PoC. DXC will utilize automation to create new cloud environments for PoC and testing on AWS and Azure.

DXC's Cloud Trial program, which includes Proof of Concept, gives enterprises an evaluation period before actually moving mission-critical applications to the cloud. During this time, clients can provision physical and virtual machines, select operating systems, and choose other options through the self-service portal. This approach enables client to "test drive" their applications and experience and evaluate how they perform in the cloud environment. DXC provides PoCs to architect, migrate, test and document cloud PoCs to assist our Purchasing Entities.

Architect Proof of Concept ("POC") Environment

In this environment, DXC will:

- Assist in developing the POC environment
- Assist in developing recommended internal process changes for the cloud environment
- Assist in developing initial internal policies for tagging, metering, provisioning, and de-provisioning for the POC environment
- Assist in developing and delivering initial set of internal standards for services, instances, sizes, and metrics for the POC environment
- Documenting and delivering foundational architectural design for the cloud environment

Migrate Proof of Concept Workload

For the Migrate Proof of Concept Workload, DXC will:

- Assist in documenting the POC migration steps
- Assist in migrating to the newly constructed POC environment
- Assist in demonstrating the release management lifecycle from development to test to production
- Assist in stabilizing the POC environment

Test Proof of Concept

For Test Proof of Concept, DXC will:

- Assist in testing the POC environment
- Analyze the POC test results
- Complete the documentation and initiate hand-over





Documentation

DXC will produce the following documentation:

- Document the POC application architecture and test results
- Document areas of improvement for future execution
- Facilitate hand-over workshop with the customer

Project Schedule

The chart below shows an example of the stages and duration of a typical Accelerator for cloud Engagement project. The actual engagement timeline may vary, based upon customer requirements:

- Assessment – Review of cloud reference architecture
- Initiation – Initiate project and align resources
- Discovery – Evaluate and assess environment
- Design – Identify areas for changes and/or enhancements
- Deployment – Exercise new design and stand-up, and deploy test case
- Wrap Up – Complete and transition

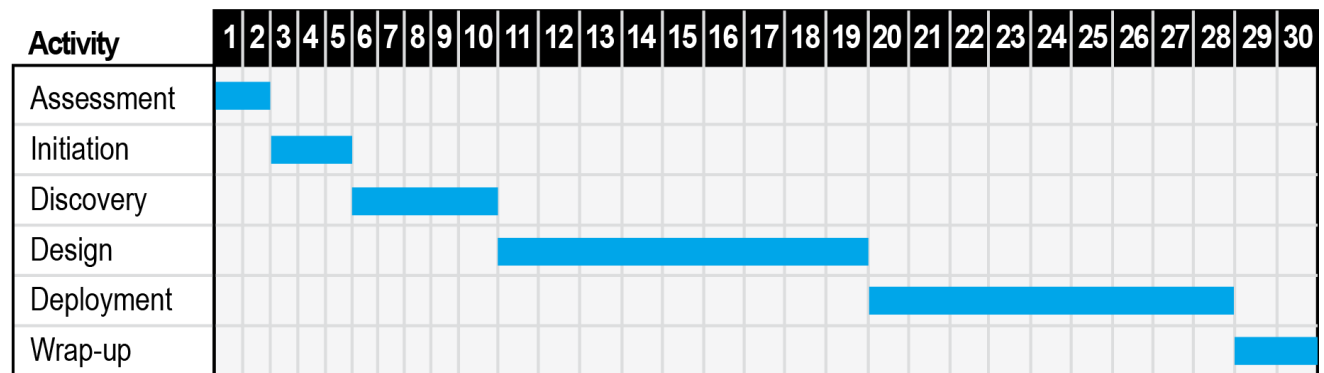


Figure 17: Accelerator for cloud Engagement project Business Days

8.17.3 Offeror must describe what training and support it provides at no additional cost.

Client University is DXC's unique approach that provides our clients training support. Within the Client University, we gather, maintain and disseminate information about the engagement to provide the best service to maintain and enhance applications and processes.

DXC deploys subject matter experts to work with our customer and the Purchasing Entities using the information to build a knowledge repository with customer-specific metadata. While some content is free, Sources of data, such as formal trainings may be costed separately. However, the data from those trainings can be deposited and accessed for free in the Client University.

The DXC subject matter experts categorize the content as courses for efficient knowledge transfer. The following diagram illustrates the process of building Client University:



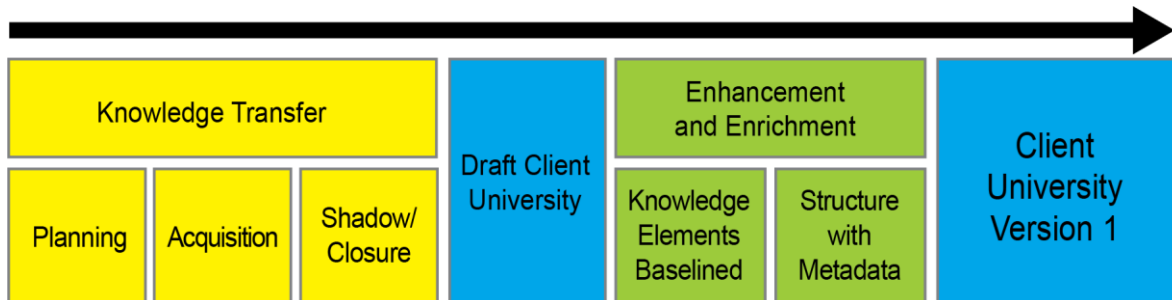


Figure 18: Process of Building Client University

Once transition activities begin during the program start-up phase, we create the basic structure for Client University on a dedicated SharePoint portal site. Courses are then built upon client-specific content in the following streams:

- Stream 1—DXC's account-specific processes
- Stream 2—DXC's account-specific soft skills and culture training
- Stream 3—Client's vision, organization, people, history, and products
- Stream 4—Client's business processes, technologies, and applications

During transition, DXC's knowledge management approach is to capture, complete, and confirm the domain and application knowledge so that critical information assets are maintained. Client University will be used as part of DXC's ongoing training program to make certain that all existing and new resources remain current with the latest processes, tools, technical requirement, guidelines and templates. In accordance with security requirements, Client University will not contain any confidential or business sensitive information. In addition, Client University will be led by a dedicated Dean who will manage the university and coach the engagement staff so they receive the maximum benefit from this initiative.

The graphic below describes the types of knowledge held in Client University. It also shows how the training courses are arranged, as well as the balance of training required for the different roles supporting the Purchasing Entities:

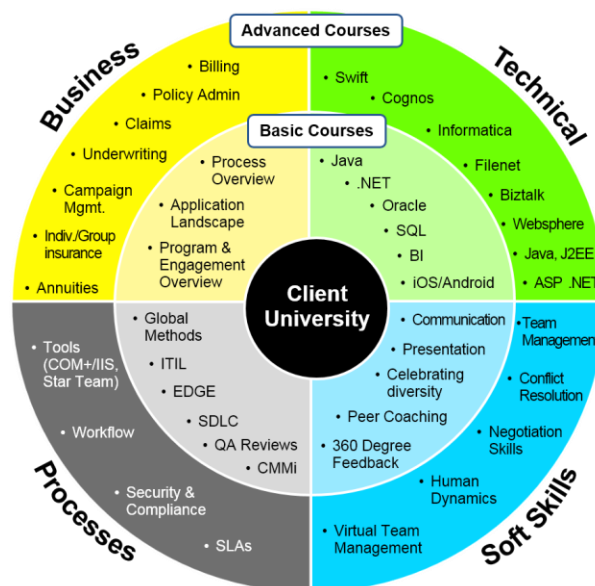


Figure 19: Client University





Client University enables DXC to deliver higher value creation and higher customer satisfaction. The benefits of Client University to the Purchasing Entities include:

- Faster on-boarding of new entrants to the DXC application development, maintenance and testing team to establish a sustainable workforce
- Ability for employees to be matched for a specific role based upon their scores and certification levels
- Opportunity for employees to be “up-skilled”
- Employee morale increased through built-in rewards and recognition
- Increased retention of well-trained employees
- Progressive certification created in an environment where a healthy balance is maintained between achieving service levels and job satisfaction
- Curriculum built by DXC subject matter experts (SMEs) based upon existing expertise and knowledge captured during knowledge transfer from Purchasing Entity.





8.18 Integration and Customization

8.18.1 Describe how the Solutions you provide can be integrated to other complementary applications, and if you offer standard-based interface to enable additional integrations.

DXC's Agility Platform is enterprise software provides a single, consolidated cloud management solution to simplify the complexities of public, private, and hybrid cloud management for large enterprises. The product automates the deployment, management, and governance of cloud applications, development platforms, and a broad range of other enterprise cloud services across hybrid cloud environments. Agility Platform also serves as an integration platform for application release automation to support DevOps and DevSecOps initiatives.

Agility Platform also provides robust cloud governance, beyond simple role-based access control or simple provisioning constraints. DXC provides more than a dozen types of application-centric policy controls out of the box with the Agility Platform, including:

- Regulatory compliance policies
- SLA policies, including compound auto-scaling rules
- Configuration management policies for continuous compliance of workloads after deployment
- Detailed security zone policies, including configuring firewall rules and embedding security agents and utilities
- Lifecycle event policies to customize environments based on software development lifecycle (SDLC) stage
- Orchestration policies
- Entitlement policies

DXC's end-to-end cloud services include application migration and integration in the cloud environment. These integration services use the latest in technical/product standards, including those on the following list:

- Azure Application Gateway, Oracle API Gateway and AWS API Gateway – gateways allow developers to create, manage, and host APIs for the purpose of connecting to other services
- Industry practices, including OAuth 2.0 authorization framework
- Use of RESTful and HTTPS
- Pre-existing IP and schemas aligned to industry models for faster implementations

These standards which are used in deploying and configuring cloud environment and developing applications, in conjunction with our Agile DevOps delivery model, reduces IT delivery cost by as much as 50 – 75 percent and reduction.

The following are descriptions of DXC's services available to assist Purchasing Entities with application integration to our cloud solutions:

DXC Professional Services for Public Sector Cloud Broker

These services manage the use, performance, and delivery of hybrid services from traditional IT to managed, private, and public cloud. This helps our public sector clients transition from traditional IT to the hybrid cloud, while establishing governance over a variety of service providers. As a broker, DXC is able to decouple individual services from providers, and harness the workload services to achieve efficiencies in costs, staffing, and throughput.





DXC Platform as a Service (PaaS) for SAP

This service includes implementation services for SAP S/4HANA and SAP Cloud Solutions. DXC focuses on rapid configuration and deployment of SAP cloud software and supporting infrastructure, including the following list.

- Fast migration to Virtual Private Cloud, or public cloud (Azure or AWS)
- Pre-set configurations that match SLA-related needs
- Support for ECC and S/4 HANA during migration and integration
- Experienced SAP practice to provide Basis guidance for cloud platforms

DXC Digital Transformation Assessment for Oracle Cloud

This service provides high-value Oracle business services for Oracle Cloud, including assessment and advisory, transformation, applications management, automation, robotics, business process outsourcing (BPO), and IT outsourcing (ITO). We have the capability to re-platform, re-architect, and re-host non-Oracle applications within a client's landscape and integrate between client business applications and Oracle Cloud.

DXC Applications Development (AD)

This service provides the Purchasing Entities with the capability, scale, and speed to drive business agility and digitalization. AD provides feature-rich and secure business applications that run on a variety of technology and user platforms, such as on-premises, cloud, mobile, and Internet of Things (IoT).

This service spans architecture, design, development, applications quality assurance, and governance throughout the lifecycle. It includes the list of components that follows.

- Agile Applications Development - Provides the capability and scale to consistently build and implement secure applications with quality and speed
- DevOps - Supports clients across a range of enablement services that range from strategic conversations from where to begin with DevOps to launching proof-of-concept (POC) implementations
- Applications Security - Provides comprehensive, full lifecycle security for our client's applications

Business and Application Integration

DXC's Agility Platform was designed around a lifecycle management framework to make certain that services and applications get provisioned and configured correctly based on the stage of their lifecycle. Services and applications all exist within the context of a lifecycle that defines how they are planned, developed, tested, and released into production.

Business and application integration helps clients create and manage the API and Application Integration capabilities. Business processes, functions and information are integrated to provide services through a portfolio of APIs, operating in cloud environments inside and outside traditional enterprise boundaries.

DXC will also provide business consulting and technical services that cover the entire API and applications integration lifecycle. These services serve as part of an end-to-end enterprise transformation. They can also focus on fulfilling the needs of a specific business initiative or technology project through three phases, described in the following list:





- **Advise**— Business and technical consulting services help the client evaluate and understand the potential opportunities and effects of the emerging digital economy upon their enterprise.
- **Transform**— In this phase, DXC delivers the API and integration solutions and capabilities that clients need to support their business's operation and strategies. This is done through consulting, POCs, solution design and implementation, vendor advice, and ecosystem support.
- **Manage**— DXC applies service management disciplines to manage the client's integration with API services and comprehensive integration services.

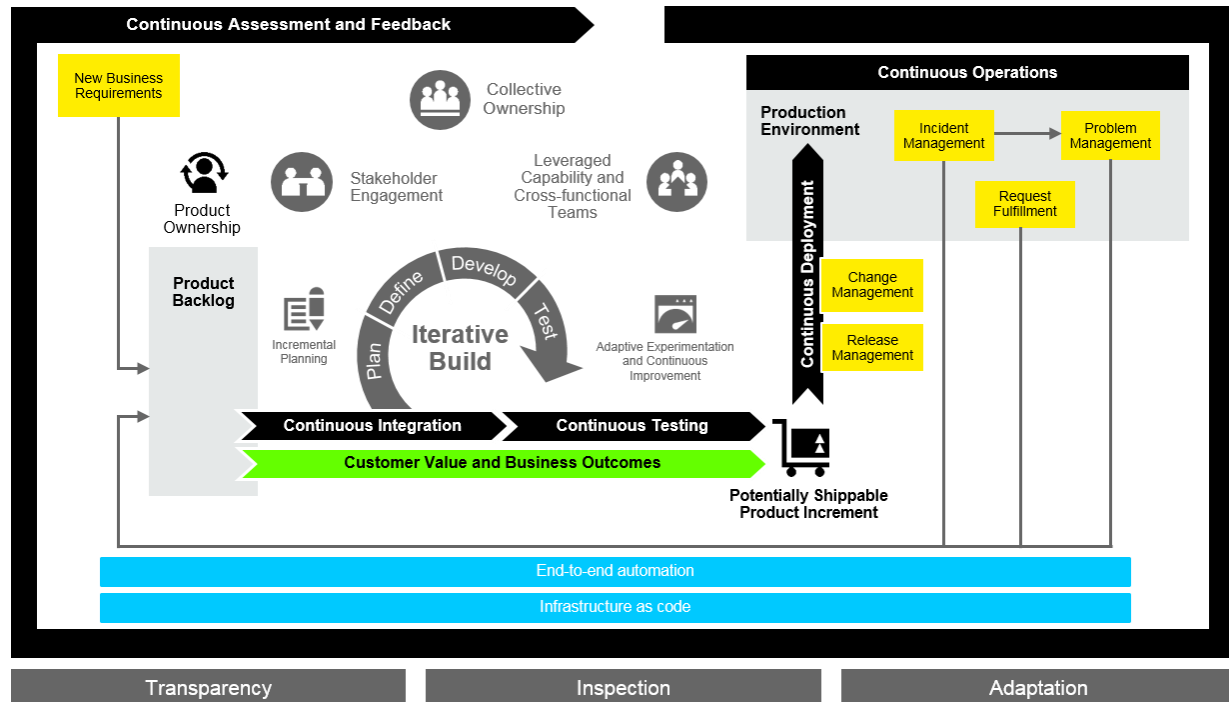
8.18.2 Describe the ways to customize and personalize the Solutions you provide to meet the needs of specific Purchasing Entities.

Agility Platform enables IT organizations to plan, design, and publish service offerings into the Agility Platform Store, third party catalogs, or other systems for consumption by the business. These include not just virtual machine templates, but also complete application environments, services, and packaged applications that can be ordered and consumed on demand.

Using our agile approach, requirements of the Purchasing Entities are gathered and approved, cloud environments are configured according to specification, tested and signed-off prior to being released to deployment.

DXC's Agile Applications Development framework provides the capability and scale to consistently configure the environment, build and implement customized, secure applications with both quality and speed. A diagram of our Agile/DevOps Framework, which leverages Agile, ITIL and continuous delivery standards, follows.





- ▶ Agile, lean practices foster a cultural change, enabling fast and quality delivery of customer value and business outcomes
- ▶ Traditional ITIL processes are enhanced through tighter collaboration and automation
- ▶ Continuous implementation of automation across the entire pipeline improves consistency, quality, and efficiency
- ▶ Engineering practices enable continuous assessment and delivery across business, development, and operations, allowing IT to deliver the right service, at the right time, and for the right price

Figure 20: Agile/DevOps Framework

DXC uses this framework in deploying cloud environments, developing cloud based solutions and custom applications for AWS and Azure.

DXC also offers Application Services for Public Cloud, a suite of application services specifically designed and optimized for AWS and Azure. This service is intended to be a one-stop for advisory, discovery, assessment, planning, data migration, code transformation, testing, and deployment.





8.19 Marketing Plan

Describe your how you intend to market your Solutions to NASPO ValuePoint and Participating Entities.

DXC recommends a two-step approach to market our cloud solutions. First, we will collaborate and strategize with NASPO regarding the best method for promoting cloud solutions within each state. We suggest that, at a minimum, we hold a joint marketing workshop with state procurement officers to determine a cloud solution marketing plan for the states.

Additionally, we will reach out to the CIO of each state to inform them of the new offerings and the catalog that is available. We will work closely with these CIOs to first understand their state's priorities, and then determine how we can best align to those priorities.

In conjunction with these efforts, we will leverage digital marketing campaigns and tools to educate the states on DXC's cloud offerings and capabilities, for example:

- Conference / Industry forums
- Social media promotion (LinkedIn, Facebook, Twitter)
- DXC forums
- Webinars
- Email campaigns
- Media Rich / video assets/ town halls

DXC understands NASPO's objectives for this RFP, and we will work closely with them, as well as the participating states, to promote the use of the Master Agreement.





8.20 Related Value-Added Services to Cloud Solutions

Describe the valued-added services that you can provide as part of an awarded contract, e.g. consulting services pre- and post- implementation. Offerors may detail professional services in the RFP limited to assisting offering activities with initial setup, training and access to the services.

DXC has extensive experience customizing cloud architectures for state, local, federal governments and enterprises and will bring our experiences to bear as we guide NASPO and Purchasing Entities in developing custom cloud solutions. DXC's services offering has a substantial Cloud Services organization and delivery team specifically focused on delivering consulting and migration-based services to our client globally. Some of the core offerings are summarized in the following text:

QuickStart

DXC QuickStarts enables DXC Technology to provide an initial start with the Purchasing Entities. It provides a low cost and low risk entry point requiring limited investment with a short time-to-market. This QuickStarts offering is made available to Purchasing Entities through advisory, as well as through solutions that are pre-priced, preconfigured, and with a fixed scope/deliverable. While the time to benefit for the QuickStarts may be short, these offerings provide continuous value by serving as a starting place for the larger transformation of a Purchasing Entities' journey to the digital enterprise.

Cloud and Workload Advisory Services

DXC Cloud and Workload Advisory Services help clients exploit hybrid technology – including cloud and traditional infrastructure – to innovate and deliver business value while enabling digital transformation. Through workshops, assessments, and roadmaps, our advisors plan and help execute a tailored hybrid IT strategy to meet client business needs. Our advisors understand the client industry, as well as both cloud-based and traditional IT. They follow the latest technology trends to identify options that enable clients to respond to business needs faster. Our advisors assist clients by clarifying options and implications for various types of workloads and also advise clients on plan execution using transformation options.

Through more than 1000 cloud journey workshops, DXC has helped enterprises build, execute, and manage plans.

Cloud and Workload Advisory Services help clients use the best mix of cloud and traditional infrastructure to run their business applications. DXC advisors will help determine workload needs, identify how to transform and migrate applications without disruption, design a secure, stable infrastructure, and enable a smooth transition to new service models.

DXC helps Purchasing Entities thrive on change. We have a clear vision for navigating the future and have met the challenges of innovation many times. Our desire is to closely align with Purchasing Entities' culture and values, bringing our experience and insight to bear on IT challenges in a manner that is both easily digested and sustained.

Cloud Adoption Services

DXC Technology offers a portfolio of application services that help customers maximize business benefits from Cloud. These services are typically deployed in support of three business scenarios: Optimize IT operations, improve business agility, and launch business initiatives.





- **Optimize IT operations:** More efficient projects and fewer operational issues allow employees to spend their time on activities that may offer a greater value to your business. This benefit is different for every organization and difficult to quantify, but people are an organization's biggest asset and Cloud allows organizations to better deploy this asset.
- **Improve business agility:** Getting the compute resources you need when you need them shortens IT projects, requiring fewer FTEs to deliver the project more quickly and at a more predictable time.
- **Launch business initiatives:** It has become much easier to start business innovation initiatives, often enabled by readily available cloud services. Using or combining these services can result in new and innovative business models, generating new value propositions. These cloud native applications and services require new paradigms and design patterns and a strong enterprise architecture function that is able to develop and sustain an agile technology roadmap in the midst of a rapidly evolving landscape.

Cloud Journey

Clients today have many challenges, such as slow time to market, manual processes, large CapEx, and capacity constraints. The following description summarizes the methods and approach DXC uses to help clients overcome their challenges:

Cloud Adoption Process

Well-designed cloud strategies are dynamic. Hence, DXC offers clients an agile three-step Start-Adopt-Run process for cloud adoption, summarized in the following list and illustrated in the figure that follows it.

- **Start** – Cloud journeys are best served by agile frameworks to hit the ground running without spending time on a detailed planning phase, as traditional waterfall projects do. This step focuses on discovery and design of the adoption storyboard.
- **Adopt** – Accelerating, optimizing and lowering risk for cloud adoption comprise the most important step in the journey to cloud. DXC uses agile concepts such as scrum teams, sprints, commit counts, and burnup and burndown charts to start delivering usable products as soon as two weeks into a program.
- **Run** – The ability to deliver, deploy and manage not only the applications but also the platform (IaaS, PaaS) as an integrated unit--wrapped in modern automation frameworks and enabled by a mandatory cultural shift to DevOps--is critical to extracting maximum value from cloud.

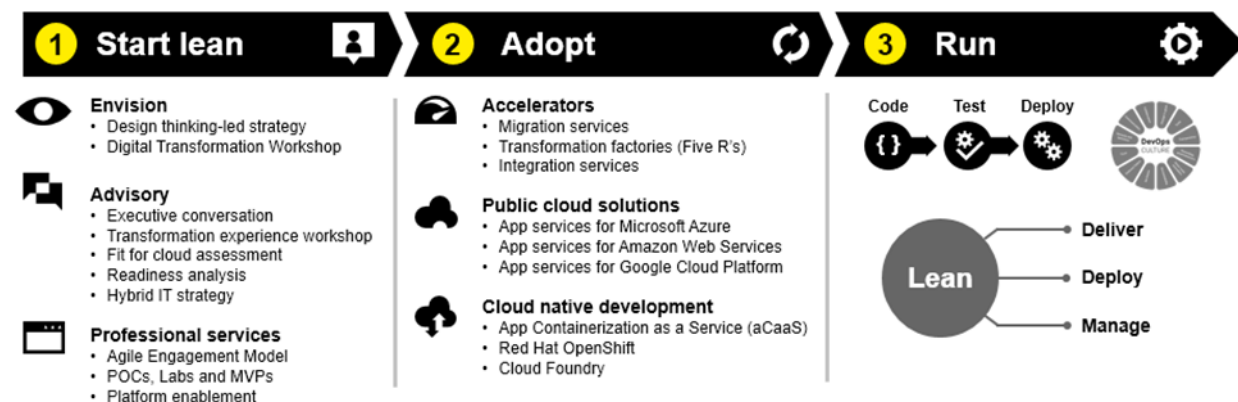


Figure 21: Three-Step Cloud Adoption Process

© 2018 DXC Technology Company. All rights reserved.

Page 107





Agile Scrum Approach

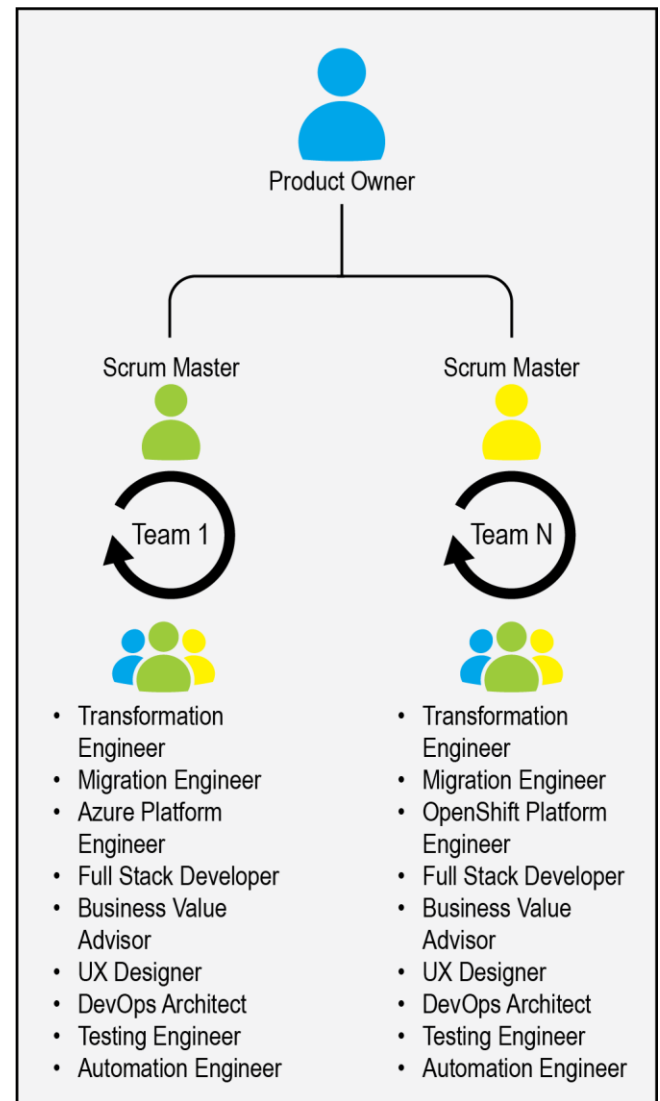
Given the agile nature of a cloud journey and the unique business value demanded from each cloud journey, the most effective approach to driving cloud adoption is through agile scrum. DXC assigns each program at least one product owner who works with the client to determine the precise outcomes and determine the number of scrum teams and the composition of each scrum team to achieve success. Teams are measured by the number of commits and the number of story points completed. Each team also has a minimum of one team member from the client and the remainder of the team is made up of various domain experts including those on the list that follows.

- Application transformation engineer
- Automation engineer (Chef, Puppet, Ansible, etc.)
- AWS-certified architect, developer, and/or engineer
- Azure-certified architect developer and/or engineer
- Business value advisor
- Database specialist
- Development operations architect
- Full stack Java developer
- Full stack .Net developer
- Google Cloud Platform architect, developer, and/or engineer
- Migration engineer (lift and shift expertise)
- Pivotal Cloud Foundry architect, developer, and/or engineer
- Red Hat OpenShift architect, developer, and/or engineer
- Testing engineer
- User Experience (UX) designer

The scrum team composition is reevaluated after each sprint as part of the standard retrospective and adjusted as the needs of the program evolve. The client and DXC are also able to adjust the number of scrum teams as part of the bi-weekly retrospective. These decisions are based on joint analysis of data that is available at the end of each sprint and that DXC shares with the stakeholders.

Over the years, DXC has created a set of standard scrum team templates. Each template addresses a specific need related to cloud that has been addressed successfully in the past. The following five templates are revised when the product owner has the opportunity to work with the client's team: Application remediation; workload migration; containerization; Azure, AWS and GCP applications; and cloud native application development.

Application Remediation: This template provides repeatable, low-risk, high-speed and price-predictable application-transformation treatments that have evolved through thousands of application modernizations. Each treatment features automated discovery/assessment and



MH102_11_0718





automated refactoring/conversion capabilities, many of which are DXC's own proprietary tools. For example, the DXC U2L Assessment Tool enables rapid assessment of application code from UNIX to Linux. We offer the 14 standard treatments on the following list as well as custom solutions.

DXC Standard Application Treatments

• Windows Upgrade • Unix to Linux • VB, ASP to .NET • Access to .NET • Refactor Java	• Refactor .NET • Rehost Legacy • Rearchitect Legacy • Fast Rearchitect • Commercial off-the-shelf (COTS) Upgrade	• Retire • Consolidate • iPaaS • Application Programming Interface (API) Enable
--	---	---

Workload Migration: This template implements the DXC Workload Assessment and Migration Framework for applications that are good candidates for automated lift-and-shift migration. The scope includes:

- application estate discovery
- Automated data analysis to determine optimum workload placement in the target cloud
- Mapping the migration waves based on application affinity
- Just-in-time infrastructure provisioning to minimize waste
- Cutover and data re-synchronization after necessary validation

Containers: The containerization template allows the customer to decompose an application or server into discrete components, such as application servers, web servers, and data services, and then package each component separately as a container. The containers are then shipped to a trusted container registry for deployment. Containers offer the highest level of workload portability and the highest level of system resource use. DXC Application Containerization as a Service (aCaaS) is a versatile container-adoption solution for a range of platforms, including Red Hat OpenShift, Kubernetes, Docker, AWS (ECS, EKS), and MS Azure (ACI, ACS, AKS).

Azure, AWS and GCP Applications: These templates help accelerate, optimize and remove risk from the public cloud journey with a suite of 15 solution sets of application services designed specifically for AWS, Azure, and Google Cloud Platform (GCP). They comprise a full-stack solution for advisory, discovery, assessment, planning, data migration, code transformation, testing, and deployment — all optimized for the three major public clouds.

These templates enable the customer to optimize the public cloud footprint by leveraging platform-native services (PaaS) for both existing applications and new applications built jointly by the customer and DXC scrum team members. Applications that use native services consume significantly fewer public cloud resources and have the ability to use native services, such as monitoring.

Cloud Native Application Development: This template drives the most fundamental shift in how software is designed and developed. Among its many features, the template supports 12-factor compliant applications that are designed to be self-managed while taking full advantage of the target cloud PaaS. It relies heavily on tools and services such as continuous integration, container engines, orchestrators and PaaS, such as Pivotal Cloud Foundry, Red Hat OpenShift, Azure, and AWS. The overall objective is to improve speed, scalability, agility and efficiency.





The following figure depicts the four major technical challenges to cloud native application development and how each of these can be overcome with tried and tested methodologies or tools and services available with this template:

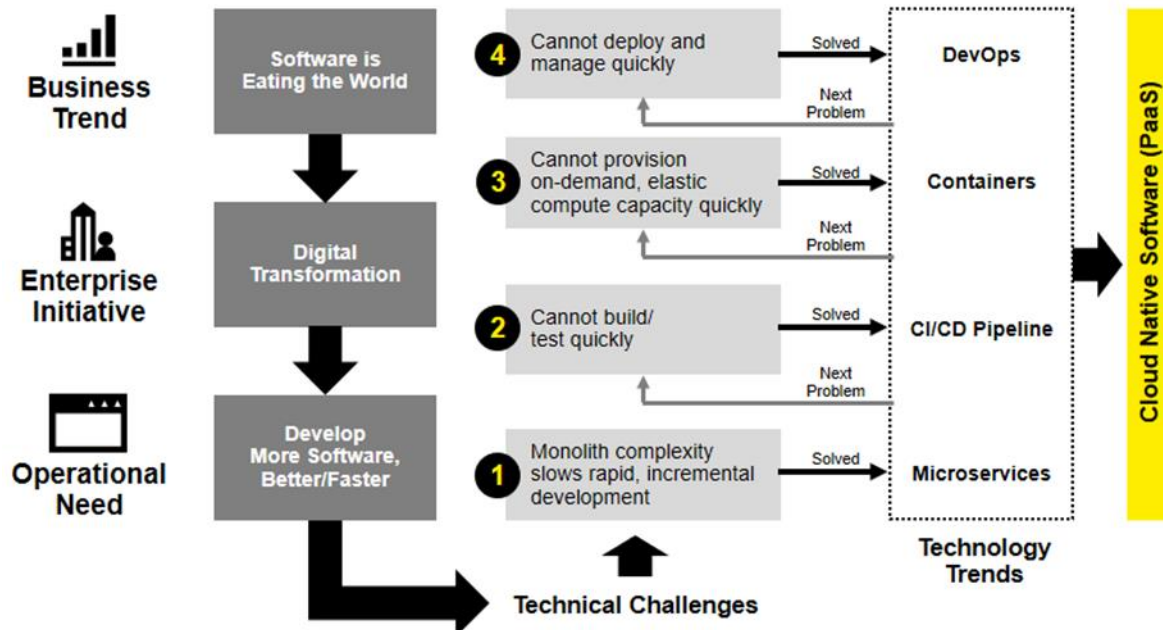


Figure 22: Cloud Native Application Development Challenges

Clients who adopt this template benefit from DXC's "pop-up" labs and on-site training environments as well as user-centric design services and modern programming techniques, such as extreme/pair programming and test driven design.

Managed Platform Operations (Run) Services

While accelerated, optimized, and predictable (low risk) adoption is critical to a cloud journey, DXC realizes that the landing zone for our customers' business-critical applications must to be robust and managed with the same care taken to migrate and develop new applications on the platform. That is why our scrum teams include architects who specialize in helping customers through the operations transformation needed to optimize the Cloud experience and achieve sustainable benefits. Some of the key ingredients in each Cloud Operations solution are captured in the following list:

- Accelerated on-boarding with the accumulated experience of hundreds of cloud deployments
- End-to-end and full stack responsibility across applications and infrastructure. DXC-designed Cloud Ops manage our customers' business solutions and everything used to compose that business solution, including servers, storage, networking, applications, platform native services (PaaS), and automations
- Management of outcomes, instead of service towers
- Maximum automation augmented by predictive analytics; DXC believes that cloud native applications can become self-healing or managed by software and not humans





- Development operations and a cultural morph to drive continuous improvement; we want to create a culture and mindset of collaboration between development and operations

Managed Systems Security Services

As an element of the Managed Services, DXC achieves OS-level security of systems with an end-point protection solution – CrowdStrike Falcon Host. This product is SaaS-based and provides advanced detection, prevention, monitoring and search capabilities, allowing users to defend against sophisticated threats and adversaries. It offers remote visibility across endpoints throughout a customer's environment, enabling instant access to the "who, what, when, where, and how" of an attack. CrowdStrike's attack-related features are described in the following table.

CrowdStrike Attack-Related Features

Attack Element	Description
What?	• SaaS solution with agents installed on VMs during VM provisioning – For existing VMs installed manually by DXC Managed Services with shell/PowerShell – Versioned installers stored in a central DXC-controlled storage account in DXC tenant – Agent updates performed automatically as soon as agent connects to the CrowdStrike SaaS solution without reboots – There are no 'signatures' updates, since CrowdStrike doesn't use signatures to detect security issues • VM Endpoint protection – anti-virus, anti-malware, attack detection and response, managed threat identification, and endpoint and application hygiene • Prevent and Insights modules are currently available • Ports and protocols use monitoring (what systems the end point is talking to and what ports they are using) • Effect on central processing unit (CPU) and memory of VM – 25 MB on HDD, ~ 25 MB of RAM, <1% of CPU on average
How?	• Data transfer – HTTPS/TLS (AES-128), certificate signed by CrowdStrike (managed with AWS KMS) – AES-256 for the payload • Data deletion upon contract termination - Specific customer-identifiable information is purged immediately after contract termination, but certain summary information related to indicators of attack (IOA) may be retained based on the data-retention period selected by the customer. • Any file can be white-listed by hash in the CrowdStrike management portal • Data retention – customer configurable • Data export – Falcon Data Replicator will be used to extract raw data to CrowdStrike to which customer will have access (through API keys); information about files delivery will be provided through queue
Who?	• CrowdStrike portal is accessible on an ongoing basis only to DXC Managed Services for Azure agents to the following: – Investigate security alerts and incidents – Generate reports on customer environment • Data access





Attack Element	Description
	- DXC and CrowdStrike Overwatch team member have access to the data - Access secured with multi-factor authentication (MFA); complex passwords are required - CrowdStrike employees are subject to access justification and authentication processes, audit logs, and monitoring as they analyze indicators of attack to protect customers • CrowdStrike alerts are sent to a customer Log Analytics Workspace • CrowdStrike security events data will be loaded into customer US Log Analytics Workspace • General non-disclosure agreement (NDA) between DXC and CrowdStrike and between customer and CrowdStrike.

CrowdStrike events collected from sensors monitoring VMs in a customer's subscription are collected analyzed in the CrowdStrike Cloud. CrowdStrike assigns every customer a unique customer ID (CID). CrowdStrike uses this security boundary to associate sensor data with an organization for billing and invoicing purposes. CrowdStrike collects a large amount of telemetry from endpoints, such as dates and times of file execution and failed user logins.

Activity Management services using ServiceNow

DXC ServiceNow instance is used for managing the operational activities by DXC Managed Services. ServiceNow's operational activity related features are described in the following table.

ServiceNow Activity-Management Features

Element	Description
What?	- Multi-tenant service management SaaS solution - Resource discovery in configuration management database (CMDB) - Cost blended into the DXC's ongoing service cost
How?	- Data collected - o Service management – information required by DXC Managed Service for cloud agents to handle the request - o Resource discovery/CMDB – Cloud resource information – TLS (HTTPS) is used over internet for DXC ServiceNow to connect to cloud with reader role on service principal to discover resources. - Data transfer - o Communication is encrypted, using TLS (HTTPS) - Data deletion upon contract termination – data is deleted within two weeks of placing the request - Data export – within two weeks from the request placement - Data retention – data is stored for the duration of the contract - ServiceNow compliance information is available on the ServiceNow website
Who?	- DXC ServiceNow is accessible by DXC Managed Service for cloud agents and selected customer employees (approved by customer IT service owners) - IOM-driven swivel chair mechanism enhanced with Robotic Process Automation is used to synchronize data about requests and incidents that were manually opened in customer ServiceNow into DXC ServiceNow





Element	Description
	- The following types of tickets are synchronized through the same process from DXC ServiceNow into customer ServiceNow: - o Security incidents – excluding alerts that were qualified as false-positives - o Any incident that requires PIM privileges elevation activation to be handled - Standard global contract between DXC and ServiceNow in place

Data Import

DXC uses the IT Service Management Connector (ITSMC) in OMS Log Analytics to integrate with DXC ServiceNow environments. The connector imports data such as incidents and change requests from ITSM solution into Log Analytics. With ITSMC, DXC can perform the following tasks:

- Centrally monitor and manage work items for ITSM products/services used across the organization
- Create ITSM work items (like alert, event, incident) in ITSM from Log Analytics alerts and through log search
- Read incidents and change requests from the DXC ITSM solution and correlate with relevant log data in Log Analytics workspace
- Find unexpected and unusual events and resolve them, even before the end users report them to the helpdesk
- View curated dashboards for deeper insights on incidents, change requests and affected systems
- Troubleshoot faster by correlating with other management solutions in the Log Analytics workspace

DXC is currently using the ITSM connector to inject OMS events into the ServiceNow event-management table. The bi-directional synchronization is not available at this time, although this may change in future DXC Managed Services for Microsoft Azure releases.

Customer Data Handling Services Using ServiceNow

DXC employs ServiceNow's Domain Separation feature to separate data into logically-defined domains. Each DXC customer is setup as a separate domain within DXC's leveraged ServiceNow instance. Domain separation allows for data separation and administration (workflow, policy and UI definition) separation. Members of a domain only see the data contained within their domain or the child domains that are lower in the domain hierarchy. This means that the customer will not have any access to the data of other DXC customers, and other DXC customers will have no access to customer data.

Cloud Billing Services Using CloudCheckr

DXC uses CloudCheckr for billing purposes and for best-practices adherence analysis of the customer cloud environment. CloudCheckr's billing analysis and related features are described in the following table:





CloudCheckr Billing and Compliance Reporting Features

Element	Description
What?	- SaaS solution - Billing analysis on the per-tag level - Azure and AWS technical and security best practices compliance reporting – selected best practices checking can be disabled (e.g., so that security best practices are not validated and reported on if resource information is ingested) - Analyze and report on Azure and AWS use and cost optimization (if resource information is ingested) - Azure and AWS resources inventory and configuration reporting (if resource information is ingested) - Discounted prices presented on the reporting and dashboards - Cost blended into the DXC ongoing service cost
How?	- Data collected: - o Cost of resources through EA portal ▪ Data ingestion can be limited to specific subscriptions ▪ Data ingest includes also tags for resources, which will allow for filtering on Support Vendor tag - o Resources information (optional, not required for billing) through representational state transfer (REST) API (TLS/HTTPS), service principal with Azure active directory (AD) Reader role is required - o Cloud AD can be used for authentication, role-based access control (RBAC) roles are not used for authorization - o User privileges are managed within the CloudCheckr tool - Data deletion upon contract termination – data is deleted in two weeks from the contract termination - Data retention – customer data is stored for minimum 180 days and is not configurable by customer - Data export – reports can be exported, raw data isn't exportable, since CloudCheckr isn't the primary source of data, which originates in Microsoft Azure - CloudCheckr compliance information is available on their website
Who?	- CloudCheckr portal is accessed by DXC Managed Services for team's agents and by the customer. For that purpose the customer is granted five accounts as baseline; to obtain additional accounts, a service request should be raised - o Static reports are provided to customer IT and CyberSec team (if resource information is ingested) - Data access - o Hosting in AWS and Azure - o Each user accessing the data has a unique username and password - o CloudCheckr actively employs a policy of least provisioning, where employees are only granted the minimum system access to perform their assigned job functions - o CloudCheckr employees cannot decrypt encrypted account data - General non-disclosure agreement (NDA) between DXC and CrowdStrike in place





Operating System Compliance services

DXC uses Symantec Control Compliance Suite – Standards Manager (CCS-SM) for checking OS compliance for cloud workloads. Symantec CCS-SM's features are described in the following table:

Operating System Compliance Features

Element	Description
What?	- Agents installed on DXC Managed VMs (servers) - Compliance reporting based on OS configuration data collection - Cost covered by customer
How?	- Data collected - o OS configuration data from VMs managed by DXC (through CCS-SM agent) - Data transfer - o All communication is done over cloud backbone and dedicated connection, not through public internet - o All communication is encrypted, TLS (HTTPS) is used - Integration method: - o CCS-SM agents – push - Data backup/retention – compliance data is captured at the compliance host reporting database
Who?	- Server OS Compliance data accessible by DXC Managed Services (on-premises) - Reports will be published using standard service reporting process and repositories

Vulnerability monitoring services

Security Center is a solution DXC Managed Services uses to deliver ongoing vulnerability-monitoring capabilities on the Core Platform level. Security Center's features are described in the following table.

Vulnerability Monitoring Features

Element	Description
What?	- Agents installed on the VM (the same as the OMS agent) for IaaS resources - Ongoing monitoring of IaaS and PaaS resources for potential security issues
How?	- Security Center dashboard availability - Security events integrated into Log Analytics Workspace (single workspace per subscription) - Ability to run custom code in response to a security event through security playbooks - Pure PaaS service, no direct access to the raw data - Enabled on the subscription level





Element	Description
Who?	- DXC operation and maintenance team agents, customer IT, and customer cyber security have access to Security Center and Log Analytic Workspaces used to store and analyze generated data

DXC Services for Office 365

DXC Services for Office 365 is a suite of advisory, transformation, and ongoing management services that assists clients in migrating to and consuming Office 365 cloud-based email and collaboration services. We have developed an extensive set of migration and user-adoption capabilities to be sure users and data migrate quickly and seamlessly to the cloud. In addition, DXC has partnered with Microsoft to develop a tightly integrated, end-to-end delivery model so clients can get the support they need quickly and focus their efforts on running their businesses.

Value proposition

DXC Services for Office 365 is a comprehensive set of advisory, transformation and management services that helps enterprise and public sector clients rapidly identify and overcome challenges in moving to Office 365. DXC's significant experience and our deep, 30-year partnership with Microsoft have contributed to creating proven migration methodologies and processes that safely move users and data to the cloud. Clients benefit from accelerated time-to-value of their Office 365 investment, as well as an integrated, co-located delivery team that provides rapid incident response and resolution to minimize business disruption. Some examples of how our clients have benefitted include:

- Cost savings—DXC is helping a client centralize a globally distributed and fragmented email and collaboration platform to reduce spend by 25 percent
- Fast, reliable migrations—DXC identified known migration blockers early on during a client's migration to Office 365, resulting in a six-month acceleration and a 46 percent cost savings
- Improved productivity—DXC helped a client deploy new productivity tools with a data-governance structure, allowing users to collaborate better and reduce time to market for new services by 15 percent

DXC O365 Services

Highlights of DXC's O365 Services include rapid support, expertise, migration experience, comprehensive portfolio, and goals shared with Microsoft, as summarized below:

Rapid support—An integrated, co-located Microsoft/DXC delivery team provides deep access to operational and engineering teams, integrated delivery processes, and regular operations reviews for rapid incident escalation and resolution.

Expertise—DXC has more than 25 years of experience supporting millions of users' email and collaboration workloads, and a highly trained workforce that includes 12,000 Microsoft certified professionals, 60 Office 365 Microsoft Certified Solutions Associates (MCSAs), and 12 Microsoft Most Valuable Professionals (MVPs).

Migration experience—DXC has successfully transitioned more than 1.5 million user workloads to Office 365, as well as performed millions of migrations to updated versions of on-premises Exchange and SharePoint. All of the lessons learned from those projects, including DXC's own





Office 365 implementation, have been captured and shared with implementation teams so our clients can benefit from that experience.

Comprehensive—DXC's extensive portfolio and experience helps clients make certain their infrastructure ecosystem and users are ready for the change to cloud-based services. We provide assistance for Office 365 as well as for the supporting ecosystem, including: authentication, network, hybrid on-premises services, Microsoft licensing, devices, applications, and Service Desk.

Microsoft/DXC shared goals—Executive-level sponsorship and shared goals enable DXC and Microsoft to work together to migrate enterprise clients successfully to new cloud services and make sure they receive the rapid support they require.

Implementing Office 365 can be a substantial challenge for clients because of the logistical and technical complexities it introduces to most IT environments. DXC helps clients of nearly any size identify and overcome challenges and complexities in moving email and collaboration workloads to Office 365. Our service provides fast and safe implementations as a result of our proven methodologies and vast experience. Users can get the support and training they need to realize their productivity potential on Office 365 combined with DXC's rapid incident response and resolution, and end-user training and adoption services.

DXC Solutions for Microsoft Dynamics 365

DXC Technology advances its position as a leading Microsoft Dynamics 365 global independent systems integrator partner with acquisitions of Sable37 and eBECS. With the acquisition of Sable37, a leading Microsoft Dynamics 365 Value Added Reseller (VAR) and global independent software vendor of cloud-based industry solutions for Dynamics 365 and eBECS, this Microsoft Gold Partner delivers total Microsoft business solutions and managed services.

DXC can help purchasing entities digitally transform their business. The additions of Sable37 and eBECS represent a key part of DXC Eclipse's strategy to lead the Microsoft partner marketplace, accelerate the digital transformation journey for DXC's Microsoft clients, and extend the organization's cloud-based industry offerings globally. With DXC Eclipse, which is one of the largest, independent Microsoft Dynamics systems integrators in the world delivering Microsoft Dynamics 365, ERP, CRM, business process, analytics, and collaboration solutions on premises and in the cloud, DXC is uniquely positioned to offer unparalleled service, innovation and opportunity for customers, partners and employees

DXC Solutions for Microsoft Dynamics 365 bring together enterprise resource planning (ERP) and customer relationship management (CRM) cloud offerings in one cloud service with specific, purpose-built applications for key business processes, such as sales, field services, operations, and customer service creating a more collaborative, interactive user-centric enterprise. Across multiple industries, DXC helps Purchasing Entities better manage their internal operations and engage with their customers. Our deep industry knowledge coupled with our preconfigured vertical industry solutions and accelerators enable us to assist Purchasing Entities with their digital transformation.

Dynamics 365 is seamlessly integrated with Microsoft's entire technology stack including their solutions for productivity, cloud and data for end-to-end digital transformation across your entire business and DXC provides flexible solution options to meet your business needs.





8.22 Supporting Infrastructure

8.22.1 Describe what infrastructure is required by the Purchasing Entity to support your Solutions or deployment models.

DXC Technology offers Managed Connectivity Services that combine our systems integration expertise with the network infrastructure experience of AT&T to transform and manage purchasing entities' network infrastructure. DXC helps Purchasing Entities to simplify managing network resources, increase efficiency, and drive down costs, understanding that next-generation technologies are creating a virtualized environment where network, platform and applications are indistinguishable to employees and customers.

For onboarding cloud services on public cloud, DXC will provision the required and supporting infrastructures as part of solutions. Depending on the solution and requirement, DXC may require the Purchasing Entity to bring the connectivity from their data center to the cloud Hub. If the Purchasing Entity requires a dedicated network link to access the cloud services, DXC can work with our network partners, such as AT&T and Verizon, to design and provision the necessary connectivity.

Next-generation technologies are creating a virtualized environment where network, platform, and applications are indistinguishable to employees and customers. Enterprise IT must gain the ability to manage the technology stack from top to bottom in this environment.

DXC network services include features critical for today's digital business:

- Global connectivity provides a standard, highly secure, SLA-driven, competitively priced solutions to clients in all regions.
- On-demand connectivity enables clients to take advantage of DXC's market presence to buy what they need when they need it, while maintaining the security and quality they expect.
- Third-party connectivity allows clients to use the transport providers they prefer while holding DXC responsible for overall solution integration.

For example, DXC supports several third-party solutions that address the following requirements, allowing DXC to maintain overall solution responsibility.

- DXC Carrier Management Services – DXC provides carrier provisioning and inventory, carrier governance, carrier broker services, and telecom expense management on our Purchasing Entities' behalf.
- DXC Rapid Connect – DXC provides pre-staged vendor bandwidth at multiple DXC data centers. This offering can be viewed as a force multiplier, providing quick and tested infrastructure deployment for our traditional and cloud services. Rapid Connect is an Enterprise Build Services Program.

DXC's partnership with AT&T NetBond services provides on-demand, secure AWS Direct Connect for clients to extend their corporate network directly to the AWS cloud. DXC's partnership with Microsoft allows to leverage ExpressRoute that can extend Purchasing Entities' on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider. With ExpressRoute, Purchasing Entities can establish connections to Microsoft cloud services, such as Microsoft Azure, Office 365, and Dynamics 365.

DXC and AT&T have combined to develop a unique business model, capitalizing on DXC's leadership in next-generation solutions and services with the industry-leading global networking capabilities of AT&T. Together, we create offerings that are market-ready and available for global deployment at scale.





8.22.2 If required, who will be responsible for installation of new infrastructure and who will incur those costs?

DXC's Delivery team will be responsible for provisioning cloud services and onboarding on OEM infrastructures. Alternatively, DXC is open to leveraging existing Purchasing Entity vendors who provision them. The labor rate cards will be shared in the Attachment F Cost Proposal section for each capability. We would like to work with each Purchasing Entity at the time of finalizing the proposals responses to determine the number of man hours or cost required.





Attachment G – Identification of Service Models Matrix

Offerors must complete the following form to identify the service models your firm offers under this RFP. You may provide a list of the different SaaS, IaaS, and/or PaaS services that you offer, including the Categorization of Risk that you have the ability to store and secure. This document is to provide purchasing entities and eligible users a quick snap shot of the cloud solutions your firm provides.

Service Model:	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered:
SaaS 1. Application - Custom Development using .NET (Azure) Java (AWS) 2. Application - Testing and Digital Assurance 3. DXC Migration Services for Oracle Cloud 4. ServiceNow Applications 5. Emerging Practices – Salesforce 6. Emerging Practices – Workday 7. Workplace AD - Integration, Migration 8. Workplace - O365 on Azure 9. Workplace- Skype for business 10. Workplace - Mobility Service 11. Security Services- Consulting service 12. Microsoft Dynamics 365	X			Public Cloud
SaaS 1. Workplace- Desktop/Application Virtualization 2. DXC Migration Services for Oracle Cloud 3. Application - Testing and Digital Assurance	X			Community Cloud
SaaS 1. DXC Migration Services for Oracle Cloud	X			Private Cloud
IaaS 1. Oracle As Service 2. Cloud Security Advisory Services 3. Managed Cloud Access Security Broker 4. On-Demand Workload Protection	X			Public Cloud





5. Infrastructure & Endpoint Security Advisory Services 6. Managed Endpoint Threat Detection & Response 7. DXC Managed Service for Azure 8. DXC Managed Service for AWS 9. Cloud & Platform Advisory Services				
IaaS 1. Virtual Private Cloud 2. Managed Services for VMware 3. Workplace AD-Integration, Migration 4. Workplace-Desktop/Application Virtualization 5. Oracle As Service 6. On-Demand Workload Protection 7. Cloud & Platform for Advisory Services	X			Community Cloud
IaaS 1. Virtual Private Cloud 2. Managed Services for VMware	X			Private Cloud
PaaS 1. PaaS for SAP on AWS 2. PaaS for SAP on Azure 3. Managed Container PaaS for RedShift	X			Public Cloud
PaaS 1. PaaS for SAP	X			Community Cloud
PaaS 1. PaaS for SAP	X			Private Cloud





Location

1775 Tysons Blvd
Tysons, VA 22102

www.dxc.technology

About DXC Technology

DXC Technology (DXC: NYSE) is the world's leading independent, end-to-end IT services company, helping clients harness the power of innovation to thrive on change. Created by the merger of CSC and the Enterprise Services business of Hewlett Packard Enterprise, DXC Technology serves nearly 6,000 private and public sector clients across 70 countries. The company's technology independence, global talent and extensive partner network combine to deliver powerful next-generation IT services and solutions. DXC Technology is recognized among the best corporate citizens globally. For more information, visit www.dxc.technology.

© 2017 DXC Technology Company. All rights reserved.

Attachment D

Page 122 of 122



Attachment E: Service Offering EULAs, SLAs

Azure

The overall service levels provided to the client comprise the following suite of service layers:

Azure Service Layers Suite

Layer	Service SLA	Notes
Infrastructure	Microsoft (typically 99.95%)	Applies regardless of whether Enterprise Agreement (EA) or Cloud Service Provider (CSP). Service levels can be changed, depending upon the design availability sets or availability zones. If no availability set is configured, the base Microsoft availability may not be available.
Infrastructure support	Microsoft – dependent on the level of support taken out	If the client has an EA, their support contract should accompany this SLA, and we will raise tickets into Microsoft based on their support contract. If the client is CSP, the support request is raised to Microsoft based upon DXC's support contract with Microsoft. For all EA clients, DXC recommends opening a case directly with Microsoft
Managed Service	SLOs added into the Solution pack for Managed Service (will be future SLAs)	This is the service level that DXC commits to for managed services.

AWS

DXC, as the reseller of the AWS services, will provide the support for both the CS for AWS service and for the AWS environments that DXC is reselling to the Purchasing Entity. The Purchasing Entity will not contact AWS directly for support.

Response Time SLA

1. If DXC fails to respond to a Priority 1 or Priority 2 incident within the Response Time SLAs, DXC will pay to the Purchasing Entity a service credit of \$250 U.S. for each incident for which the Response Time SLA was not met ("Response Service Credit"). Multiple, related incidents will count as a single incident for the purposes of measuring Response Time SLAs.
2. DXC will pay a maximum of three Response Service Credits in any given month.
3. DXC will not pay Response Service Credits for Priority 3 and Priority 4 incidents or for incidents that are incorrectly classified as Priority 1 or Priority 2 by the Purchasing Entity.





4. "Respond" means DXC will begin working on the incident reported by the Purchasing Entity as evidenced by documentation in the CS for AWS Portal - for example, by hot hand-off, by calling the user to clarify the issue, or by starting a technical investigation. Responding does not mean that DXC will resolve an incident within the Response Time SLAs.

Severity Descriptions

The following priority levels are used to classify incidents for the CS for AWS service that are reported by the Purchasing Entity to DXC using the methods set out in function ID SD5:

1. Priority 1: Complete loss of function so that Purchasing Entity is unable to access the CS for AWS portal, or application(s) located within the AWS environment; or a critical security event. Incidents reported by email may not be classified as Priority 1.
2. Priority 2: Degradation of CS for AWS Portal and/or service performance that has a material adverse effect on either the CS for AWS Portal or AWS environment based applications performance, but does not result in an outage; or a circumstance that, in DXC's reasonable discretion, if not corrected, could result in an outage or loss of Purchasing Entity data; or a major security event that degrades or could degrade service.
3. Priority 3: No impact on end users or any degradation of service; or no material degradation or loss of a noncritical business function; or services are functioning normally, but an individual experiences a problem; or a noncritical security event that does not impact performance of the services.
4. Priority 4: A service request that is not a problem with the CS for AWS Service or the AWS environment (e.g., Purchasing Entity seeking advice on the best use of AWS features or functions).

Response Time SLA and Support Process

The following table sets out the Response Times SLAs for the CS for AWS service:

CS for AWS Service Response Times SLAs

Priority Level	Process of Purchasing Entity Submission and DXC Response	Response Time SLA
1	If a Purchasing Entity representative calls the DXC Service Desk, the ticket is logged real-time in the CS for AWS Portal and DXC will respond by a hot hand-off to the appropriate technician while Purchasing Entity representative is still on the phone. If DXC has received notice through a monitoring alert or Purchasing Entity has opened the ticket by any means other than calling the DXC Service Desk or by email, DXC will send a notification to the Purchasing Entity's contact person/mailbox.	<15 minutes
2	If a Purchasing Entity representative calls the DXC Service Desk, the ticket is logged real-time and DXC will respond by a hot hand-off to the appropriate technician while Purchasing Entity representative is still on the phone. If DXC has received notice through a monitoring alert or Purchasing Entity has opened the ticket by any means other than calling the	<75 minutes





Priority Level	Process of Purchasing Entity Submission and DXC Response	Response Time SLA
	DXC Service Desk, DXC will send a notification to the Purchasing Entity's contact person/mailbox	
3	Upon Purchasing Entity's contact to the DXC Service Desk, the ticket is logged real-time and DXC will respond by forwarding to an appropriate technician for follow up.	<4.25 hours
4	Upon Purchasing Entity's contact to the DXC Service Desk, the ticket is logged real-time and DXC will respond by forwarding to an appropriate technician to follow up.	<1 business day

VPC Service Level Agreements

Managed VPC provides Service Level Agreement (SLA) from 99.0% to 99.95% across the Service Environment for Tier 2 to Tier 4. Availability is measured monthly.

NOTE: Only the Tier-2, Tier-3 (option B) and the Tier-4 (option C) are available in the current version of the NextGen Portal.

VPC Service Level Agreement Tiers

	Tier 2 (Option A)	Tier 2 (Option B)	Tier 3 (Option A)	Tier 3 (Option B)	Tier 4 (Option A)	Tier 4 (Option B)	Tier 4 (Option C)
Data Center Type	Single	Single	Single	Single	Dual	Dual	Dual
Server Type	1 Physical Server	1 Virtual Server	2 or more Physical Servers	1 Virtual Server	2 or 3 Physical Servers	4 or more Physical Servers	1 Virtual Server
Cluster Type	None	Hypervisor Cluster	OS Cluster	Hypervisor Cluster	OS Cluster	OS Cluster	Hypervisor Cluster
Server Management	Managed or Unmanaged Server	Managed or Unmanaged Server	Managed Server	Managed or Unmanaged Server	Managed Server	Managed Server	Managed or Unmanaged Server
SLA Applies to:	Physical Server	Virtual Server	OS Cluster	Virtual Server	OS Cluster	OS Cluster	Virtual Server
Service Level	99.0%	99.90%	99.95%	99.95%	99.99%	99.999%	99.95%

Oracle Cloud SLA

Oracle Cloud is the only service to offer end-to-end SLAs covering availability, manageability and performance services.





- **Availability** -Purchasing Entity cloud workloads will be in continual operation because of Oracle's commitment to uptime and connectivity.
- **Manageability** - The elasticity and configurability of infrastructure is one reason why organizations move applications to the cloud. Purchasing Entity services need to be continuously manageable to deliver this benefit. Oracle is the first cloud vendor to offer manageability SLAs, enabling Purchasing Entities to manage, monitor and modify their resources.
- **Performance** - IaaS resources should be accessible and consistently perform as customers expect. Oracle is the first cloud vendor to guarantee performance, which means Purchasing Entities can rely on the infrastructure for enterprise applications.

Enterprises demand more than just availability from their cloud infrastructure. Mission-critical workloads also require consistent performance, and the ability to manage, monitor and modify resources running in the cloud at any time.

The following graphics further describe availability, manageability and performance services:

Availability

Service/Resource	Measurement	Monthly SLA Percentage	Oracle service credit if SLA breached
Compute	Region Unavailability	Greater than or equal to 99.99% uptime	10%
		Greater than or equal to 99% uptime	25%
Block Volumes	Region Unavailability	Greater than or equal to 99.99% uptime	10%
		Greater than or equal to 99% uptime	25%
Object Storage	API error rate	Greater than or equal to 99.99% uptime	10%
		Greater than or equal to 99% uptime	25%
FastConnect	Private Connectivity	Greater than or equal to 99.99% uptime	10%
		Greater than or equal to 99% uptime	25%

Manageability

Service/Resource	Measurement	Monthly SLA Percentage	Oracle service credit if SLA breached
Compute	API Error rate	Greater than or equal to 99.99% uptime	10%
		Greater than or equal to 99% uptime	25%
Block Volumes	API Error rate	Greater than or equal to 99.99% uptime	10%
		Greater than or equal to 99% uptime	25%
Database	API Error rate	Greater than or equal to 99.99% uptime	10%
		Greater than or equal to 99% uptime	25%





Performance

Service/Resource	Measurement	Monthly SLA Percentage	Oracle service credit if SLA breached
Compute local NVMe drive	Disk IOPS	Resource performance greater than 90% of published performance 99.9% of the time	10%
		Resource performance greater than 90% of published performance 99% of the time	25%
Block Volumes	Disk IOPS	Resource performance greater than 90% of published performance 99.9% of the time	10%
		Resource performance greater than 90% of published performance 99% of the time	25%
Network	Network Performance	Resource performance greater than 90% of published performance 99.9% of the time	10%
		Resource performance greater than 90% of published performance 99% of the time	25%

Service Desk - Contact Channels and SLA

A Service Desk contact is a client-initiated communication, submitted through one of four contact channels - telephone, web-based Portal interface, email form, or chat - which reports an incident or requests a service and requires an agent to record or read, research, find a resolution, and then respond to the client request. The contacts are recorded and tracked for Service Desk billing and service performance reporting purposes. There is not necessarily a one-to-one correlation between a submitted communication and a Contact, because a single submission may contain multiple requests for assistance. In this case, each item is logged as a Contact and becomes a billable unit of work.

The standard volume of contacts to a Service Desk is one contact per month. This may be adjusted based on client data and complexity. There is no standard division of contacts among the four channels as this is dependent on client's industry, user maturity, and other factors.

The Service Desk Offering provides various standard SLAs for the contact channels, as shown in the following figure:

Service Desk Offering Channel SLAs

Channel	Primary SLA	Secondary SLA(s)
Voice	80% in 60 seconds	80% in 30 seconds
Email	95% in 80 seconds	Multiple
Chat	80% in 120 seconds	80% in 60 seconds 80% in 45 seconds
Portal	95% in 12 hours	Multiple





VDA Service Availability (in a DXC-managed Data Center)

The Target Availability Service Level for the VDA Services hosted at a DXC service location or at a customer site is 99.85% availability during the total minutes in each measurement period of one calendar month starting on the first day of the month following the start of user onboarding.

Availability is defined as the services being available for and capable of delivering the virtual desktops and hosted shared applications to users. Availability is calculated as a percentage (rounded to two decimal places) where the measurement period in the following list applies:

$$\frac{[(Actual\ Services\ Available\ Minutes) + (Permitted\ Outage\ Minutes)]}{(Total\ Minutes)} \times 100$$
and where:

1. Actual Services Available Minutes is calculated as 24 x 60 x the number of days in the measurement period minus total outage time in that measurement period
2. Permitted Outage Minutes means the period in minutes for all permitted outages during a measurement period
3. Total Minutes is calculated as 24 x 60 x the number of days in the measurement period
4. Outage means the services are unavailable to more than 10% of the active users attempting to access them. Following resolution of an incident, DXC will calculate the total number of possible active users attempting to access the services based upon the timing and location of an outage.

Outage Time means the time in minutes between the start time logged for an incident and the time that incident is resolved or a workaround implemented as documented in the unavailability record for Priority 1 or Priority 2 incidents.

Availability measurements relate only to availability of the services, and do not include availability of the network connecting the user to the services.

