

Contract # AR2491**STATE OF UTAH COOPERATIVE CONTRACT**

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

The Consultants Consortium d/b/a TCC Software Solutions

Name

1022 East 52nd Street

Address

Indianapolis

IN

46205

City

State

Zip

LEGAL STATUS OF CONTRACTOR

- ☐ Sole Proprietor
☐ Non-Profit Corporation
☒ For-Profit Corporation
☐ Partnership
☐ Government Agency

Contact Person Mike Boyle Phone #317-625-2547 Email mike.boyle@e-tcc.comVendor # VC205731 Commodity Code #920-05

2. **GENERAL PURPOSE OF CONTRACT:** Contractor is permitted to provide the Cloud Solutions identified in Attachment B to Participating States once a Participating Addendum has been signed
3. **PROCUREMENT PROCESS:** This contract is entered into as a result of the procurement process on Bid#CH16012.
4. **CONTRACT PERIOD:** Effective Date: 09/16/2016 Termination Date: 09/15/2026 unless terminated early or extended in accordance with the terms and conditions of this contract. Note: Pursuant to Solicitation #CH16012, Contract must re-certify its qualifications each year.
5. **Administrative Fee,** as described in the Solicitation and Attachment A: 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.
6. **ATTACHMENT A:** NASPO ValuePoint Master Terms and Conditions, including that attached Exhibits
ATTACHMENT B: Scope of Services Awarded to Contractor
ATTACHMENT C: Pricing Discounts and Pricing Schedule
ATTACHMENT D: Contractor's Response to Solicitation #CH16012
- Any conflicts between Attachment A and the other Attachments will be resolved in favor of Attachment A.**
8. **DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:**
a. All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this contract.
b. Utah State Procurement Code, Procurement Rules, and Contractor's response to Bid #CH16012.
9. 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.

CONTRACTOR**STATE**

Contractor's

09/22/2016

Date

for Director, Division of Purchasing9.26.16
DateAlison J. Maloof

Type or Print Name and Title

Christopher Hughes

Division of Purchasing Contact Person

801-538-3254

Telephone Number

Fax Number

christopherhughes@utah.gov

Email

(Revision 16 June 2016)



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 SaaS.

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 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: The initial term of this Master Agreement is for ten (10) years with no renewal options.

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. Contractor acknowledges that it and its employees or agents may, in the course of providing a Product under this Master Agreement, be exposed to or acquire information that is confidential to Purchasing Entity's or Purchasing Entity's clients. Any reports or other documents or items (including software) that result from the use of the Confidential Information by Contractor 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 Contractor) publicly known; (2) is furnished by Purchasing Entity to others without restrictions similar to those imposed by this Master Agreement; (3) is rightfully in Contractor'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 Purchasing Entity without the obligation of confidentiality, (5) is disclosed with the written consent of Purchasing Entity or; (6) is independently developed by employees, agents or subcontractors of Contractor who can be shown to have had no access to the Confidential Information.

b. Non-Disclosure. Contractor 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 or use Confidential Information for any purposes whatsoever other than what is necessary to the performance of Orders placed under this Master Agreement. Contractor shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. Contractor shall use commercially reasonable efforts to assist Purchasing Entity in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the generality of the foregoing, Contractor shall advise Purchasing Entity, applicable Participating Entity, and the Lead State immediately if Contractor 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 Contractor shall at its

expense cooperate with Purchasing Entity in seeking injunctive or other equitable relief in the name of Purchasing Entity or Contractor against any such person. Except as directed by Purchasing Entity, Contractor 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 Purchasing Entity's request, Contractor shall turn over to Purchasing Entity all documents, papers, and other matter in Contractor's possession that embody Confidential Information. Notwithstanding the foregoing, Contractor 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. Contractor acknowledges that breach of this section, including disclosure of any Confidential Information, will cause irreparable injury to Purchasing Entity that is inadequately compensable in damages. Accordingly, Purchasing Entity 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. Contractor acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of Purchasing Entity 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, Lead State shall issue a written notice of default, identifying the nature of the default, and providing a period of 30 calendar days in which Contractor 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 Contractor's liability for damages.

c. If Contractor is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, Contractor shall be in breach of its obligations under this Master Agreement and Lead State 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 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. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, and Purchasing Entities, along with their officers, agents, and employees as well as any person or entity for which they may be liable, from and against claims, damages or causes of action including reasonable attorneys' fees and related costs for any death, injury, or damage to property arising directly or indirectly from act(s), error(s), or omission(s) of the Contractor, 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 claims, damages or causes of action including reasonable attorneys' fees and related costs arising out of the claim that the Product or its use, infringes Intellectual Property rights ("Intellectual Property Claim") of another person or entity.

(1) The Contractor's obligations under this section shall not extend to any claims arising from the combination of the Product with any other product, system or method, unless the Product, system or method is:

(a) provided by the Contractor or the Contractor's subsidiaries or affiliates;

(b) specified by the Contractor to work with the Product; or

(c) reasonably required, in order to use the Product in its intended manner, and the infringement could not have been avoided by substituting another reasonably available product, system or method capable of performing the same function; or

(d) It would be reasonably expected to use the Product in combination with such product, system or method.

(2) The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of an Intellectual Property Claim. Even if the Indemnified Party fails to provide reasonable notice, the Contractor shall not be relieved from its obligations unless the Contractor can demonstrate that it was prejudiced in defending the Intellectual Property Claim resulting in increased expenses or loss to the Contractor and then only to the extent of the prejudice or expenses. If the Contractor promptly and reasonably investigates and defends any Intellectual Property 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 Contractor's reasonable request and expense, information and assistance necessary for such defense. If the Contractor fails to vigorously pursue the defense or settlement of the Intellectual Property Claim, the Indemnified Party may assume the defense or settlement of it and the Contractor shall be liable for all costs and expenses, including reasonable attorneys' fees and related costs, incurred by the Indemnified Party in the pursuit of the Intellectual Property 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.

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. 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 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.

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.

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: 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 Staff 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.

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 for any reason 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.

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 its best 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 and perpetual license to use the API.

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 SciQuest, Inc. whereby SciQuest 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://www.naspo.org/WNCPO/Calculator.aspx>. 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 shown in Attachment F.

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. 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 for any reason 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 technical support. 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 immediately 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, 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 it's 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, 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, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

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.

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 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 for any reason 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 technical support. 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 immediately 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, 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, 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, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

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.

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.

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 for any reason 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 technical support. 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 immediately 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, 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, 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, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

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.

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.

Attachment B

TCC is capable of providing SaaS, IaaS, and PaaS service models, as well as private cloud, community cloud, public cloud and hybrid cloud deployment models under the terms of this RFP.

TCC is capable of operating and managing environments that adhere to high security standards, such as PCI and FISMA. The AWS control environment is subject to various internal and external risk assessments. AWS' Compliance and Security teams have established an information security framework and policies based on the Control Objectives for Information and related Technology (COBIT) framework and have effectively integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, the PCI DSSv3.1, and the National Institute of Standards and Technology (NIST) Publication 800-53 Rev 3 (Recommended Security Controls for Federal Information Systems). AWS maintains the security policy, provides security training to employees, and performs application security reviews. These reviews assess the confidentiality, integrity, and availability of data, as well as conformance to the information security policy.



1022 East 52nd St., Indianapolis, IN 46205
Mike Boyle | Mike.Boyle@e-tcc.com
317-625-2547 | e-tcc.com

Prepared for:

State of Utah Division of Purchasing

NASPO ValuePoint Master Agreement for Cloud Solutions

Cost Proposal

Utah Solicitation Number CH16012
Due: February 26, 2016 – 1:00pm MTN

Section Title: Cost Proposal

9.1 (M)

Given that technology products generally depreciate over time and go through typical product lifecycles, it is more favorable for Purchasing Entities to have the Master Agreement be based on minimum discounts off the Offeror's commercially published pricelists versus fixed pricing. In addition, Offerors must have the ability to update and refresh their respective price books, as long as the agreed-upon discounts are fixed. 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.

Offeror must identify its cost proposal as "Cost Proposal – CH16012 Cloud solutions". No specific format is required for an Offeror's price schedule; however the Offeror must provide and list a discount from its government pricing catalog. New discount levels may be offered for new services that become available during the term of the Master Agreement.

Pricing catalogs should include the price structures of the cloud solutions models and deployment models that it intends to provide including the types of data it is able to hold under each model. Pricing must be all-inclusive of infrastructure and software costs and management of infrastructure, network, OS, and software.

The Lead State understands that each Offeror may have its own pricing models and schedules for the Services described in the RFP. It is the intent of the RFP to allow price schedules that are viewed in the traditional line item structure or price schedule that have pay-as-you-go characteristics.

An Offeror's price catalog should be clear and readable. Participating Entities, in reviewing an Offeror's Master Agreement, will take into account the discount offered by the Offeror along with the transparent, publicly available, up-to-date pricing and tools that will allow customers to evaluate their pricing.

Individual Participating Addendums will use the cost proposals pricing as a base and may negotiate an adjusted rate. Any negotiated Participating Addendum rates, exclusive of taxes or any individual state's administrative fee, shall not exceed the submitted cost proposal rates.

Offeror's price catalog should be broken into category for each service category. For example if an Offeror provides a SaaS offering then its price catalog should be divided into education SaaS offerings, e-procurement SaaS offerings, information SaaS offering, etc.

Some Participating Entities may desire to use an Offeror for other related application modifications to optimize or deploy cloud solutions applications. Responses to the RFP must include hourly rates by job specialty for use by Participating Entities for these types of database/application administration, systems engineering & configuration services and consulting throughout the contract period. The hourly rates should be a fully burdened rate that includes labor, per diem, travel, overhead, and any other costs related to the service. The specific rate (within a range) charged for each proposed contracted service would be the lowest rate shown unless justified in writing and approved by the Lead State. Any of these valued-added services must be included in your cost proposal, e.g., by an hourly rate.

Attachment G – Cost Schedule

Solicitation Number CH16012 NASPO ValuePoint Cloud Solutions RFP

Cloud Solutions By Category. Specify **Discount Percent %** Offered for products in each category.
Highest discount will apply for products referenced in detail listings for multiple categories. Provide a detailed product offering for each category.

Software as a Service Discount % 3

Infrastructure as a Service Discount % 3

Platform as a Services Discount % 3

Additional Value Added Services:

Maintenance Services

Onsite Hourly Rate \$ 205.58
Remote Hourly Rate \$ 103.97

Professional Services

- **Deployment Services** Onsite Hourly Rate \$ 217.65
Remote Hourly Rate \$ 121.19
- **Consulting/Advisory Services** Onsite Hourly Rate \$ 267.84
Remote Hourly Rate \$ 152.43
- **Architectural Design Services** Onsite Hourly Rate \$ 267.84
Remote Hourly Rate \$ 152.43
- **Statement of Work Services** Onsite Hourly Rate \$ 217.65
Remote Hourly Rate \$ 121.19

Partner Services

Onsite Hourly Rate \$ N/A
Remote Hourly Rate \$ 251.49

Training Deployment Services

Onsite Hourly Rate \$ 205.58
Online Hourly Rate \$ 103.97

Product Offerings

Software as a Service

- eXpedite (mobile inspection software)
- early childhood integrated data systems

Infrastructure as a Service

- Private Cloud
- Public Cloud
- Community Cloud
- Hybrid Cloud
- AWS Partner

Platform as a Services

- Dynamics CRM



1022 East 52nd St., Indianapolis, IN 46205
Mike Boyle | Mike.Boyle@e-tcc.com
317-625-2547 | e-tcc.com

Prepared for:

State of Utah Division of Purchasing

NASPO ValuePoint Master Agreement for Cloud Solutions

Technical Response

Utah Solicitation Number CH16012
Due: March 10, 2016 – 1:00pm MTN



Table of Contents

Section Title: Technical Response..... 5

8.1 (M)(E) Technical Requirements 5

8.1.1 5

8.1.2 6

8.1.3 8

8.1.4 10

8.1.5 11

8.2 (E) Subcontractors..... 12

8.2.1 12

8.2.2 12

8.2.3 12

8.3 (E) Working with Purchasing Entities..... 12

8.3.1 12

8.3.2 15

8.3.3 16

8.3.4 16

8.3.5 16

8.3.6 16

8.3.7 17

8.4 (E) Customer Service 17

8.4.1 17

8.4.2 23

8.5 (E) Security of Information 24

8.5.1 24

8.5.2 27

8.5.3 27

8.6 (E) Privacy and Security 27

8.6.1 27

8.6.2 28

8.6.3 29

8.6.4 29

8.6.5 30

8.6.6 31

8.6.7 31

8.6.8 32

8.6.9 32

8.6.10 33

8.6.11 34

8.6.12 34

8.6.13 35

8.7 (E) Migration and Redeployment Plan	37
8.7.1	37
8.7.2	37
8.8 (E) Service or Data Recovery.....	37
8.8.1	37
8.8.2	38
8.9 (E) Data Protection	39
8.9.1	39
8.9.2	40
8.9.3	40
8.10 (E) Service Level Agreements.....	40
8.10.1	40
8.10.2	40
8.11 (E) Data Disposal.....	40
8.12 (E) Performance Measures and Reporting.....	41
8.12.1	41
8.12.2	41
8.12.3	42
8.12.4	42
8.12.5	43
8.12.6	44
8.12.7	44
8.12.8	45
8.12.9	45
8.12.10	45
8.13 (E) Cloud Security Alliance	46
8.14 (E) Service Provisioning	46
8.14.1	46
8.14.2	48
8.15 (E) Backup and Disaster Plan	48
8.15.1	48
8.15.2	48
8.15.3	49
8.16 (E) Solution Administration.....	49
8.16.1	49
8.16.2	49
8.16.3	49
8.16.4	49
8.16.5	50
8.17 (E) Hosting and Provisioning.....	50
8.17.1	50
8.17.2	50



8.17.3 54

8.18 (E) Trial and Testing Periods (Pre- and Post-Purchase) 55

8.18.1 55

8.18.2 56

8.18.3 56

8.19 (E) Integration and Customization 56

8.19.1 56

8.19.2 57

8.20 (E) Marketing Plan 57

8.21 (E) Related Value-Added Services to Cloud Solutions 57

8.22 (E) Supporting Infrastructure 58

8.22.1 58

8.22.2 58

8.23 (E) Alignment of Cloud Computing Reference Architecture 59

Appendix A 60

AWS Risk and Compliance with CCM 60

Appendix B 6147

TCC Service Level Agreement Template 6147

Appendix E 62

Sample Project Plan and Project Schedule 62

Section Title: Technical Response

8.1 (M)(E) Technical Requirements

If applicable to an Offeror's Solution, an Offeror must provide a point by point responses to each technical requirement demonstrating its technical capabilities. If a technical requirement is not applicable to an Offeror's Solution then the Offeror must explain why the technical requirement is not applicable.

Affirm your understanding of, and willingness to comply with, the requirements of Attachments C & D.

8.1.1

Offeror must identify the cloud service model(s) and deployment model(s) it intends to provide to Eligible Users. See Attachment D.

TCC proposes Infrastructure as a Service as the cloud service and deployment model for the State of Utah.

TCC's Network and Managed Services discipline assures that optimal system performance and security for applications which are mission-critical to our clients. **TCC's network and managed services help our clients streamline operations and reduce costs.**

TCC leverages a secure, state-of-the-art data center, resident ITIL professionals and economies of scale to develop, manage, and maintain several application hosting systems. TCC uses ITIL methods to be a step above dedicated hosting. Managed infrastructure from TCC includes daily management of the hardware, operating systems and standardized applications to ensure optimal performance, as well as system upgrades and updates to ensure your systems are operating efficiently. TCC's network and managed services include the following:

Implementation Services:

Installing and configuring hardware and back-office software

Virtual and physical servers, firewalls, routers, switches, tape drives and backup media, anti-virus software, imaging system hardware and software, and the suite of Microsoft Windows Server and SQL Server products

Domain name administration including ordering and maintenance of domain names and zone files, configuration of hostnames and URLs, and SSL certificate services

Maintenance Processes:

Providing essential maintenance tasks

Backup monitoring, tape exchanges and periodic test restores, antivirus monitoring and update maintenance, event log monitoring for Windows servers, regularly updated security patches, website and data base availability monitoring

Break/fix and support work as needed

Security Practices

Actively driven Information System Security Management for business areas of government

Building and maintaining secured hosted environments, developing secure software applications, and performing Disaster Recovery services

Multi-layered approach to security and services

Reliable tools applied with best practices to minimize security risk

Segmented network design and deployment of the “principle of least privilege” access model; isolating information areas from one another

Audit trail and audit analysis confirm the success of our efforts

8.1.2

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

8.1.2.1 NIST Characteristic - On-Demand Self-Service: Provide a brief written description of how the cloud solutions proposed satisfies this individual essential NIST Characteristic. Attest capability and briefly describe how self-service technical capability is met.

AWS provides an On-Demand Self-Service portal through their AWS Management Console. The Console facilitates cloud management for all aspects of your AWS account, including monitoring your monthly spending by service, managing security credentials, or even setting up new IAM Users.

8.1.2.2 NIST Characteristic - Broad Network Access: Provide a brief written description of how the cloud solutions proposed satisfies this individual essential NIST Characteristic. Attest capability and briefly describe how network access is provided.

AWS provides a Broad Network Access through the AWS Management console and the AWS Console Mobile app, user can quickly and easily view your existing resources, including CloudWatch alarms, and perform operational tasks from your mobile device.



FIGURE 1 AWS INFRASTRUCTURE REGION

8.1.2.3 NIST Characteristic - Resource Pooling: Provide a brief written description of how the cloud solutions proposed satisfies this individual essential NIST Characteristic. Attest capability and briefly describe how resource pooling technical capability is met.

AWS provides the flexibility to place instances and store data within multiple geographic regions as well as across multiple availability zones within each region. Each availability zone is designed as an independent failure zone. This computing resources are pooled together to serve multiple consumers using multiple-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. The resources include among others storage, processing, memory, network bandwidth, virtual machines and email services.

8.1.2.4 NIST Characteristic - Rapid Elasticity: Provide a brief written description of how the cloud solutions proposed satisfies this NIST Characteristic. Attest capability and briefly describe how rapid elasticity technical capability is met.

AWS can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time. AWS provides different solutions such as Cloudfront, Elastic Beanstalk, and DynamoDB that allow automated provisioning as well as rules to enable users to manually provisions as well.

8.1.2.5 NIST Characteristic - Measured Service: Provide a brief written description of how the cloud solutions proposed satisfies this NIST Characteristic. Attest capability and briefly describe how measured service technical capability is met.

The Billing and Cost Management service provides features that you can use to estimate and plan your AWS costs, receive alerts if your costs exceed a threshold that you set, assess your biggest investments in AWS resources, and, if you work with multiple AWS accounts, simplify your accounting. The AWS Billing and Cost Management console includes the no-cost Cost Explorer tool for viewing your AWS cost data as a graph. With

Cost Explorer you can filter graphs by API operations, Availability Zones, AWS service, custom cost allocation tags, Amazon EC2 instance type, purchase options, region, or, if you use Consolidated Billing, by linked account.

8.1.3

Offeror must identify for each Solution the subcategories that it offers for each service model. For example if an Offeror provides a SaaS offering then it should be divided into education SaaS offerings, e-procurement SaaS offerings, information SaaS offering, etc.

AWS SaaS under ISO 27017:

- Amazon CloudFront
- Amazon DynamoDB
- Amazon EC2 Container Service (ECS)
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic File System (EFS)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon Glacier
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow Service (SWF)
- Amazon SimpleDB
- Amazon Virtual Private Cloud (VPC)
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- AWS Directory Service
- AWS Elastic Beanstalk
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- AWS Storage Gateway
- AWS WAF (Web Application Firewall)
- Elastic Load Balancing



- VM Import/Export

AWS IaaS under ISO 27001:

- AWS CloudFormation
- Amazon CloudFront
- AWS Cloudtrail
- AWS Directory Service
- Amazon DynamoDB
- AWS Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Cloud Compute (EC2)
- Amazon EC2 Container Service (ECS)
- AWS Direct Connect
- Amazon EC2 VM Import/Export
- AWS Cloud Hardware Security Model (HSM)
- Elastic Load Balancing (ELB)
- Amazon Elastic File System (EFS)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon Glacier
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- AWS Route 53
- Amazon SimpleDB
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow Service (SWF)
- AWS Storage Gateway
- Amazon Virtual Private Cloud (VPC)
- AWS WAF
- Web Application Firewall
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- The underlying physical infrastructure (including GovCloud) and the AWS Management Environment

AWS PaaS under ISO 27018:

- Amazon CloudFront
- Amazon DynamoDB
- Amazon EC2 Container Service (ECS)
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic File System (EFS)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon Glacier
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow Service (SWF)
- Amazon SimpleDB
- Amazon Virtual Private Cloud (VPC)
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- AWS Directory Service
- AWS Elastic Beanstalk
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- AWS Storage Gateway
- AWS WAF (Web Application Firewall)
- Elastic Load Balancing
- VM Import/Export

8.1.4

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

TCC protects all security aspects of this project by establishing and strictly adhering to project specific policies and procedures established on the basis of standards published by the United States Department of Commerce, Computer Security Division, Information Technology Laboratory and National Institute of Standards and



Technology (NIST). The Federal Information Processing Standards Publication 199 (FIPS PUB 199) provides direction on the classification level of government information systems containing confidential and personal information. Due to the confidentiality level of the system data at rest and in transit within the proposed system, TCC shall design a solution to meet the requirements defined in NIST SP 800-53 Revision 3 as amended and applicable.

TCC actively manages the security requirements through development and ongoing maintenance of a crossover document which correlates the solution against the NIST SP 800-53 requirements. These activities are managed through the application of project specific TCC policies and procedures which govern the implementation and measurement of technical, administrative, and physical safeguards. Compliance with the policies and procedures are enforced by the regular monitoring and review of security related deliverables by the project security officer and the TCC security executive.

Control procedures for this project regulate access to both the data residing in the information system and the process for allowing individuals access to the system. This includes regulating how data is accessed by individuals and interdependent systems. Access to the proposed systems is controlled by the establishment and strict adherence to procedures restricting access to only those individuals who are approved. Restrictions of privileges within the application ensure that users only have access to the data necessary to complete their assigned tasks. Technical controls designed specifically for this project monitor, at a minimum, general access, unsuccessful login attempts, user access trends, and intrusion attempts from both internal and external threat sources.

All of the Cloud Service Based Models offered by TCC follow the NIST definition of cloud computing found in NIST Special Publication 800-145.

8.1.5

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.

TCC provides hosting, maintenance, and support for state government clients. TCC employs industry standard software development techniques and processes to ensure that each system is deployed to provide security for its user community. We currently host and support over 1500 servers for our clients. TCC has experience hosting critical web applications and is accustomed to maintaining similar or higher levels of service.

Our Network Operations Group consists of ITIL and CISSP certified staff. TCC has experience with deploying highly available environments in a secure manner. We have worked in multiple similar state government environments and are familiar with the standards and methodologies that should be used during implementation. Our Infrastructure as a Service offering uses proven processes for anti-virus updates, installation of software patches, data backups, disaster relief preparation, monitoring of uptime and performance, software license administration, lifecycle management and documentation of these procedures.

Cloud Services makes up over thirty percent of TCC's annual revenue. We currently provide cloud services to a dozen different agencies across four different states coast to coast. TCC has been providing cloud services to state government agencies for over ten years and continues to innovate and improve our cloud solutions. Our

staff have several and continue to pursue AWS certifications as we continue to expand our presence as an AWS Partner.

8.2 (E) 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.

TCC does not intend to utilize subcontractors for this effort. TCC is able to deliver all services without the use of subcontractors.

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.

TCC does not intend to utilize subcontractors for this effort.

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.

TCC does not intend to utilize subcontractors for this effort.

8.3 (E) 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.*

Security is an essential component of information privacy. It is one of the basic principles of fair information practice: Organizations that collect or manage individuals' Personal Information should use security safeguards to protect that information against unauthorized access, use, disclosure, modification or destruction. Implementing an effective information security program is essential for an organization to fulfill its responsibility to the individuals who entrust it with their Personal Information. It is the best way to reduce the risk of exposing individuals to the possibility of identity theft. It is also the best way to reduce the risk of exposing the organization to the damage to its reputation and finances resulting from an information security breach.

The following sections provide procedures to follow in preparing for, detecting and reacting to a security breach. Sections I and II are activities that agencies should engage in immediately to protect data from a security breach and prepare the agency for a security breach. Section III and IV are activities that take place if a security breach has occurred.

I: Protection, Prevention and Detection

While an organization's information security program may be unique to its situation, there are recognized basic components of a comprehensive, multilayered program to protect Personal Information from unauthorized access. An organization should protect the confidentiality of Personal Information whether it pertains to members of the public, employees or other individuals. For both paper and electronic records, these components include physical, technical and administrative safeguards. The items below are examples and each item will need reviewed at time of scope creation and contract formation. This is not an exclusive nor exhaustive list, merely a representation of practices:

1. Collect the minimum amount of Personal Information necessary to accomplish the business purposes, and retain it for the minimum time necessary.
2. Collect notification contact information (mailing address and/or e-mail address) from individuals when notice-triggering Personal Information is collected. If the procedure calls for contacting affected individuals by e-mail, obtain the individuals' prior written consent to the use of e-mail for that purpose.
3. Create an inventory of records systems, critical computing systems, databases, files and storage media containing Personal Information. Include laptops and handheld devices used to store Personal Information.
4. Classify Personal Information in records systems according to sensitivity (notice-triggering, private information and High-Risk Personal Information). Identify systems containing Notice-Triggering Information and those containing High-Risk Personal Information in the inventory.
5. Use physical and technological security safeguards as appropriate to protect Personal Information, particularly High-Risk Personal Information such as Social Security number, driver's license number, Washington state identification card number, financial account numbers and any associated passwords and PIN numbers, other financial information, and health information, in paper as well as electronic records.
 - a. Authorize Workforce Members to have access to only the specific categories of Personal Information that are required by their job responsibilities.
 - b. Where possible, use technological means to restrict internal access to specific categories of Personal Information (e.g. access rights).



- c. Monitor Workforce Member access to notice-triggering and High-Risk Personal Information (e.g. via system audit logs).
 - d. Immediately remove access privileges of former Workforce Members.
6. Promote awareness of security and privacy policies and procedures through training and communications. TCC mandates monthly training for its employees on a reoccurring basis.
7. Use intrusion detection/prevention technology and procedures to ensure rapid detection of unauthorized access to High-Risk Personal Information. OIRM offers Host Intrusion Detection services to agencies for servers and workstations. This service can assist in protecting databases and systems containing High-Risk Personal Information. Host intrusion detection can identify unauthorized attempts to obtain such information. For information on Host Intrusion Detection systems contact the Chief Information Security and Privacy Officer.
8. Ensure that audit logging is active on systems and that logs are reviewed regularly. Ensure that logs are analyzed, unusual access to High-Risk Personal Information is investigated and logs are retained.

II: Preparations in Advance of a Security Breach

Identification of a security breach, reporting and notification are the responsibilities of each agency. To ensure timely notice to affected individuals when appropriate, the following practices are among those that to be included in every agency's procedures:

1. Each agency should develop and adopt an incident response plan. This plan should include methodologies and technology that will assist in identifying the occurrence of a security breach of Personal Information.
2. Deploy and use all available systems that can assist in detecting and preventing a security breach. This would include but is not limited to Host Intrusion Prevention Systems (on all workstations and all mission critical servers or those containing higher risk Personal Information), vulnerability scanners, encryption systems, Anti-virus and Anti-Spyware tools. Carefully configure alerts and check logs regularly in order to detect inappropriate activity.
3. Adopt written procedures for internal reporting of security incidents that may involve unauthorized access to High-Risk Personal Information.
4. Designate one staff member as the Security Breach Coordinator for the agency. This person manages internal procedures and coordination with the Chief Information Security and Privacy Officer.
5. Regularly train Workforce Members for their roles and responsibilities during incident response.
6. Establish an incident response team. Collect 24/7 contact information for response team members. Ensure that all team members have this information.
7. Identify responsible individuals in the agency response plan and define key terms.
8. Plan for and use measures to contain, control and correct any security incident that may involve High-Risk Personal Information.

III: Security Breach Reporting, Coordination, Communication and Investigation Procedures

Unauthorized Access:

In determining whether unencrypted Notice-Triggering Information has been inappropriately accessed, or is reasonably believed to have been accessed, by an unauthorized person, consider the following factors, among others:

- Indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer, CD, diskette, report or other device or media containing unencrypted High-Risk Personal Information.
- Indications that the information has been downloaded, emailed, faxed, printed or copied by an unauthorized individual.
- Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

Each agency must determine its own specific methodology for identifying such a security breach. Once it has been determined that Personal Information may have been accessed by an unauthorized person the following procedure begins:

Agency Activities:

Agencies may augment the following notification process with additional notification steps.

1. Data Custodian or person detecting unauthorized access notifies Data Owner.
2. Data Owner notifies IT group (ITSDM, IT Manager, TMB member, etc.).
3. Data Owner notifies agency management (Department/Division Manager, BMC member, etc.).
4. TMB/BMC member notifies agency Security Breach Coordinator.
5. Data Owner and Data Custodian completes the following incident forms and presents them to the Security Breach Coordinator.
6. Security Breach Coordinator completes the following incident forms.
7. Security Breach Coordinator provides Chief Information Security and Privacy Officer (CISPO) with copies of all report forms.

The CISPO will notify and coordinate with the following agencies (if necessary). Actions taken will be documented in the Security Breach Communications Log for law enforcement and debrief sessions.

1. Security Breach Coordinator
 - Receives incident reports
 - Provides ongoing status reports
 - Authorizes notification process. Unless investigation is underway by a designated law enforcement agency, this authorization will be provided within 10 business days of CISPO notification of incident.

8.3.2

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

TCC will not engage in nor permit its agents to push adware, software, or marketing not explicitly authorized by the Participating Entity or the Master Agreement. TCC also recommends that Participating Entities should allow antivirus and antimalware updates whether through change management or through a review panel to push updates as needed to maintain a best practice security model.

8.3.3

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

Running development and test workloads on Amazon Web Services enables you to remove hardware-based resource constraints to quickly create developer environments and expand your testing machine fleet. Customers get instant access to machines that you can configure any way you want and you only pay for what you use. This allows customers to stand and deploy new environments that run on exactly the same infrastructure standards that your production environment utilizes.

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.

TCC understands the importance of providing a user experience that is compliant with Section 508 standards for accessibility. TCC is completely able to meet or exceed the minimum requirements of the standards noted in Requirement 8.3.4 in the development of the requested software. As part of its testing processes, TCC utilizes assistive technology testing software JAWS to ensure that its software meets or exceeds minimum standards of accessibility.

8.3.5

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

TCC's applications and content delivered through Web browsers are accessible using the current and past two released versions of Internet Explorer, Firefox, Chrome and Safari. TCC shall support the state's security strategies by building to and maintaining compliance with both the minimum information security requirements established by the state and the National Institute for Standards and Technology (NIST) Special Publication 800-53 Rev. 4: Security Controls for Federal Information Systems and Organizations moderate-level security controls.

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.

TCC will perform due diligence through meetings and cooperation with the Purchasing Entity to determine the sensitivity of the data that will be managed and how to protect it. TCC is prepared to perform Data Discovery exercises to help the Purchasing Entity find and protect sensitive information quickly and cost effectively. TCC has experience working with highly sensitive data and knows where it should reside within the environments.

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.

Please refer to the sample Work Breakdown Structure included in Appendix E.

8.4 (E) Customer Service

8.4.1

Offeror must describe in detail how it ensures 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).*

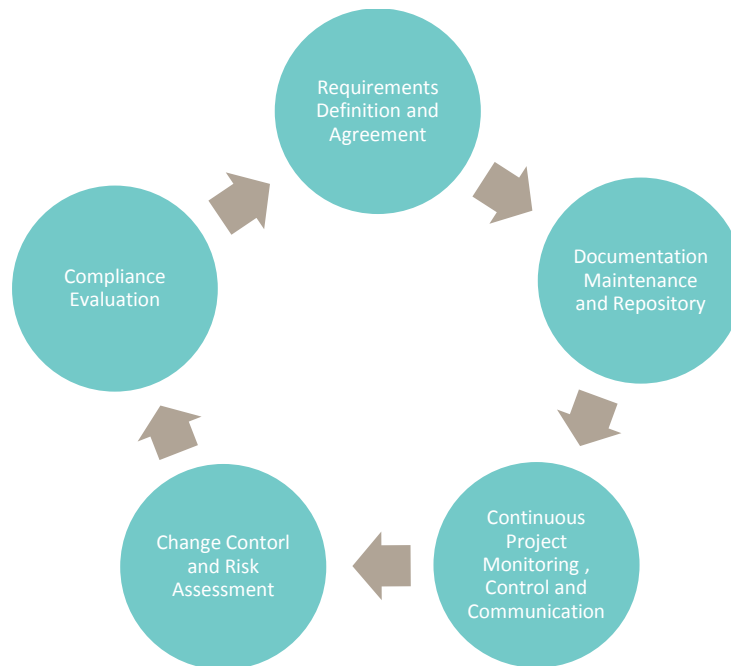
Quality Assurance

TCC creates a Contract Compliance Matrix which contains all business requests as outlined by the State in the RFP, Contract and Charter. Using the Contract Compliance Matrix, TCC tracks each request throughout the development life cycle to ensure compliance. This document is located on SharePoint which is made available for the State to review as needed. For each business request, there is associated supporting documentation, also stored in SharePoint, which details how the requirement was met.

A contract compliance report, similar to the example included below, is available on SharePoint:

Requirement		Performance		Verification Method	Link to Documentation
ID	Description	Expected Result	Actual Result	Analysis (A), Test (T), Inspection (I), Document (D)	
FR.1					
FR.2					
FR.3					

To ensure compliance in the delivery of all requirements of this RFP, TCC adheres to a Quality Assurance Plan which consists of the following five standardized and repeatable processes:



- **Requirements Definition and Agreement**

A successful transition of services from one vendor to another requires significant time, effort and commitment from both the incumbent vendor and the new vendor. Transition periods are critical as they may require various levels of the transferring of necessary knowledge, documentation, data, and files. The first and most important step in a transition is Requirements Definition and Agreement. During this process, TCC works closely with subject matter experts as well as the incumbent vendor to clearly define and document the project requirements as well as develop traceability measures which enhance status reporting and evaluation of project progress.

- **Documentation Maintenance and Repository**

Project documentation provides all of the information required to initiate, plan, execute, monitor, and complete the project in a timely and cost-effective manner. TCC is committed to the maintenance and continuous updating of the project documentation library, which resides on TCC's SharePoint repository.

All project documentation is maintained and updated to ensure State and vendor personnel always have access to the most up-to-date and accurate information. TCC has developed proven procedures and processes to ensure that client data and project documentation is properly and routinely archived and protected from loss, unauthorized access or destruction.

- **Continuous Project Monitoring, Control and Communication**



The purpose of project monitoring and control is to provide an understanding of the project's progress so that appropriate corrective actions can be taken when the project's performance deviates significantly from the plan. A project's documented plan is the basis for monitoring activities, communicating status, and taking corrective action. Progress is determined by comparing actual work product, effort, cost, and schedule to the plan at prescribed milestones or control levels within the project schedule or work breakdown structure (WBS). TCC understands that project visibility enables timely corrective action is taken when project risks or issues are identified. TCC's strategy in achieving effective project monitoring, control, and communication is to submit weekly status reports along with project plan progress and the contract compliance matrix.

- **Change Control and Risk Management**

The executed contract and requirements outlined in the RFP are modified only by a written Change Order. All approved and rejected change requests are documented in the Change Request Log and maintained on the TCC SharePoint site. The change management process is followed to ensure that each change introduced to the project is appropriately defined, evaluated and approved prior to implementation.

TCC adheres to a risk management process wherein risks to the project are formally identified, quantified and managed throughout the duration of the project. The key to this process is completing a series of tasks intended to reduce the likelihood of occurrence and the severity of impact of each risk.

- **Compliance Evaluation**

TCC affirms that we are capable of furnishing all necessary services required to successfully complete all of the tasks and work requirements and produce the high quality deliverables described in this proposal. We leverage our in-house expertise as well as the expertise from any subcontractors to fulfill the requirements at the highest level of quality.

TCC complies with the all federal laws, regulations, policies, standards and guidelines. As a contractor with several State governments, we are experienced with staying abreast of current, new and revised laws, regulations, etc.

Our team adheres to the practice of constant process review and evaluation. Through our comprehensive reporting practices, project management methodologies utilized and clearly defined communication procedures TCC is confident that the compliance evaluation process is efficient, thorough and beneficial, resulting in a successful project implementation.

Incident Management

The purpose of formalizing these procedures accomplishes the following benefits:

- Minimized outage time
- Proper communication and coordination of incident resolution activities

- Proper incident notification and escalation
- Improved end-user productivity
- Basis for capturing Experience and maintaining a knowledge base

Incident Management Life Cycle

Identify – Incident is identified and realized, the incident management life cycle begins. Incidents can originate from end-users, developers, testers, etc... The owner of the incident then gathers the proper data relative to the incident, assigns the severity level, and begins to enter a ticket into the TCC's ticketing system

Analyze – During this phase of the process, Root Cause Analysis (see below) is performed.

Resolve – From RCA a resolution to the incident can be identified. A change record may be required to document any change required to resolve the incident. This process will vary depending on the particular application and the severity level of the incident.

Communicate – Inform the interested parties on how and why the incident occurred, and the solution to fix it. Document lessons learned and capture the solution in the knowledge base.



Severity Level Classification

SEV1 – Critical/Severity 1

A Critical/Severity 1 (SEV1) incident has one or more of the following characteristics.

- The incident has a major business impact
- Normal business operations cannot be conducted
- Multiple end-users cannot run a production application
- The affected end-user is high profile (as defined)
- The incident cannot be circumvented
- Work around does not exist



Process:

- Immediate notification to Project Manager/Technical Lead
- Incident takes precedent over all work
- Identify solution
- Communicate to project team and stakeholders
- Notify TCC Executive Leadership of incident within 24 hours
- Corrective Action Plan created by Project Manager
- Enter issue into Help Desk / Incident Tracking system

SEV2 – High/Severity 2

A Critical/Severity 2 (SEV2) incident has one or more of the following characteristics.

- The incident has substantial business impact
- Normal business operations are severely impeded
- The application/system functions, but usability is severely limited for multiple end-users
- The application/system has experienced continual or repeated incidents
- Work around does not exist

Process:

- Immediate notification to Project Manager/Technical Lead
- Incident takes precedent over all other work
- Identify solution
- Communicate to project team and stakeholders
- Corrective Action Plan created by Project Manager
- Enter issue into system

SEV3 – Medium/Severity

A Critical/Severity 3 (SEV3) incident has one or more of the following characteristics.

- The incident has limited business impact
- Normal business operations are minimally impeded
- The end-user can run the application but has lost some functionality
- The incident is not continual or repeated
- Work around exists

Process:

- Root Cause Analysis performed to identify the issue
- Identify solution
- Enter issue into system



SEV4 – Low/Severity

A Critical/Severity 4 (SEV4) incident has one or more of the following characteristics.

- The incident has no business impact
- Normal business operations are not impeded
- The end-user can run the application
- The request is an end-user inquiry only
- Work around exists

Process:

- Root Cause Analysis performed to identify the issue
- Identify solution
- Enter into system

TCC Incident Escalation

Tier 1

Incidents found and reported to the Help Desk at the Tier 1 level are easily resolved by the Help Desk Technician. The Help Desk technician will log this incident and resolution. Work around is established. Open issues that are not resolved are escalated to Tier 2.

Tier 2

Incidents found and reported to the Help Desk at the Tier 2 level require application help desk investigation. Work around is established. Help Desk technician will escalate the case to Tier 3 if unable to resolve.

Tier 3

Incidents found and reported to the Tier 3 level require investigation by the technical lead of the program. Tier 3 will engage the Network Operations Group at this level. The Project Manager is alerted to this issue and follows the progress of the incident until resolution identified.

Service Level Agreement (SLA)

TCC performs due diligence through meetings and cooperation with the Purchasing Entity to determine the sensitivity of the data that will be managed and how to protect it. TCC is prepared to perform Data Discovery exercises to help the Purchasing Entity find and protect sensitive information quickly and cost effectively. TCC has experience working with highly sensitive data and knows where it should reside within the environments.

TCC has provide a copy of our Service Level Agreement template in Appendix B of this proposal.

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.*
- 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.*
- c. Customer Service Representative will respond to inquiries within one business day.*
- d. You must provide design services for the applicable categories.*
- e. You must provide Installation Services for the applicable categories.*

TCC is able to comply with all of the above customer service requirements. TCC will provide a lead representative for each entity that executes a Participating Addendum, and contact information will be kept current.

TCC will provide help desk support phone or email at a minimum, from 7AM to 6PM on Monday through Sunday for the applicable time zones. Help Desk representatives will respond to inquiries within one business day.

TCC's Help Desk discipline provides prompt, reliable support that aligns with our client's standards and expectations. Our incident management and ticketing system makes it easy to report incidents, and we promptly respond and manage each one through to resolution. TCC's staff are highly skilled at resolving help requests without escalation to a higher level of support.

Predefined Problem Solving that is Proactive and Highly Responsive

Our Help Desk staff comprises experienced, technical personnel with support training to meet our client's exacting standards. Our problem management process is based on proven ITIL methodology and all of our staff are ITIL certified.

Using a proactive approach, as well as predefined scripts and procedures, our staff works to quickly resolve incidents. With each user contact the goals are to:

- Let users know the status of their ticket
- Maintain an audit trail of all actions relating to a ticket
- Keep our clients informed regarding the state of service via regular reports and service review meetings
- Create a satisfied user group

TCC provides the following levels of Help Desk Support:

Level 1

Basic level of support where service problems are logged into the TCC help desk, triaged, troubleshooting occurs, and elementary problems are resolved. Examples of this include basic “how to” questions, hardware diagnostics, password resets, account creation, etc.

Level 2

This level of support is where incoming customer phone calls or e-mails are logged into the TCC team helpdesk. The relevant problem or request details are obtained and the call is routed to an appropriate support resource.

Level 3

The call is received by the TCC team helpdesk, the call is logged and the caller is directed to an appropriate resource. These problems usually involve advanced levels of support that require specialized technical or application expertise.

8.5 (E) Security of Information

8.5.1

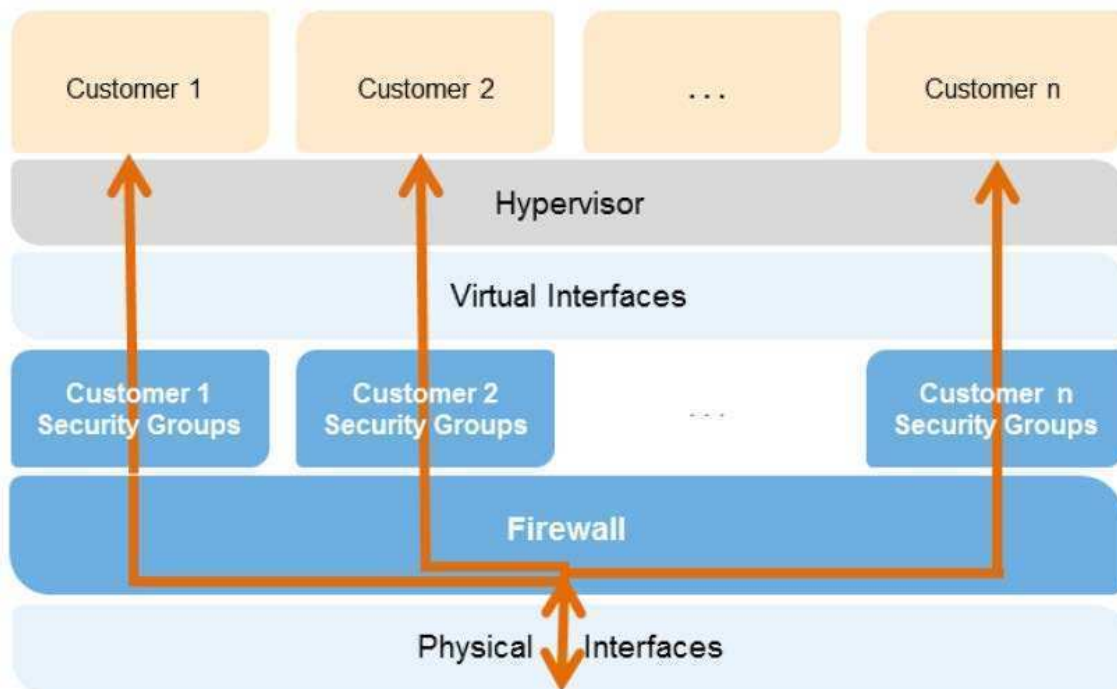
Offeror must describe in detail the measures you take to protect data. Include a description of the method by which you will hold, protect, and dispose of data following completion of any contract services.

Amazon EC2 currently utilizes a highly customized version of the Xen hypervisor, taking advantage of paravirtualization (in the case of Linux guests). Because paravirtualized guests rely on the hypervisor to provide support for operations that normally require privileged access, the guest OS has no elevated access to the CPU. The CPU provides four separate privilege modes: 0-3, called rings. Ring 0 is the most privileged and 3 the least. The host OS executes in Ring 0. However, rather than executing in Ring 0 as most operating systems do, the guest OS runs in a lesser-privileged Ring 1 and applications in the least privileged Ring 3. This explicit virtualization of the physical resources leads to a clear separation between guest and hypervisor, resulting in additional security separation between the two.

Customer instances have no access to raw disk devices, but instead are presented with virtualized disks. The AWS proprietary disk virtualization layer automatically resets every block of storage used by the customer, so that one customer’s data is never unintentionally exposed to another. In addition, memory allocated to guests is scrubbed (set to zero) by the hypervisor when it is unallocated to a guest. The memory is not returned to the pool of free memory available for new allocations until the memory scrubbing is complete.

AWS recommends customers further protect their data using appropriate means. One common solution is to run an encrypted file system on top of the virtualized disk device.

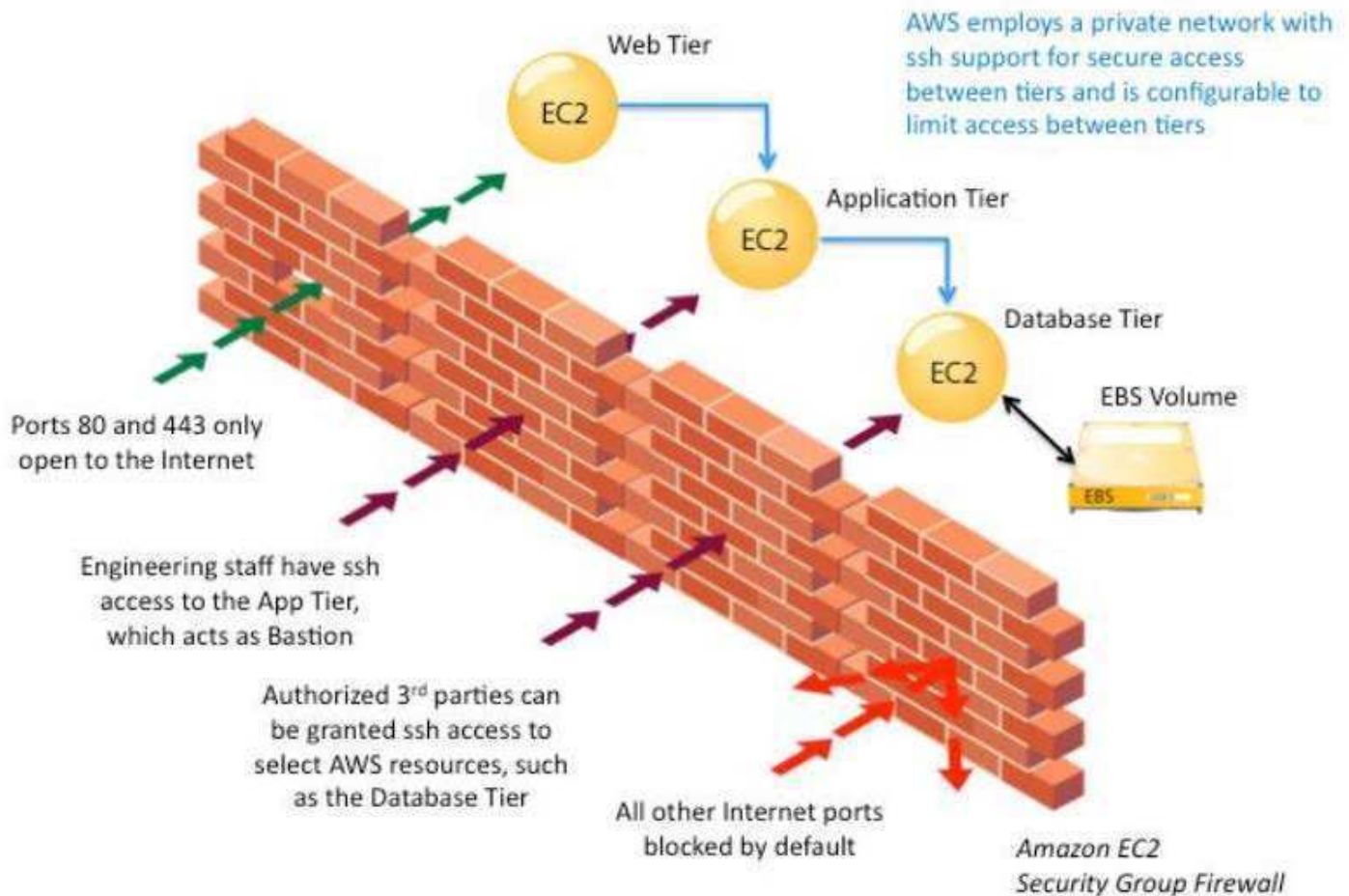
FIGURE 2 AMAZON EC2 MULTIPLE LAYERS OF SECURITY



Amazon EC2 provides a complete firewall solution; this mandatory inbound firewall is configured in a default deny-all mode and Amazon EC2 customers must explicitly open the ports needed to allow inbound traffic. The traffic may be restricted by protocol, by service port, as well as by source IP address (individual IP or Classless Inter-Domain Routing (CIDR) block).

The firewall can be configured in groups permitting different classes of instances to have different rules. Consider, for example, the case of a traditional three-tiered web application. The group for the web servers would have port 80 (HTTP) and/or port 443 (HTTPS) open to the Internet. The group for the application servers would have port 8000 (application specific) accessible only to the web server group. The group for the database servers would have port 3306 (MySQL) open only to the application server group. All three groups would permit administrative access on port 22 (SSH), but only from the customer's corporate network. Highly secure applications can be deployed using this expressive mechanism.

FIGURE 3 AMAZON EC2 SECURITY GROUP FIREWALL



The firewall isn't controlled through the guest OS; rather it requires your X.509 certificate and key to authorize changes, thus adding an extra layer of security. AWS supports the ability to grant granular access to different administrative functions on the instances and the firewall, therefore enabling you to implement additional security through separation of duties. The level of security afforded by the firewall is a function of which ports you open, and for what duration and purpose. The default state is to deny all incoming traffic, and you should plan carefully what you will open when building and securing your applications. Well-informed traffic management and security design are still required on a per-instance basis. AWS further encourages you to apply additional per-instance filters with host-based firewalls such as IPtables or the Windows Firewall and VPNs. This can restrict both inbound and outbound traffic.

8.5.2

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

TCC commits that our solutions comply with NIST regarding personally identifiable information (PII) and is committed to ensure and maintain the confidentiality and security of this data. TCC has developed Personnel Security policies that apply to the information systems, facilities, communications networks and information under the control of TCC. The policies apply equally to all users, including: management, end users, system owners, operators and administrators, developers, and third parties.

Based upon published standards, TCC has developed procedures to protect our clients' infrastructure and assets from unauthorized access, information disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft whether accidental or intentional.

These policies and procedures map directly to the NIST Personnel Security control criteria as defined in NIST Special Publication 800-53, Revision 4.

These policies and procedures are reviewed with our employees and compliance with the Information Security Procedures is mandatory. Failure to comply with the Information Security policy and associated standards and procedures can result in disciplinary action up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal action also may be taken for violations of applicable regulations and laws.

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.

TCC maintains policies that prohibit unauthorized 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.

8.6 (E) 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.

TCC commits that our solutions comply with NIST regarding personally identifiable information (PII) and is committed to ensure and maintain the confidentiality and security of this data. TCC has developed Personnel Security policies that apply to the information systems, facilities, communications networks and information under the control of TCC. The policies apply equally to all users, including: management, end users, system owners, operators and administrators, developers, and third parties.



Based upon published standards, TCC has developed procedures to protect our clients' infrastructure and assets from unauthorized access, information disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft whether accidental or intentional.

These policies and procedures map directly to the NIST Personnel Security control criteria as defined in NIST Special Publication 800-53, Revision 4.

These policies and procedures are reviewed with our employees and compliance with the Information Security Procedures is mandatory. Failure to comply with the Information Security policy and associated standards and procedures can result in disciplinary action up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal action also may be taken for violations of applicable regulations and laws.

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.

Amazon Web Services Compliance enables customers to understand the robust controls in place at AWS to maintain security and data protection in the cloud. As systems are built on top of AWS cloud infrastructure, compliance responsibilities will be shared. By tying together governance-focused, audit-friendly service features with applicable compliance or audit standards, AWS Compliance enablers build on traditional programs; helping customers to establish and operate in an AWS security control environment. The IT infrastructure that AWS provides to its customers is designed and managed in alignment with security best practices and a variety of IT security standards, including:

1. SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70)
2. SOC 2
3. SOC 3
4. FISMA, DIACAP, and FedRAMP
5. DOD CSM Levels 1-5
6. PCI DSS Level 1
7. ISO 9001 / ISO 27001
8. ITAR
9. FIPS 140-2
10. MTCS Level 3

In addition, the flexibility and control that the AWS platform provides allows customers to deploy solutions that meet several industry-specific standards, including:

1. Criminal Justice Information Services (CJIS)
2. Cloud Security Alliance (CSA)
3. Family Educational Rights and Privacy Act (FERPA)
4. Health Insurance Portability and Accountability Act (HIPAA)



5. Motion Picture Association of America (MPAA)

AWS provides a wide range of information regarding its IT control environment to customers through white papers, reports, certifications, accreditations, and other third-party attestations.

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.

Amazon Web Services is responsible for protecting the global infrastructure that runs all of the services offered in the AWS cloud. This infrastructure is comprised of the hardware, software, networking, and facilities that run AWS services. Protecting this infrastructure is AWS's number one priority, and while you can't visit our data centers or offices to see this protection firsthand, we provide several reports from third-party auditors who have verified our compliance with a variety of computer security standards and regulations (for more information, visit aws.amazon.com/compliance).

When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

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.).

AWS utilizes a wide variety of automated monitoring systems to provide a high level of service performance and availability. AWS monitoring tools are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts. The tools have the ability to set custom performance metrics thresholds for unusual activity.

The AWS network provides significant protection against traditional network security issues, and you can implement further protection. The following are a few examples:

Distributed Denial Of Service (DDoS) Attacks. AWS API endpoints are hosted on large, Internet-scale, world-class infrastructure that benefits from the same engineering expertise that has built Amazon into the world's largest online retailer. Proprietary DDoS mitigation techniques are used. Additionally, AWS's networks are multi-homed across a number of providers to achieve Internet access diversity.

Man in the Middle (MITM) Attacks. All of the AWS APIs are available via SSL-protected endpoints which provide server authentication. Amazon EC2 AMIs automatically generate new SSH host certificates on first boot and log them to the instance's console. You can then use the secure APIs to call the console and access the host

certificates before logging into the instance for the first time. We encourage you to use SSL for all of your interactions with AWS.

IP Spoofing. Amazon EC2 instances cannot send spoofed network traffic. The AWS-controlled, host-based firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own.

Port Scanning. Unauthorized port scans by Amazon EC2 customers are a violation of the AWS Acceptable Use Policy. Violations of the AWS Acceptable Use Policy are taken seriously, and every reported violation is investigated.

Packet sniffing by other tenants. It is not possible for a virtual instance running in promiscuous mode to receive or “sniff” traffic that is intended for a different virtual instance. While you can place your interfaces into promiscuous mode, the hypervisor will not deliver any traffic to them that is not addressed to them. Even two virtual instances that are owned by the same customer located on the same physical host cannot listen to each other’s traffic. Attacks such as ARP cache poisoning do not work within Amazon EC2 and Amazon VPC.

TCC’s Acceptable Use Policy is a universal policy that applies to all Users and all Systems. For some Users and/or some Systems a more specific policy exists: in such cases the more specific policy has precedence in areas where they conflict, but otherwise both policies apply on all other points.

This policy covers only internal use of TCC’s systems, and does not cover use of our products or services by customers or other third parties.

Some aspects of this policy affect areas governed by local legislation in certain countries (e.g., employee privacy laws): in such cases the need for local legal compliance has clear precedence over this policy within the bounds of that jurisdiction. In such cases local teams should develop and issue users with a clarification of how the policy applies locally.

Staff members at TCC who monitor and enforce compliance with this policy are responsible for ensuring that they remain compliant with relevant local legislation at all times.

8.6.5

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

Amazon Web Services Compliance enables customers to understand the robust controls in place at AWS to maintain security and data protection in the cloud. As systems are built on top of AWS cloud infrastructure, compliance responsibilities will be shared. By tying together governance-focused, audit-friendly service features with applicable compliance or audit standards, AWS Compliance enablers build on traditional programs; helping customers to establish and operate in an AWS security control environment. The IT infrastructure that AWS provides to its customers is designed and managed in alignment with security best practices and a variety of IT security standards, including:

11. SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70)
12. SOC 2
13. SOC 3
14. FISMA, DIACAP, and FedRAMP
15. DOD CSM Levels 1-5
16. PCI DSS Level 1
17. ISO 9001 / ISO 27001
18. ITAR
19. FIPS 140-2
20. MTCS Level 3

In addition, the flexibility and control that the AWS platform provides allows customers to deploy solutions that meet several industry-specific standards, including:

6. Criminal Justice Information Services (CJIS)
7. Cloud Security Alliance (CSA)
8. Family Educational Rights and Privacy Act (FERPA)
9. Health Insurance Portability and Accountability Act (HIPAA)
10. Motion Picture Association of America (MPAA)

AWS provides a wide range of information regarding its IT control environment to customers through white papers, reports, certifications, accreditations, and other third-party attestations.

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.

AWS CloudTrail is a web service that records AWS API calls for your account and delivers log files to you. The recorded information 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 AWS service.

With CloudTrail, you can get a history of AWS API calls for your account, including API calls made via the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS services (such as AWS CloudFormation). The AWS API call history produced by CloudTrail enables security analysis, resource change tracking, and compliance auditing.

8.6.7

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

AWS Identity and Access Management (IAM) enables control access to AWS service APIs and to specific resources. IAM also enables customers to add specific conditions such as time of day to control how a user can use AWS, their originating IP address, whether they are using SSL, or whether they have authenticated with a multi-factor authentication device.

IAM can be used to grant employees and applications federated access to the AWS Management Console and AWS service APIs, using your existing identity systems such as Microsoft Active Directory. You can use any identity management solution that supports SAML 2.0, or feel free to use one of our federation samples (AWS Console SSO or API federation).

AWS Multi Factor Authentication, a security feature available at no extra cost that augments user name and password credentials. MFA requires users to prove physical possession of a hardware MFA token or MFA-enabled mobile device by providing a valid MFA code.

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.

The Amazon Incident Management team employs industry-standard diagnostic procedures to drive resolution during business-impacting events. Staff operators provide 24x7x365 coverage to detect incidents and to manage the impact and resolution.

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.

Data centers are built in clusters in various global regions. All data centers are online and serving customers; no data center is “cold.” In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely.

Security within Amazon EC2 is provided on multiple levels: the operating system (OS) of the host platform, the virtual instance OS or guest OS, a firewall, and signed API calls. Each of these items builds on the capabilities of the others. The goal is to prevent data contained within Amazon EC2 from being intercepted by unauthorized systems or users and to

The Hypervisor

Amazon EC2 currently utilizes a highly customized version of the Xen hypervisor, taking advantage of paravirtualization (in the case of Linux guests). Because paravirtualized guests rely on the hypervisor to provide support for operations that normally require privileged access, the guest OS has no elevated access to the CPU. The CPU provides four separate privilege modes: 0-3, called *rings*. Ring 0 is the most privileged and 3 the least. The host OS executes in Ring 0. However, rather than executing in Ring 0 as most operating systems do, the guest OS runs in a lesser-privileged Ring 1 and applications in the least privileged Ring 3. This explicit virtualization of the physical resources leads to a clear separation between guest and hypervisor, resulting in additional security separation between the two.

Instance Isolation

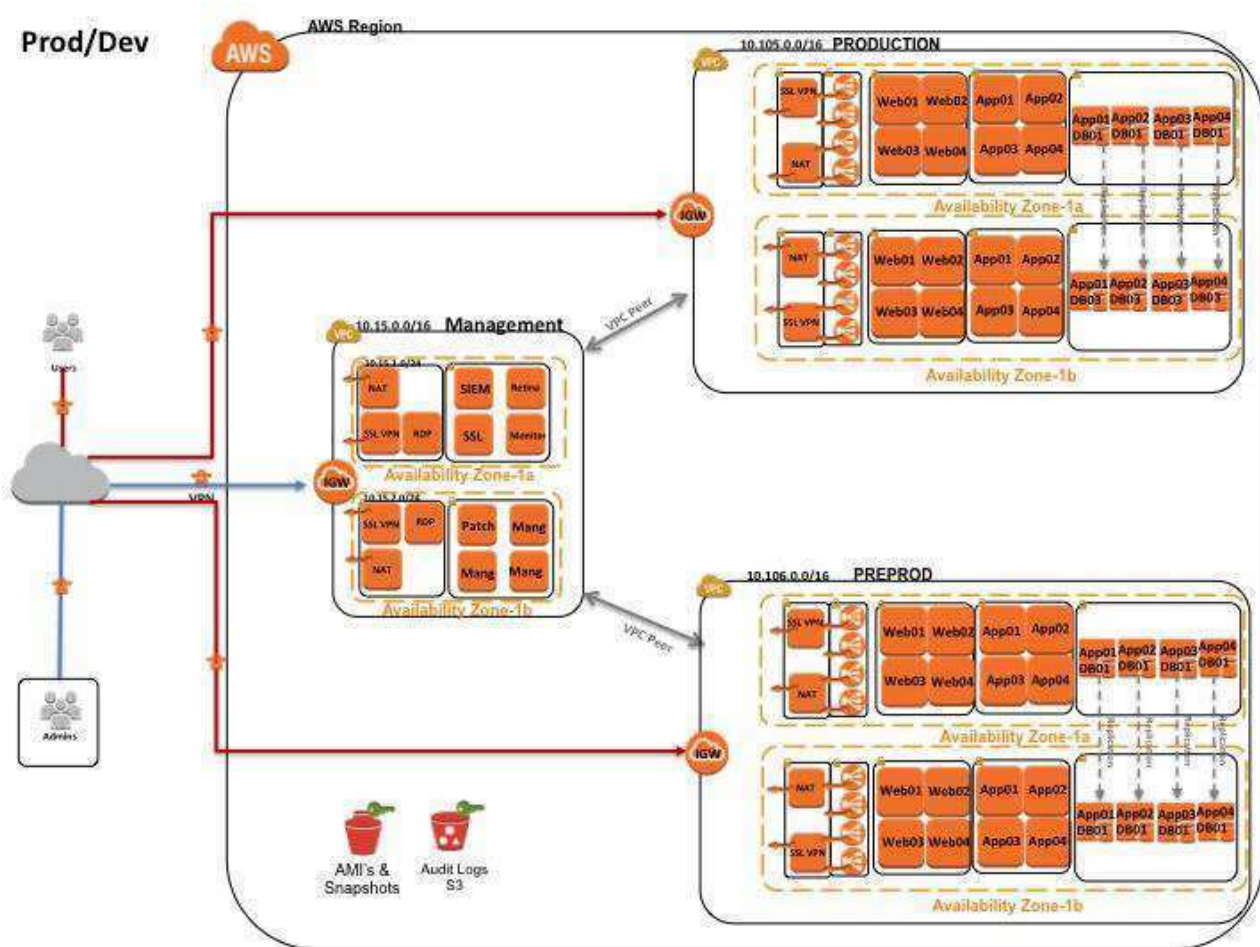
Different instances running on the same physical machine are isolated from each other via the Xen hypervisor. Amazon is active in the Xen community, which provides awareness of the latest developments. In addition, the AWS firewall resides within the hypervisor layer, between the physical network interface and the instance's virtual interface. All packets must pass through this layer, thus an instance's neighbors have no more access to that instance than any other host on the Internet and can be treated as if they are on separate physical hosts. The physical RAM is separated using similar mechanisms.

Customer instances have no access to raw disk devices, but instead are presented with virtualized disks. The AWS proprietary disk virtualization layer automatically resets every block of storage used by the customer, so that one customer's data is never unintentionally exposed to another. In addition, memory allocated to guests is scrubbed (set to zero) by the hypervisor when it is unallocated to a guest. The memory is not returned to the pool of free memory available for new allocations until the memory scrubbing is complete.

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).





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.

TCC uses Screening One as the service provider for background investigations. Screening One utilizes both public and private databases and records to provide background results on applicants. TCC is able to provide various levels of background screening through Screening One to meet agency requirements.

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.

AWS has several different methods of data storage including and not limited to S3, Glacier and other databases. Amazon Simple Storage Service (S3) allows you to upload and retrieve data at any time, from anywhere on the web. Amazon S3 stores data as objects within buckets. An object can be any kind of file: a text file, a photo, a video, etc. When you add a file to Amazon S3, you have the option of including metadata with the file and setting permissions to control access to the file. For each bucket, you can control access to the bucket (who can

create, delete, and list objects in the bucket), view access logs for the bucket and its objects, and choose the geographical region where Amazon S3 will store the bucket and its contents.

For maximum security, you can securely upload/download data to Amazon S3 via the SSL encrypted endpoints. The encrypted endpoints are accessible from both the Internet and from within Amazon EC2, so that data is transferred securely both within AWS and to and from sources outside of AWS.

Amazon S3 provides multiple options for protecting data at rest. For customers who prefer to manage their own encryption, they can use a client encryption library like the Amazon S3 Encryption Client to encrypt data before uploading to Amazon S3. Alternatively, you can use Amazon S3 Server Side Encryption (SSE) if you prefer to have Amazon S3 manage the encryption process for you. Data is encrypted with a key generated by AWS or with a key you supply, depending on your requirements. With Amazon S3 SSE, you can encrypt data on upload simply by adding an additional request header when writing the object. Decryption happens automatically when data is retrieved.

Like Amazon S3, the Amazon Glacier service provides low-cost, secure, and durable storage. But where Amazon S3 is designed for rapid retrieval, Glacier is meant to be used as an archival service for data that is not accessed often and for which retrieval times of several hours are suitable.

Amazon Glacier stores files as archives within vaults. Archives can be any data such as a photo, video, or document, and can contain one or several files. You can store an unlimited number of archives in a single vault and can create up to 1,000 vaults per region. Each archive can contain up to 40 TB of data.

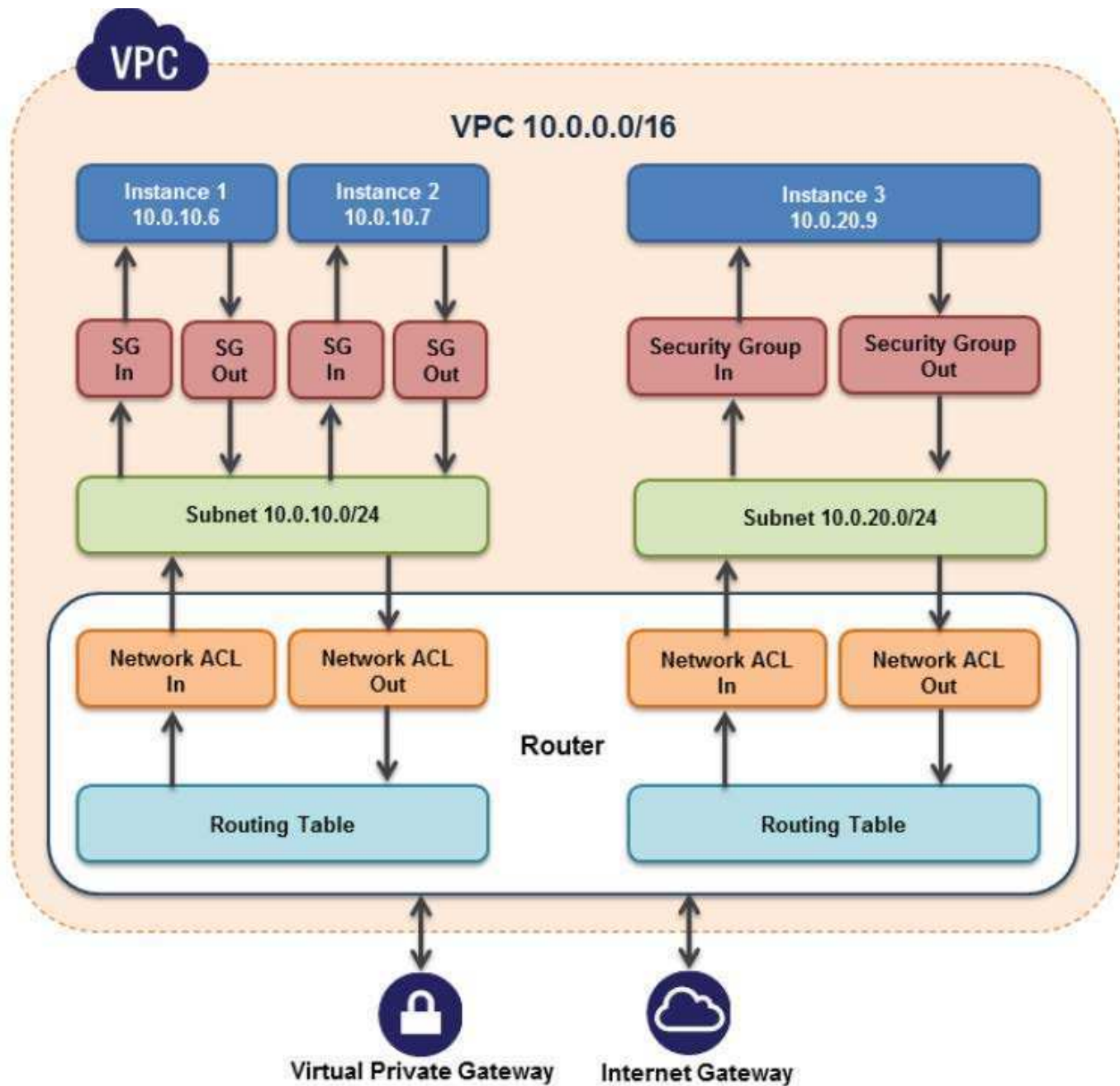
Amazon Glacier automatically encrypts the data using AES-256 and stores it durably in an immutable form. Amazon Glacier is designed to provide average annual durability of 99.999999999% for an archive. It stores each archive in multiple facilities and multiple devices. Unlike traditional systems which can require laborious data verification and manual repair, Glacier performs regular, systematic data integrity checks and is built to be automatically self-healing.

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.



FIGURE 4 FLEXIBLE NETWORK TOPOLOGIES AND INSTANCE SECURITY



8.7 (E) 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.

Transition Out Acceptance Criteria

Prior to beginning Transition Out activities, all parties will need to agree upon suitable acceptance criteria. These criteria will be identified, documented, and agreed to by all parties prior to the initiation of Transition Out activities.

Transition Out Deliverables

As part of the overall Transition Plan, the team will develop a separate document describing all turnover deliverables and the scheduled date(s) for transfer to the agency or its designee.

Knowledge Transfer Plan

Our team understands that transitioning is a process that requires sufficient planning methods as well as resources to ensure a successful and responsible transfer. The key to planning this initiative is to establish a methodology framework which fosters a respectful and yet aggressive transition schedule. Over the course of the transition period, our team works closely with the client to ensure that a successful knowledge transfer occurs and ongoing operations remain stable.

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.

Knowledge Transfer Plan

Our team understands that transitioning is a process that requires sufficient planning methods as well as resources to ensure a successful and responsible transfer. The key to planning this initiative is to establish a methodology framework which fosters a respectful and yet aggressive transition schedule. Over the course of the transition period, our team works closely with the client to ensure that a successful knowledge transfer occurs and ongoing operations remain stable.

8.8 (E) 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.

Communication plans are a part of downtime policies and procedures. Communicating planned and semi-planned downtime to staff in advance will minimize frustration and confusion as to why the system is unavailable. TCC will communicate to the affected entities for continued information.

b. Suffers an unrecoverable loss of data.

Amazon S3 and EBS is designed to provide 99.999999999% durability and 99.99% availability of objects over a given year. Objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 region. To help provide durability, Amazon S3 PUT and COPY operations synchronously store customer data across multiple facilities before returning SUCCESS. Once stored, Amazon S3 helps maintain the durability of the objects by quickly detecting and repairing any lost redundancy. Amazon S3 also regularly verifies the integrity of data stored using checksums. If corruption is detected, it is repaired using redundant data. In addition, Amazon S3 calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data.

While the durability of S3 and EBS is significant TCC recommends that Purchasing entities still maintain backups as part of a data protection best practice.

c. Offeror experiences a system failure.

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

Depending on the method of data protection most events can be met with data recover as stated within the contract however should the degree of data recover exceed normal (multiple terabytes) the timeframe will change as needed.

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

Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are one of the most important parameters of a disaster recovery or data protection plan. These objectives guide the enterprises to choose an optimal data backup (rather restore) plan.

Recovery Point Objective (RPO) describes the interval of time that might pass during a disruption before the quantity of data lost during that period exceeds the Business Continuity Plan's maximum allowable threshold or "tolerance."

The Recovery Time Objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity.

TCC will work with the Purchasing entity to determine correct RPOs and RTOs that meet the requirements of the Purchasing entities needs.

8.8.2

Describe your methodologies for the following backup and restore services:

a. Method of data backups

TCC employs a data backup strategy that encompasses the customer requirements. This backup solution provides the flexibility to incorporate incremental and differential, file level and block level, and both dedupe and compression. Depending on the needs of the client TCC will craft a backup solution to meet customer ends.

b. Method of server image backups

The Amazon Elastic Compute Cloud (Amazon EC2) service enables the backup and recovery of a standard server, such as a web server or application server, so that you can focus on protecting configuration and stateful data—rather than the server itself. This set of data is much smaller than the aggregate set of server data, which typically includes various application files, operating system files, temporary files, and so on. This change of approach means that regular nightly incremental or weekly full backups can take far less time and consume less storage space. When a compute instance is started in Amazon EC2, it is based upon an Amazon Machine Image (AMI)² and can also connect to existing storage volumes—for example, Amazon Elastic Block Store (Amazon EBS)³. In addition, when launching a new instance, it is possible to pass “user data”⁴ to the instance that can be accessed internally as dynamic configuration parameters.

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

Amazon S3 offers a range of storage classes designed for different use cases including Amazon S3 Standard for general-purpose storage of frequently accessed data, Amazon S3 Standard - Infrequent Access (Standard - IA) for long-lived, but less frequently accessed data, and Amazon Glacier for long-term archive. Amazon S3 also offers configurable lifecycle policies for managing your data throughout its lifecycle. Once a policy is set, your data will automatically migrate to the most appropriate storage class without any changes to your applications.

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

AWS provides you with the flexibility to place instances and store data within multiple geographic regions as well as across multiple availability zones within each region. Each availability zone is designed as an independent failure zone. This means that availability zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by region). In addition to utilizing discrete uninterruptable power supply (UPS) and onsite backup generators, they are each fed via different grids from independent utilities to further reduce single points of failure. Availability zones are all redundantly connected to multiple tier-1 transit providers. There are multiple regions: US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US).

8.9 (E) 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.

Encryption of sensitive data is generally a good security practice, and AWS provides the ability to encrypt Amazon Elastic Block Storage volumes and their snapshots with AES-256. The encryption occurs on the servers that host the EC2 instances, providing encryption of data as it moves between EC2 instances and EBS storage.

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.

TCC is willing to sign a relevant and applicable Business Associate Agreement or any other agreement that may be necessary to protect data with a Purchasing Entity.

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.

TCC agrees that we will only use data for purposes defined in the Master Agreement, participating addendum, or related service level agreement.

8.10 (E) 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.

TCC's Service Level Agreement is negotiable and has been included with our response.

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.

TCC performs due diligence through meetings and cooperation with the Purchasing Entity to determine the sensitivity of the data that will be managed and how to protect it. TCC is prepared to perform Data Discovery exercises to help the Purchasing Entity find and protect sensitive information quickly and cost effectively. TCC has experience working with highly sensitive data and knows where it should reside within the environments.

TCC has provide a copy of our Service Level Agreement template in Appendix B of this proposal.

8.11 (E) Data Disposal

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

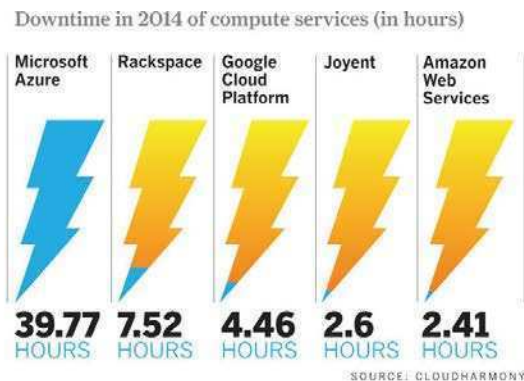
Amazon Elastic Block Storage volumes are presented to you as raw unformatted block devices that have been wiped prior to being made available for use. Wiping occurs immediately before reuse so that you can be assured that the wipe process completed. If you have procedures requiring that all data be wiped via a specific method, such as those detailed in DoD 5220.22-M (“National Industrial Security Program Operating Manual”) or NIST 800-88 (“Guidelines for Media Sanitization”), you have the ability to do so on Amazon EBS. You should conduct a specialized wipe procedure prior to deleting the volume for compliance with your established requirements.

8.12 (E) 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.

EC2 in all 4 regions as of 2015 uptime of 99.989% in EU West, 99.997% in APAC and 100% in US East and West.



8.12.2

Provide your standard uptime service and related Service Level Agreement (SLA) criteria.

Coverage parameters specific to the service(s) covered in this Agreement are as follows:

- **Service Availability – General.** TCC’s goal is to provide Service Availability twenty-four hours per day, seven (7) days per week (referred to as “24x7 Availability”) EXCEPT during times of Service Maintenance as set forth in Section 4.3 herein. However, the parties recognize that 24x7 Availability is only a GOAL, and TCC cannot represent or guarantee that such goal can be achieved. As per TCC’s CLOUD SUPPORT POLICY (show below), response time goals cover predominantly Production Clouds.
- **Service Availability Level Goals.** TCC shall use reasonable efforts to achieve the target Service Availability Goal of 99.99% network uptime except during Scheduled Service Maintenance. Notwithstanding the foregoing, the Customer recognizes that the Internet is comprised of thousands upon thousands of autonomous systems that are beyond the control of TCC. Routing anomalies, asymmetries, inconsistencies and failures of the Internet outside of the control of TCC can and will occur, and such instances shall not be considered any failure of the 99.99% network uptime. While the Customer is free to monitor network uptime on their systems and other

monitoring services, TCC proactively monitors network uptime and the results of these monitoring systems shall provide the sole and exclusive determination of network uptime.

- Response Time to Error. TCC has internal notification tools for Cloud service problems. Additionally, the Customer may report problems to TCC Support. Once notified TCC Support will respond as per the CLOUD SUPPORT POLICY (show below). Note that these guidelines specify the time to begin investigation of the problem, not the length of time within which such problem are resolved.

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.

Technical support consists of remote assistance provided by TCC with support requests and includes email and phone support during standard business hours. TCC's standard business hours are 8AM – 5PM EST, except for holidays observed by TCC. Additionally, TCC provides 24x7x365 on-call support for production clouds. Support for non-standard hours is available upon request and at a negotiable cost. Technical support is provided for problems that are demonstrable in the current and supported TCC managed environments, running unaltered on appropriate hardware and operating system configured as specified in the TCC documentation. TCC shall only be obligated to provide support for the services delivered by TCC. TCC shall have no obligation to provide maintenance for any software that has been altered or modified by any party, other than TCC.

The TCC Helpdesk operates to the ITIL ITSM Framework and processes, which follows the standard support request model of process, assign, solve, close, and notify for end-user problems or requests. Additionally, TCC logs and tracks the problems or requests and continually analyzes and determines the best manner to address the problems or requests for continual service improvement. One of the top priorities of the TCC Helpdesk is to ensure a consistent response to problem resolution, service requests, status reporting and notification of changes. It is important that when submitting a request to the TCC Helpdesk the certain required information is provided. That list includes, but not limited to a completed description of the issue, steps to reproduce, timeline, environment issue is occurring in, impact to the business, and any attachments including screenshots and log files.

8.12.4

Describe the consequences/SLA remedies if the Respondent fails to meet incident response time and incident fix time.

In the event that TCC fails to meet the mutually agreed upon response times a negotiated financial penalty structure will be used as consequence to those SLA violations. An analysis of the reasons for a response failure will be performed and improvement steps will be taken to minimize any future issues, if warranted.

TCC will always endeavor to resolve problems as swiftly as possible. It recognizes that the client's computer systems are key to its business and that any downtime can cost money. However, the supplier is unable to provide guaranteed resolution times. This is because the nature and causes of problems can vary enormously. For instance, it may be possible to resolve a fatal server issue in minutes, simply by restarting the server. But if a server fails due to disk error or a hardware fault (also classed as a fatal issue) it may take much longer to get

back up and running. TCC will make its best efforts to resolve problems as quickly as possible. It will also provide frequent progress reports to the client.

8.12.5

Describe the firm's procedures and schedules for any planned downtime.

TCC shall provide scheduled and preventative maintenance with the schedule based on the balanced needs of the Customer, the software and the equipment. TCC shall use commercially reasonable efforts to limit Service Maintenance and minimize the impact on system availability.

The process for notification of planned network and/or service downtimes is as follows:

1. Once a downtime date/time span has been determined, the customer will be notified via email 1 week in advance of the planned downtime. This notification will include purpose of the downtimes; the systems, networks, or services that will be unavailable or otherwise impacted; the day/date start and end times of the downtime; and contact information for the individual or office coordinating the downtime. The customer reserves the right to cancel the planned downtime up to the moment of the downtime for reasons including, but not limited to, customer support issues/events, presentations, demos, and other conflicts.
2. Official downtime notifications are shared with the stakeholders who will be affected by the outage via email using the "downtime-notices" communication list. Communication will also be sent to the Customer's Technology Support Center. The notification will include the purpose of the downtimes; the systems, networks, or services that will be unavailable or otherwise impacted; the day/date start and end times of the downtime; and contact information for the individual or office coordinating the downtime.
3. Upon completion of the downtime, notice will be sent to the "downtime-notices" list, the Technology Support Center, and the customer confirming its conclusion and the restoration of impacted services.

TCC shall attempt to schedule Service Maintenance during the times as specified in Table 1 – Service Maintenance Times. However, the parties agree that it may be necessary for TCC to perform Service Maintenance during times other than those specified in Table 1, and TCC reserves the right to perform Service Maintenance during times other than those specified in Table 1.

Table 1 – Service Maintenance Times

Service Maintenance Times (Day)	Service Maintenance Times (Hours)
Monday to Friday	8pm to 4am (EST)
Saturday	12pm to 12 am (EST)
Sunday	12pm to 12 am (EST)

8.12.6

Describe the consequences/SLA remedies if disaster recovery metrics are not met.

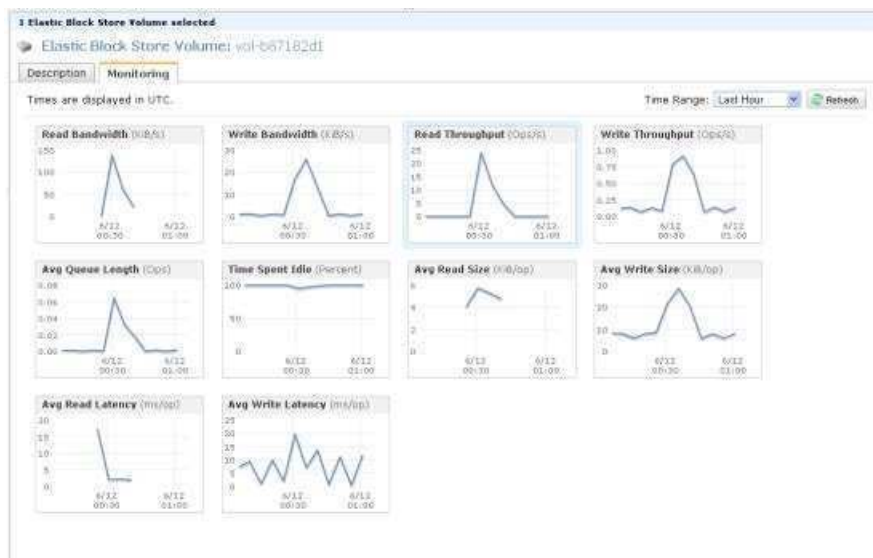
In the event that TCC fails to meet disaster recovery metrics a negotiated financial penalty structure will be used as consequence to those SLA violations. An analysis of the reasons for a DR metric failure will be performed and improvement steps will be taken to minimize any future issues, if warranted.

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.

Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS. You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in your AWS resources. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by your applications and services, and any log files your applications generate. CloudWatch is available over the Web.

CloudWatch Logs monitor and troubleshoot your systems and applications using your existing system, application, and custom log files. You can send your existing system, application, and custom log files to CloudWatch Logs and monitor these logs in near real-time (minimum increments at 60 seconds, standard aggregates at 5 minutes). This can help you better understand and operate your systems and applications, and you can store your logs using highly durable, low-cost storage for later access.



Log Groups > Streams for /var/log/messages > Events for pcf_poc

Date/Time:	2015/04/22 15:34:02 UTC (GMT)
Creation Time	Event Data
2015-04-22 15:34:02 UTC	Apr 22 15:34:02 10.0.16.20 vcap.warden [job=dea-partition-9f1f61
2015-04-22 15:34:03 UTC	Apr 22 15:34:03 10.0.16.24 vcap.hm9000.sender [job=health_manage
2015-04-22 15:34:03 UTC	Apr 22 15:34:03 10.0.16.23 vcap.cloud_controller_ng [job=cloud_c
2015-04-22 15:34:03 UTC	Apr 22 15:34:03 10.0.16.24 vcap.hm9000.sender [job=health_manage
2015-04-22 15:34:03 UTC	Apr 22 15:34:03 10.0.16.24 vcap.hm9000.sender [job=health_manage
2015-04-22 15:34:03 UTC	Apr 22 15:34:03 10.0.16.20 vcap.warden [job=dea-partition-9f1f61
2015-04-22 15:34:03 UTC	Apr 22 15:34:03 10.0.16.13 vcap.cloud_controller_ng [job=cloud_c
2015-04-22 15:34:05 UTC	Apr 22 15:34:05 10.0.16.24 vcap.hm9000.listener [job=health mana
2015-04-22 15:34:06 UTC	Apr 22 15:34:06 10.0.16.13 vcap.cloud_controller_ng [job=cloud_c
2015-04-22 15:34:06 UTC	Apr 22 15:34:06 10.0.16.13 vcap.cloud_controller_ng [job=cloud_c
2015-04-22 15:34:06 UTC	Apr 22 15:34:06 10.0.16.13 vcap.cloud_controller_ng [job=cloud_c
2015-04-22 15:34:06 UTC	Apr 22 15:34:06 10.0.16.20 vcap.warden [job=dea-partition-9f1f61
2015-04-22 15:34:06 UTC	Apr 22 15:34:06 10.0.16.20 vcap.warden [job=dea-partition-9f1f61
2015-04-22 15:34:06 UTC	Apr 22 15:34:06 10.0.16.20 vcap.warden [job=dea-partition-9f1f61

8.12.8

Ability to print historical, statistical, and usage reports locally.

Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS. You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in your AWS resources. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by your applications and services, and any log files your applications generate.

AWS CloudTrail is a web service that records AWS API calls for your account and delivers log files to you. The recorded information 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 AWS service. With CloudTrail, you can get a history of AWS API calls for your account, including API calls made via the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS services (such as AWS CloudFormation). The AWS API call history produced by CloudTrail enables security analysis, resource change tracking, and compliance auditing.

8.12.9

Offeror must describe whether or not its on-demand deployment is supported 24x365.

AWS is available as an on-demand deployment that is supported 24x365. AWS is built to allow Purchasing Entities the availability to deploy, modify, and change their environment 24x7x365.

8.12.10

Offeror must describe its scale-up and scale-down, and whether it is available 24x365.

As needs change, you might find that your instance is over-utilized (the instance type is too small) or under-utilized (the instance type is too large). If this is the case, you can change the size of your instance. When you resize an instance, you must select an instance type that is compatible with the configuration of the instance. If the instance type that you want is not compatible with the instance configuration you have, then you must migrate your application to a new instance with the instance type that you want.

8.13 (E) Cloud Security Alliance

Describe your level disclosure of compliance with CSA Star Registry for each Solution offered.

- a. *Completion of a CSA STAR Self-Assessment, as described in Section 5.5.3.*
- b. *Completion of Exhibits 1 and 2 to Attachment B.*
- c. *Completion of a CSA STAR Attestation, Certification, or Assessment.*
- d. *Completion CSA STAR Continuous Monitoring.*

A report documenting AWS risk and compliance with the Cloud Controls Matrix (CCM) of Attachment B, Exhibit 2 has been included as Appendix A to this document.

8.14 (E) Service Provisioning

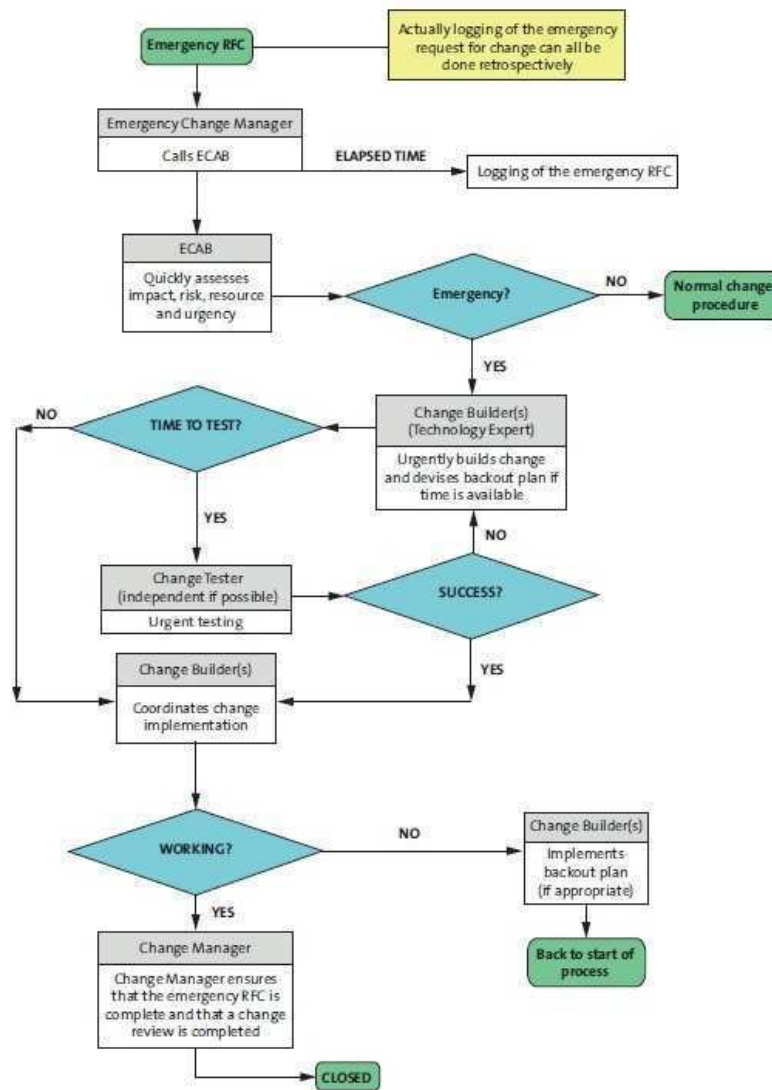
8.14.1

Describe in detail how your firm processes emergency or rush services implementation requests by a Purchasing Entity.

The number of emergency changes should be kept to an absolute minimum, because they are generally more disruptive and prone to failure.

However, there will be occasions when emergency changes are essential and so the emergency change process and underpinning procedure has been documented to deal with these types of changes quickly, without sacrificing normal management controls.

The process diagram for the emergency change process is shown below.



Emergency changes will only be accepted for one of the following two reasons:

- To correct any issue/issue(s) on a business critical system or service
- To protect the business/organization

The ECAB (Emergency Change Advisory Board) need to ensure that the request for emergency change is in line with one of the two reasons given above.

Only the IT teams have access to the request for change form to initiate emergency changes. However, it is common that as the change is needed urgently that the emergency request can be made to the Change Manager verbally so that the ECAB can be called immediately. All documentation within the emergency RFC can be done retrospectively for emergency changes.

Approved emergency changes will be allocated to the relevant technical group for building. The Change Manager, in collaboration with the appropriate technical manager(s), will ensure that sufficient staff and resources (machine time etc.) are available to do the emergency change. Back out plans will still be devised despite the urgency of implementing emergency change.

As much testing of the emergency change as is possible will be carried out. Completely untested changes will not be implemented if at all avoidable.

The emergency change management process will give as much advance warning as possible to customers and users about any imminent emergency changes. This will be done via the service desk. When any emergency changes are implemented, particularly those that have not been adequately tested, change management will ensure that an adequate technical presence is available to tackle any Incidents that may occur after the emergency change has been implemented.

8.14.2

Describe in detail the standard lead-time for provisioning of your Solution.

Each client's lead time for provisioning varies on the nature of the statement of work. TCC follows proven processes for provisioning that can vary from hours to days to weeks based on the complexity of the project. Please see TCC's submitted sample project plans and work breakdown structures in Appendix E for a sample of steps utilized for our projects.

8.15 (E) Backup and Disaster Plan

8.15.1

Ability to apply legal retention periods and disposition by agency per purchasing entity policy and/or legal requirements.

RPO and RTO are predominately set by customer expectations and risk tolerance. TCC currently manages a number of clients with differing RPO and RTO SLAs and uses a variety of dedup, synthetic full and disk to disk style backups with snapshots to meet customer requirements.

8.15.2

Describe any known inherent disaster recovery risks and provide potential mitigation strategies.

TCC architects your AWS usage to take advantage of multiple regions and availability zones. Distributing applications across multiple availability zones provides the ability to remain resilient in the face of most failure scenarios, including natural disasters or system failures. However, you should be aware of location-dependent privacy and compliance requirements, such as the EU Data Privacy Directive. Data is not replicated between regions unless proactively done so by the customer, thus allowing customers with these types of data placement and privacy requirements the ability to establish compliant environments. It should be noted that all communications between regions is across public Internet infrastructure; therefore, appropriate encryption methods should be used to protect sensitive data.

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.

Data centers are built in clusters in various global *regions*. All data centers are online and serving customers; no data center is “cold.” In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

AWS provides you with the flexibility to place instances and store data within multiple geographic regions as well as across multiple availability zones within each region. Each availability zone is designed as an independent failure zone. This means that availability zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by region). In addition to utilizing discrete uninterruptable power supply (UPS) and onsite backup generators, they are each fed via different grids from independent utilities to further reduce single points of failure. Availability zones are all redundantly connected to multiple tier-1 transit providers.

8.16 (E) Solution Administration

8.16.1

Ability of the Purchasing Entity to fully manage identity and user accounts.

AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

8.16.2

Ability to provide anti-virus protection, for data stores.

Trend Micro Deep Security as a Service delivers hosted security capabilities for cloud environments, including proactive intrusion detection and prevention (IDS/IPS), firewall, anti-malware, web reputation, log inspection, and integrity monitoring. Manage all these controls from a single console and with a single light-weight agent, seamlessly integrated with leading cloud providers like AWS

8.16.3

Ability to migrate all Purchasing Entity data, metadata, and usage data to a successor Cloud Hosting solution provider.

AWS and TCC provide the ability to migrate customer data to a successor cloud.

8.16.4

Ability to administer the solution in a distributed manner to different participating entities.

AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

8.16.5

Ability to apply participating entity defined administration policies in managing solution.

AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources. Utilizing IAM TCC can allow customers to manager portions or all components of their environment.

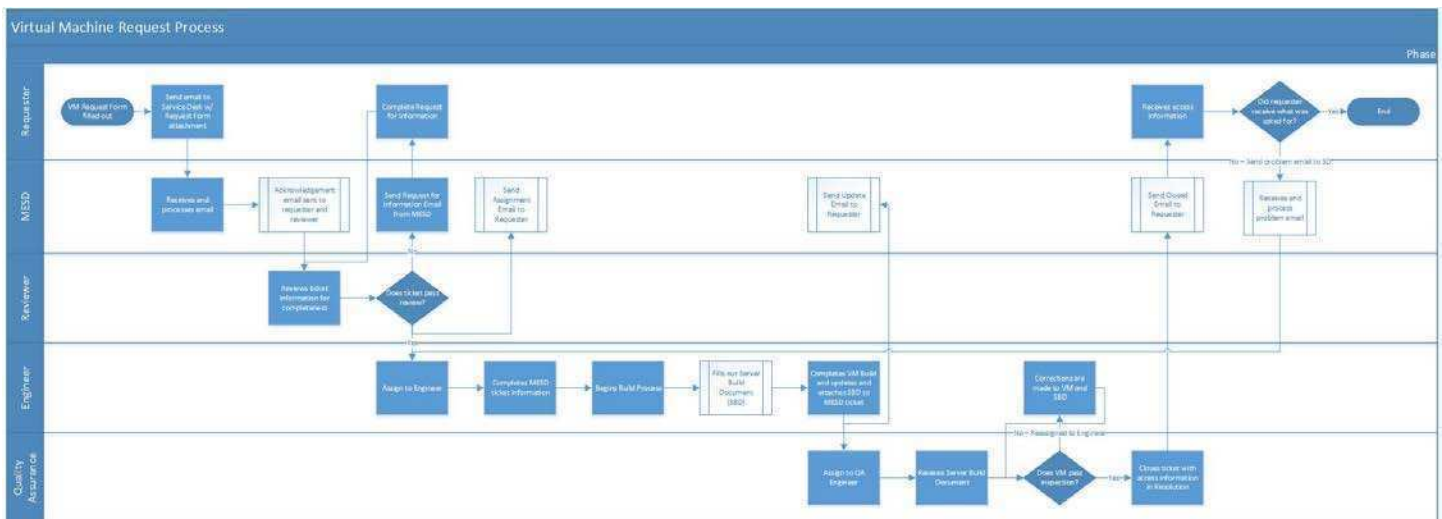
8.17 (E) Hosting and Provisioning

8.17.1

Documented cloud hosting provisioning processes, and your defined/standard cloud provisioning stack.

TCC utilizes different types of provisioning and works with each individual customer to arrive at the most effective solution. Whether it is with advance provisioning, dynamic provisioning or automation and self-service, TCC strives to optimize the process through the entire cloud lifecycle.

TCC uses a standard service request model to facilitate provisioning requests. Below is new virtual machine request workflow model.



8.17.2

Provide tool sets at minimum for:

- Deploying new servers (determining configuration for both stand alone or part of an existing server farm, etc.) AWS EC2 Catalogue*

b. Creating and storing server images for future multiple deployments

An Amazon Machine Image (AMI) provides the information required to launch an instance, which is a virtual server in the cloud. You specify an AMI when you launch an instance, and you can launch as many instances from the AMI as you need. You can also launch instances from as many different AMIs as you need.

An AMI includes the following:

- A template for the root volume for the instance (for example, an operating system, an application server, and applications)
- Launch permissions that control which AWS accounts can use the AMI to launch instances
- A block device mapping that specifies the volumes to attach to the instance when it's launched

Instance Type	vCPU	Memory (GiB)	Storage (GB)	Networking Performance	Physical Processor	Clock Speed (GHz)	Intel AVX+	Intel AVX2 ⁺	Intel Turbo	EBS OPT	Enhanced Networking ⁺
t2.nano	1	0.5	EBS Only	Low	Intel Xeon family	up to 3.3	Yes	-	Yes	-	-
t2.micro	1	1	EBS Only	Low to Moderate	Intel Xeon family	Up to 3.3	Yes	-	Yes	-	-
t2.small	1	2	EBS Only	Low to Moderate	Intel Xeon family	Up to 3.3	Yes	-	Yes	-	-
t2.medium	2	4	EBS Only	Low to Moderate	Intel Xeon family	Up to 3.3	Yes	-	Yes	-	-
t2.large	2	8	EBS Only	Low to Moderate	Intel Xeon family	Up to 3.0	Yes	-	Yes	-	-
m4.large	2	8	EBS Only	Moderate	Intel Xeon E5-2676 v3	2.4	Yes	Yes	Yes	Yes	Yes
m4.xlarge	4	16	EBS Only	High	Intel Xeon E5-2676 v3	2.4	Yes	Yes	Yes	Yes	Yes
m4.2xlarge	8	32	EBS Only	High	Intel Xeon E5-2676 v3	2.4	Yes	Yes	Yes	Yes	Yes
m4.4xlarge	16	64	EBS Only	High	Intel Xeon E5-2676 v3	2.4	Yes	Yes	Yes	Yes	Yes
m4.10xlarge	40	160	EBS Only	10 Gigabit	Intel Xeon E5-2676 v3	2.4	Yes	Yes	Yes	Yes	Yes
m3.medium	1	3.75	1 x 4 SSD	Moderate	Intel Xeon E5-2670 v2*	2.5	Yes	-	Yes	-	-

Instance Type	vCPU	Memory (GiB)	Storage (GB)	Networking Performance	Physical Processor	Clock Speed (GHz)	Intel AVX+	Intel AVX2 ⁺	Intel Turbo	EBS OPT	Enhanced Networking ⁺
m3.large	2	7.5	1 x 32 SSD	Moderate	Intel Xeon E5-2670 v2*	2.5	Yes	-	Yes	-	-
m3.xlarge	4	15	2 x 40 SSD	High	Intel Xeon E5-2670 v2*	2.5	Yes	-	Yes	Yes	-
m3.2xlarge	8	30	2 x 80 SSD	High	Intel Xeon E5-2670 v2*	2.5	Yes	-	Yes	Yes	-
c4.large	2	3.75	EBS Only	Moderate	Intel Xeon E5-2666 v3	2.9	Yes	Yes	Yes	Yes	Yes
c4.xlarge	4	7.5	EBS Only	High	Intel Xeon E5-2666 v3	2.9	Yes	Yes	Yes	Yes	Yes
c4.2xlarge	8	15	EBS Only	High	Intel Xeon E5-2666 v3	2.9	Yes	Yes	Yes	Yes	Yes
c4.4xlarge	16	30	EBS Only	High	Intel Xeon E5-2666 v3	2.9	Yes	Yes	Yes	Yes	Yes
c4.8xlarge	36	60	EBS Only	10 Gigabit	Intel Xeon E5-2666 v3	2.9	Yes	Yes	Yes	Yes	Yes
c3.large	2	3.75	2 x 16 SSD	Moderate	Intel Xeon E5-2680 v2	2.8	Yes	-	Yes	-	Yes
c3.xlarge	4	7.5	2 x 40 SSD	Moderate	Intel Xeon E5-2680 v2	2.8	Yes	-	Yes	Yes	Yes
c3.2xlarge	8	15	2 x 80 SSD	High	Intel Xeon E5-2680 v2	2.8	Yes	-	Yes	Yes	Yes
c3.4xlarge	16	30	2 x 160 SSD	High	Intel Xeon E5-2680 v2	2.8	Yes	-	Yes	Yes	Yes
c3.8xlarge	32	60	2 x 320 SSD	10 Gigabit	Intel Xeon E5-2680 v2	2.8	Yes	-	Yes	-	Yes
g2.2xlarge	8	15	1 x 60 SSD	High	Intel Xeon E5-2670	2.6	Yes	-	Yes	Yes	-
g2.8xlarge	32	60	2 x 120 SSD	10 Gigabit	Intel Xeon E5-2670	2.6	Yes	-	Yes	-	-
r3.large	2	15.25	1 x 32 SSD	Moderate	Intel Xeon E5-2670 v2	2.5	Yes	-	Yes	-	Yes

Instance Type	vCPU	Memory (GiB)	Storage (GB)	Networking Performance	Physical Processor	Clock Speed (GHz)	Intel AVX+	Intel AVX2 ⁺	Intel Turbo	EBS OPT	Enhanced Networking ⁺
r3.xlarge	4	30.5	1 x 80 SSD	Moderate	Intel Xeon E5-2670 v2	2.5	Yes	-	Yes	Yes	Yes
r3.2xlarge	8	61	1 x 160 SSD	High	Intel Xeon E5-2670 v2	2.5	Yes	-	Yes	Yes	Yes
r3.4xlarge	16	122	1 x 320 SSD	High	Intel Xeon E5-2670 v2	2.5	Yes	-	Yes	Yes	Yes
r3.8xlarge	32	244	2 x 320 SSD	10 Gigabit	Intel Xeon E5-2670 v2	2.5	Yes	-	Yes	-	Yes
i2.xlarge	4	30.5	1 x 800 SSD	Moderate	Intel Xeon E5-2670 v2	2.5	Yes	-	Yes	Yes	Yes
i2.2xlarge	8	61	2 x 800 SSD	High	Intel Xeon E5-2670 v2	2.5	Yes	-	Yes	Yes	Yes
i2.4xlarge	16	122	4 x 800 SSD	High	Intel Xeon E5-2670 v2	2.5	Yes	-	Yes	Yes	Yes
i2.8xlarge	32	244	8 x 800 SSD	10 Gigabit	Intel Xeon E5-2670 v2	2.5	Yes	-	Yes	-	Yes
d2.xlarge	4	30.5	3 x 2000	Moderate	Intel Xeon E5-2676 v3	2.4	Yes	Yes	Yes	Yes	Yes
d2.2xlarge	8	61	6 x 2000	High	Intel Xeon E5-2676 v3	2.4	Yes	Yes	Yes	Yes	Yes
d2.4xlarge	16	122	12 x 2000	High	Intel Xeon E5-2676 v3	2.4	Yes	Yes	Yes	Yes	Yes
d2.8xlarge	36	244	24 x 2000	10 Gigabit	Intel Xeon E5-2676 v3	2.4	Yes	Yes	Yes	Yes	Yes

c. Securing additional storage space

You can increase the storage space of an existing EBS volume without losing the data on the volume. To do this, you migrate your data to a larger volume and then extend the file system on the volume to recognize the newly-available space. After you verify that your new volume is working properly, you can delete the old volume.

d. 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).

Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS. You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and

automatically react to changes in your AWS resources. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by your applications and services, and any log files your applications generate. You can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health. You can use these insights to react and keep your application running smoothly.

8.17.3

Ability to provide IaaS, PaaS, and SaaS services as defined service offerings with established rate structures.

TCC has the ability to provide IaaS, PaaS, and SaaS services as defined service offerings. As an example the following rate structures apply for EC2 instances, AWS Storage, and AWS networking:

	vCPU	ECU	Memory (GiB)	Instance Storage (GB)	Windows Usage
General Purpose - Current Generation					
t2.nano	1	Variable	0.5	EBS Only	\$0.0088 per Hour
t2.micro	1	Variable	1	EBS Only	\$0.018 per Hour
t2.small	1	Variable	2	EBS Only	\$0.036 per Hour
t2.medium	2	Variable	4	EBS Only	\$0.072 per Hour
t2.large	2	Variable	8	EBS Only	\$0.134 per Hour
m4.large	2	6.5	8	EBS Only	\$0.246 per Hour

Region	Price per NAT gateway (\$/hour)	Price per GB data processed (\$)
US East (N.Virginia)	0.045	0.045
US West (Oregon)	0.045	0.045
US West (N. California)	0.048	0.048
EU (Ireland)	0.048	0.048
EU (Frankfurt)	0.052	0.052
Asia Pacific (Singapore)	0.059	0.059
Asia Pacific (Tokyo)	0.062	0.062
Asia Pacific (Sydney)	0.059	0.059

8.18 (E) Trial and Testing Periods (Pre- and Post-Purchase)

8.18.1

Describe your testing and training periods that you offer for your service offerings.

TCC's training discipline provides high quality training which is vital to ensuring that once implemented, all users are able to use TCC's systems to their full potential. TCC understands that most systems have a wide variety of users. **We provide our clients with training support that leads to sustainability and empowers our clients to self-manage as desired.**

TCC's training methodology consists of three Phases.

Phase 1: Planning

TCC works closely with project stakeholders to define all intended user groups and to establish agreement about training scope, objectives, resources, preferred methods and measureable success criteria.

Phase 2: Training Rollout

Based upon the agreed to schedule and methodology, the TCC team implements the approved training plan and schedule. We are able to provide training in a variety of formats including classroom training, train-the-trainer and online training.

Phase 3: Ongoing Support and Help

After delivery of the trainings has been completed, all training materials will be available to users. In addition, all final materials will be given to the appropriate project staff so that they may be updated as needed. TCC typically offers additional training once the system is deployed to production

8.18.2

Describe how you intend to provide a test and/or proof of concept environment for evaluation that verifies your ability to meet mandatory requirements.

Certain test sites may be accesses as a proof of concept to allow customers to verify our solutions capability of meeting functional requirements

8.18.3

Offeror must describe what training and support it provides at no additional cost.

TCC provides soft copy user manuals and online help at no additional cost.

8.19 (E) Integration and Customization

8.19.1

Describe how the Solutions you provide can be integrated to other complementary applications, and if you offer standard-based interface to enable additional integrations.

System integration involves integrating existing (often disparate) subsystems and then creating unique and new value for the client. We understand that integration is cost effective when a desired application is not available from a client's primary technology vendor. The TCC Team has worked with numerous IT vendor partners to implement and integrate innovative technology solutions in the human services arena.

The TCC Team utilizes a proven and systematic approach to the integration process. First the integration effort must be defined by each vendor participating in the process. Each element must be clearly defined so that the customer has full functionality from each vendor's product. Next, the business requirements must be clearly defined so that the functionality implemented meets the needs of the customer. The software versions to be integrated must also be clearly defined. Vendors typically support multiple versions of their solution and it is important that the team understand which version is currently integrated and what the vendor intends to implement. The next step is to clearly identify the hardware and software required from each vendor to support the solution. Next, the core setup is defined and customized to meet the business needs. Finally, data mapping is performed to design a solution that takes into account differences in data structures among all of the disparate systems.



The TCC project management process takes into account all of the variables involved with integrating systems from different vendors, and we will take the time to develop collaborative relationships with all vendors to deliver a decision making tool that meets the needs of the state.

8.19.2

Describe the ways to customize and personalize the Solutions you provide to meet the needs of specific Purchasing Entities.

As a software solutions provider, TCC understand that rarely off the shelf solutions meet at government requirements out of the box. Code bases and be customized to add new data fields, provide needed workflows, and produce necessary reports.

8.20 (E) Marketing Plan

Describe your how you intend to market your Solutions to NASPO ValuePoint and Participating Entities.

TCC intends on utilizing our website and case studies as marketing collateral that will be shared with NASPO entities. TCC intends to reach out to NASPO entities to initiate discovery sessions where we share success stories and strategies with NASPO entities as a means to marketing solutions.

8.21 (E) 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.

- Cloud Managed Services
 - Cloud Management Services
 - Cloud Hosting Services
 - Cloud Operations Services
 - Server Provisioning Services
 - Data Storage, Protection and Management Services
 - Storage Services
 - Data Backup Services
 - Enterprise Database Management Services
 - Disaster Recovery and Business Continuity Services
 - Disaster Recovery Services
 - Business Continuity Services
 - Enterprise Network Services
 - Network Operations and Advanced Monitoring Services
 - Managed Network Services

- Internet and Utility Services
 - Network Capacity Planning and Management Services
- Platform Management Services
 - Windows and Virtualization Services
 - UNIX and Linux Services
- End User Managed Services
 - Asset Management Services
 - Hardware Asset Lifecycle Management Services
 - Software Asset Lifecycle Management Services
 - Messaging and Collaboration Services
 - Messaging Services (ITIL)
 - Microsoft SharePoint Services
 - Messaging and Collaboration Services
 - Microsoft® Office 365™ Services
- Managed Security Services
 - Information Security Management Services
 - Security Operations and Engineering Services
 - Network Security Services
 - User Account Administration Services

8.22 (E) Supporting Infrastructure

8.22.1

Describe what infrastructure is required by the Purchasing Entity to support your Solutions or deployment models.

TCC working with AWS strives to ensure that a fully virtualized infrastructure is available offsite to promote Fault Tolerance and High Availability. While this means no servers in house or required there may be some instances in which certain applications are required to be in house or additional routers\network edge equipment are required for additional bandwidth.

8.22.2

If required, who will be responsible for installation of new infrastructure and who will incur those costs?

Depending on the geolocation of the client, TCC may be able to provide assistance either onsite or remotely. The client would incur all costs and ownership of said equipment.

8.23 (E) Alignment of Cloud Computing Reference Architecture

Clarify how their architecture compares to the NIST Cloud Computing Reference Architecture, in particular, to describe how they align with the three domains e.g. Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS).

Infrastructure as a Service, sometimes abbreviated as IaaS, contains the basic building blocks for cloud IT and typically provide access to networking features, computers (virtual or on dedicated hardware), and data storage space. Infrastructure as a Service provides you with the highest level of flexibility and management control over your IT resources and is most similar to existing IT resources that many IT departments and developers are familiar with today. AWS provides its infrastructure such as EC2, VCPs, Route53, S3, and Glacier to customers to provide flexible environment.

Platforms as a service remove the need for organizations to manage the underlying infrastructure (usually hardware and operating systems) and allow you to focus on the deployment and management of your applications. This helps you be more efficient as you don't need to worry about resource procurement, capacity planning, software maintenance, patching, or any of the other undifferentiated heavy lifting involved in running your application. AWS provides its platforms such as RDS, DMS, API gateway, and SNS to customers to provide a platform to develop resource procurement.

Software as a Service provides you with a completed product that is run and managed by the service provider. In most cases, people referring to Software as a Service are referring to end-user applications. With a SaaS offering you do not have to think about how the service is maintained or how the underlying infrastructure is managed; you only need to think about how you will use that particular piece software. A common example of a SaaS application is web-based email where you can send and receive email without having to manage feature additions to the email product or maintaining the servers and operating systems that the email program is running on. AWS provides its services using software such as WorkSpaces, WorkDocs, and WorkMail.

Appendix A

AWS Risk and Compliance with CCM



Amazon Web Services: Risk and Compliance

December 2015

(Consult <http://aws.amazon.com/compliance/aws-whitepapers/>
for the latest version of this paper)



This document is intended to provide information to assist AWS customers with integrating AWS into their existing control framework supporting their IT environment. This document includes a basic approach to evaluating AWS controls and provides information to assist customers with integrating control environments. This document also addresses AWS-specific information around general cloud computing compliance questions.

Table of Contents

Risk and Compliance Overview	3
<i>Shared Responsibility Environment</i>	<i>3</i>
<i>Strong Compliance Governance</i>	<i>4</i>
Evaluating and Integrating AWS Controls	4
<i>AWS IT Control Information</i>	<i>5</i>
<i>AWS Global Regions</i>	<i>5</i>
AWS Risk and Compliance Program	6
<i>Risk Management</i>	<i>6</i>
<i>Control Environment</i>	<i>6</i>
<i>Information Security</i>	<i>7</i>
AWS Certifications, Programs, Reports, and Third-Party Attestations	7
<i>CJIS</i>	<i>7</i>
<i>CSA</i>	<i>7</i>
<i>Cyber Essentials Plus</i>	<i>8</i>
<i>DoD SRG Levels 2 and 4</i>	<i>8</i>
<i>FedRAMP SM</i>	<i>8</i>
<i>FERPA</i>	<i>9</i>
<i>FIPS 140-2</i>	<i>9</i>
<i>FISMA and DIACAP</i>	<i>9</i>
<i>HIPAA</i>	<i>10</i>
<i>IRAP</i>	<i>10</i>
<i>ISO 9001</i>	<i>11</i>
<i>ISO 27001</i>	<i>12</i>
<i>ISO 27017</i>	<i>13</i>
<i>ISO 27018</i>	<i>14</i>
<i>ITAR</i>	<i>15</i>
<i>MPAA</i>	<i>15</i>
<i>MTCS Tier 3 Certification</i>	<i>16</i>
<i>NIST</i>	<i>16</i>

<i>PCI DSS Level 1</i>	16
<i>SOC 1/ISAE 3402</i>	17
<i>SOC 2</i>	19
<i>SOC 3</i>	19
<i>Key Compliance Questions and AWS</i>	19
AWS Contact	24
Appendix A: CSA Consensus Assessments Initiative Questionnaire v3.0.1	25
Appendix B: AWS alignment with the Australian Signals Directorate (ASD) Cloud Computing Security Considerations	62
Appendix C: Glossary of Terms	82

Risk and Compliance Overview

AWS and its customers share control over the IT environment, both parties have responsibility for managing the IT environment. AWS' part in this shared responsibility includes providing its services on a highly secure and controlled platform and providing a wide array of security features customers can use. The customers' responsibility includes configuring their IT environments in a secure and controlled manner for their purposes. While customers don't communicate their use and configurations to AWS, AWS does communicate its security and control environment relevant to customers. AWS does this by doing the following:

- Obtaining industry certifications and independent third-party attestations described in this document
- Publishing information about the AWS security and control practices in whitepapers and web site content
- Providing certificates, reports, and other documentation directly to AWS customers under NDA (as required)

For a more detailed description of AWS security please see:

[AWS Security Center](https://aws.amazon.com/security/): <https://aws.amazon.com/security/>

For a more detailed description of AWS Compliance please see

[AWS Compliance page](https://aws.amazon.com/compliance/): <https://aws.amazon.com/compliance/>

Additionally, The [AWS Overview of Security Processes Whitepaper](#) covers AWS' general security controls and service-specific security.

Shared Responsibility Environment

Moving IT infrastructure to AWS services creates a model of shared responsibility between the customer and AWS. This shared model can help relieve customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall. Customers should carefully consider the services they choose as their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations. It is possible for customers to enhance



security and/or meet their more stringent compliance requirements by leveraging technology such as host based firewalls, host based intrusion detection/prevention, encryption and key management. The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment of solutions that meet industry-specific certification requirements.

This customer/AWS shared responsibility model also extends to IT controls. Just as the responsibility to operate the IT environment is shared between AWS and its customers, so is the management, operation and verification of IT controls shared. AWS can help relieve customer burden of operating controls by managing those controls associated with the physical infrastructure deployed in the AWS environment that may previously have been managed by the customer. As every customer is deployed differently in AWS, customers can take advantage of shifting management of certain IT controls to AWS which results in a (new) distributed control environment. Customers can then use the AWS control and compliance documentation available to them (described in the [AWS Certifications and Third-party Attestations](#) section of this document) to perform their control evaluation and verification procedures as required.

The next section provides an approach on how AWS customers can evaluate and validate their distributed control environment effectively.

Strong Compliance Governance

As always, AWS customers are required to continue to maintain adequate governance over the entire IT control environment regardless of how IT is deployed. Leading practices include an understanding of required compliance objectives and requirements (from relevant sources), establishment of a control environment that meets those objectives and requirements, an understanding of the validation required based on the organization's risk tolerance, and verification of the operating effectiveness of their control environment. Deployment in the AWS cloud gives enterprises different options to apply various types of controls and various verification methods.

Strong customer compliance and governance might include the following basic approach:

1. Review information available from AWS together with other information to understand as much of the entire IT environment as possible, and then document all compliance requirements.
2. Design and implement control objectives to meet the enterprise compliance requirements.
3. Identify and document controls owned by outside parties.
4. Verify that all control objectives are met and all key controls are designed and operating effectively.

Approaching compliance governance in this manner will help companies gain a better understanding of their control environment and will help clearly delineate the verification activities to be performed.

Evaluating and Integrating AWS Controls

AWS provides a wide range of information regarding its IT control environment to customers through white papers, reports, certifications, and other third-party attestations. This documentation assists customers in understanding the controls in place relevant to the AWS services they use and how those controls have been validated. This information also assists customers in their efforts to account for and to validate that controls in their extended IT environment are operating effectively.

Traditionally, the design and operating effectiveness of control objectives and controls are validated by internal and/or external auditors via process walkthroughs and evidence evaluation. Direct observation/verification, by the customer or customer's external auditor, is generally performed to validate controls. In the case where service providers, such as AWS, are used, companies request and evaluate third-party attestations and



certifications in order to gain reasonable assurance of the design and operating effectiveness of control objective and controls. As a result, although customer's key controls may be managed by AWS, the control environment can still be a unified framework where all controls are accounted for and are verified as operating effectively. Third-party attestations and certifications of AWS can not only provide a higher level of validation of the control environment, but may relieve customers of the requirement to perform certain validation work themselves for their IT environment in the AWS cloud.

AWS IT Control Information

AWS provides IT control information to customers in the following two ways:

1. **Specific control definition.** AWS customers are able to identify key controls managed by AWS. Key controls are critical to the customer's control environment and require an external attestation of the operating effectiveness of these key controls in order to comply with compliance requirements—such as the annual financial audit. For this purpose, AWS publishes a wide range of specific IT controls in its Service Organization Controls 1 (SOC 1) Type II report. The SOC 1 report, formerly the Statement on Auditing Standards (SAS) No. 70, Service Organizations report, is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). The SOC 1 audit is an in-depth audit of both the design and operating effectiveness of AWS' defined control objectives and control activities (which include control objectives and control activities over the part of the infrastructure AWS manages). "Type II" refers to the fact that each of the controls described in the report are not only evaluated for adequacy of design, but are also tested for operating effectiveness by the external auditor. Because of the independence and competence of AWS' external auditor, controls identified in the report should provide customers with a high level of confidence in AWS' control environment. AWS' controls can be considered designed and operating effectively for many compliance purposes, including Sarbanes-Oxley (SOX) Section 404 financial statement audits. Leveraging SOC 1 Type II reports is also generally permitted by other external certifying bodies (e.g., ISO 27001 auditors may request a SOC 1 Type II report in order to complete their evaluations for customers).

Other specific control activities relate to AWS' Payment Card Industry (PCI) and Federal Information Security Management Act (FISMA) compliance. As discussed below, AWS is compliant with FISMA Moderate standards and with the PCI Data Security Standard. These PCI and FISMA standards are very prescriptive and require independent validation that AWS adheres to the published standard.

2. **General control standard compliance.** If an AWS customer requires a broad set of control objectives to be met, evaluation of AWS' industry certifications may be performed. With the AWS ISO 27001 certification, AWS complies with a broad, comprehensive security standard and follows best practices in maintaining a secure environment. With the PCI Data Security Standard (PCI DSS), AWS complies with a set of controls important to companies that handle credit card information. With AWS' compliance with the FISMA standards, AWS complies with a wide range of specific controls required by US government agencies. Compliance with these general standards provides customers with in-depth information on the comprehensive nature of the controls and security processes in place and can be considered when managing compliance.

AWS Global Regions

Data centers are built in clusters in various global regions. As of this writing, there are eleven regions: US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US) (Oregon), EU (Frankfurt), EU (Ireland), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), China (Beijing), and South America (Sao Paulo).



AWS Risk and Compliance Program

AWS provides information about its risk and compliance program to enable customers to incorporate AWS controls into their governance framework. This information can assist customers in documenting a complete control and governance framework with AWS included as an important part of that framework.

Risk Management

AWS management has developed a strategic business plan which includes risk identification and the implementation of controls to mitigate or manage risks. AWS management re-evaluates the strategic business plan at least biannually. This process requires management to identify risks within its areas of responsibility and to implement appropriate measures designed to address those risks.

In addition, the AWS control environment is subject to various internal and external risk assessments. AWS' Compliance and Security teams have established an information security framework and policies based on the Control Objectives for Information and related Technology (COBIT) framework and have effectively integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, the PCI DSS v3.1, and the National Institute of Standards and Technology (NIST) Publication 800-53 Rev 3 (Recommended Security Controls for Federal Information Systems). AWS maintains the security policy, provides security training to employees, and performs application security reviews. These reviews assess the confidentiality, integrity, and availability of data, as well as conformance to the information security policy.

AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. In addition, external vulnerability threat assessments are performed regularly by independent security firms. Findings and recommendations resulting from these assessments are categorized and delivered to AWS leadership. These scans are done in a manner for the health and viability of the underlying AWS infrastructure and are not meant to replace the customer's own vulnerability scans required to meet their specific compliance requirements. Customers can request permission to conduct scans of their cloud infrastructure as long as they are limited to the customer's instances and do not violate the AWS Acceptable Use Policy. Advance approval for these types of scans can be initiated by submitting a request via the [AWS Vulnerability / Penetration Testing Request Form](#).

Control Environment

AWS manages a comprehensive control environment that includes policies, processes and control activities that leverage various aspects of Amazon's overall control environment. This control environment is in place for the secure delivery of AWS' service offerings. The collective control environment encompasses the people, processes, and technology necessary to establish and maintain an environment that supports the operating effectiveness of AWS' control framework. AWS has integrated applicable cloud-specific controls identified by leading cloud computing industry bodies into the AWS control framework. AWS continues to monitor these industry groups for ideas on which leading practices can be implemented to better assist customers with managing their control environment.

The control environment at Amazon begins at the highest level of the Company. Executive and senior leadership play important roles in establishing the Company's tone and core values. Every employee is provided with the Company's Code of Business Conduct and Ethics and completes periodic training. Compliance audits are performed so that employees understand and follow the established policies.



The AWS organizational structure provides a framework for planning, executing and controlling business operations. The organizational structure assigns roles and responsibilities to provide for adequate staffing, efficiency of operations, and the segregation of duties. Management has also established authority and appropriate lines of reporting for key personnel. Included as part of the Company's hiring verification processes are education, previous employment, and, in some cases, background checks as permitted by law and regulation for employees commensurate with the employee's position and level of access to AWS facilities. The Company follows a structured on-boarding process to familiarize new employees with Amazon tools, processes, systems, policies and procedures.

Information Security

AWS has implemented a formal information security program designed to protect the confidentiality, integrity, and availability of customers' systems and data. AWS publishes a security whitepaper that is available on the public website that addresses how AWS can help customers secure their data.

AWS Certifications, Programs, Reports, and Third-Party Attestations

AWS engages with external certifying bodies and independent auditors to provide customers with considerable information regarding the policies, processes, and controls established and operated by AWS.

CJIS

AWS complies with the FBI's Criminal Justice Information Services (CJIS) standard. We sign CJIS security agreements with our customers, including allowing or performing any required employee background checks according to the [CJIS Security Policy](#).

Law enforcement customers (and partners who manage CJI) are taking advantage of AWS services to improve the security and protection of CJI data, using the advanced security services and features of AWS, such as activity logging ([AWS CloudTrail](#)), encryption of data in motion and at rest (S3's Server-Side Encryption with the option to bring your own key), comprehensive key management and protection ([AWS Key Management Service](#) and [CloudHSM](#)), and integrated permission management (IAM federated identity management, multi-factor authentication).

AWS has created a Criminal Justice Information Services (CJIS) [Workbook](#) in a security plan template format aligned to the CJIS Policy Areas. Additionally, a CJIS Whitepaper has been developed to help guide customers in their journey to cloud adoption.

Visit the CJIS Hub Page: <https://aws.amazon.com/compliance/cjis/>

CSA

In 2011, the Cloud Security Alliance (CSA) launched [STAR](#), an initiative to encourage transparency of security practices within cloud providers. The [CSA Security, Trust & Assurance Registry](#) (STAR) is a free, publicly accessible registry that documents the security controls provided by various cloud computing offerings, thereby helping users assess the security of cloud providers they currently use or are considering contracting with. [AWS is a CSA STAR registrant](#) and has completed the Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire (CAIQ). This CAIQ published by the CSA provides a way to reference and



document what security controls exist in AWS' Infrastructure as a Service offerings. The CAIQ provides 298 questions a cloud consumer and cloud auditor may wish to ask of a cloud provider.

See: [Appendix A: CSA Consensus Assessments Initiative Questionnaire v3.0.1](#)

Cyber Essentials Plus

[Cyber Essentials Plus](#) is a UK Government-backed, industry-supported certification scheme introduced in the UK to help organizations demonstrate operational security against common cyber-attacks.

It demonstrates the baseline controls AWS implements to mitigate the risk from common Internet-based threats, within the context of the UK Government's "[10 Steps to Cyber Security](#)". It is backed by industry, including the Federation of Small Businesses, the Confederation of British Industry and a number of insurance organizations that offer incentives for businesses holding this certification.

Cyber Essentials sets out the necessary technical controls; the related assurance framework shows how the independent assurance process works for Cyber Essentials Plus certification through an annual external assessment conducted by an accredited assessor. Due to the regional nature of the certification, the certification scope is limited to EU (Ireland) region.

DoD SRG Levels 2 and 4

[The Department of Defense \(DoD\) Cloud Security Model \(SRG\)](#) provides a formalized assessment and authorization process for cloud service providers (CSPs) to gain a DoD Provisional Authorization, which can subsequently be leveraged by DoD customers. A Provisional Authorization under the SRG provides a reusable certification that attests to our compliance with DoD standards, reducing the time necessary for a DoD mission owner to assess and authorize one of their systems for operation on AWS. AWS currently holds provisional authorizations at Levels 2 and 4 of the SRG.

Additional information of the security control baselines defined for [Levels 2, 4, 5, and 6 can be found at: \[http://iase.disa.mil/cloud_security/Pages/index.aspx\]\(http://iase.disa.mil/cloud_security/Pages/index.aspx\)](#).

Visit the DoD Hub Page: <https://aws.amazon.com/compliance/dod/>

FedRAMP SM

AWS is a Federal Risk and Authorization Management Program (FedRAMPSM) Compliant Cloud Service Provider. AWS has completed the testing performed by a FedRAMPSM accredited Third-Party Assessment Organization (3PAO) and has been granted two Agency Authority to Operate (ATOs) by the US Department of Health and Human Services (HHS) after demonstrating compliance with FedRAMPSM requirements at the Moderate impact level. All U.S. government agencies can leverage the AWS Agency ATO packages stored in the FedRAMPSM repository to evaluate AWS for their applications and workloads, provide authorizations to use AWS, and transition workloads into the AWS environment. The two FedRAMPSM Agency ATOs encompass all U.S. regions (the AWS GovCloud (US) region and the AWS US East/West regions).

The following services are in the accreditation boundary for the regions stated above:

- [Amazon Redshift](#). Amazon Redshift is a fast, fully managed, petabyte-scale data warehouse service that makes it simple and cost-effective to efficiently analyze all your data using your existing business intelligence tools.
- [Amazon Elastic Compute Cloud \(Amazon EC2\)](#). Amazon EC2 provides resizable compute capacity in the cloud. It is designed to make web-scale computing easier for developers.
- [Amazon Simple Storage Service \(S3\)](#). Amazon S3 provides a simple web services interface that can be used to store and retrieve any amount of data, at any time, from anywhere on the web.
- [Amazon Virtual Private Cloud \(VPC\)](#). Amazon VPC provides the ability for you to provision a logically isolated section of AWS where you can launch AWS resources in a virtual network that you define.
- [Amazon Elastic Block Store \(EBS\)](#). Amazon EBS provides highly available, highly reliable, predictable storage volumes that can be attached to a running Amazon EC2 instance and exposed as a device within the instance.
- [AWS Identity and Access Management \(IAM\)](#). IAM enables you to securely control access to AWS services and resources for your users. Using IAM, you can create and manage AWS users and groups and use permissions to allow and deny their access to AWS resources.

For more information on AWS FedRAMPsm compliance please see the [AWS FedRAMPsm FAQs](#) at: <https://aws.amazon.com/compliance/fedramp/>

FERPA

[The Family Educational Rights and Privacy Act](#) (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18, or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

AWS enables covered entities and their business associates subject to FERPA to leverage the secure AWS environment to process, maintain, and store protected education information.

AWS also offers a [FERPA-focused whitepaper](#) for customers interested in learning more about how they can leverage AWS for the processing and storage of educational data.

The "[FERPA Compliance on AWS Whitepaper](#)" outlines how companies can use AWS to process systems that facilitate FERPA compliance:
https://do.awsstatic.com/whitepapers/compliance/AWS_FERPA_Whitepaper.pdf

FIPS 140-2

[The Federal Information Processing Standard \(FIPS\) Publication 140-2](#) is a US government security standard that specifies the security requirements for cryptographic modules protecting sensitive information. To support customers with FIPS 140-2 requirements, SSL terminations in [AWS GovCloud \(US\)](#) operate using FIPS 140-2 validated hardware. AWS works with AWS GovCloud (US) customers to provide the information they need to help manage compliance when using the [AWS GovCloud \(US\) environment](#).

FISMA and DIACAP

AWS enables US government agencies to achieve and sustain compliance with the Federal Information Security Management Act ([FISMA](#)). The AWS infrastructure has been evaluated by independent assessors for a variety of government systems as part of their system owners' approval process. Numerous Federal Civilian and Department of Defense (DoD) organizations have successfully achieved security authorizations for systems hosted on AWS in accordance with the Risk Management Framework (RMF) process defined in NIST 800-37 and DoD Information Assurance Certification and Accreditation Process ([DIACAP](#)).

HIPAA

AWS enables covered entities and their business associates subject to the U.S. Health Insurance Portability and Accountability Act (HIPAA) to leverage the secure AWS environment to process, maintain, and store protected health information and AWS will be signing business associate agreements with such customers. AWS also offers a HIPAA-focused whitepaper for customers interested in learning more about how they can leverage AWS for the processing and storage of health information. The [Architecting for HIPAA Security and Compliance on Amazon Web Services](#) whitepaper outlines how companies can use AWS to process systems that facilitate HIPAA and Health Information Technology for Economic and Clinical Health (HITECH) compliance.

Customers may use any AWS service in an account designated as a HIPAA account, but they should only process, store and transmit PHI in the HIPAA-eligible services defined in the BAA. There are nine HIPAA-eligible services today, including:

- [Amazon DynamoDB](#)
- [Amazon Elastic Block Store \(EBS\)](#)
- [Amazon Elastic Cloud Compute \(EC2\)](#)
- [Elastic Load Balancing \(ELB\)](#)
- [Amazon Elastic MapReduce \(EMR\)](#)
- [Amazon Glacier](#)
- [Amazon Redshift](#)
- [Amazon Relational Database Service \(Amazon RDS\)](#) using only MySQL and Oracle engines
- [Amazon Simple Storage Service \(S3\)](#)

AWS follows a standards-based risk management program to ensure that the HIPAA-eligible services specifically support the security, control, and administrative processes required under HIPAA. Using these services to store and process PHI allows our customers and AWS to address the HIPAA requirements applicable to our utility-based operating model. AWS prioritizes and adds new eligible services based on customer demand.

For additional information please see our HIPAA Compliance FAQs:
<https://aws.amazon.com/compliance/hipaa-compliance/>

Architecting for HIPAA Security and Compliance on Amazon Web Services:
https://do.awsstatic.com/whitepapers/compliance/AWS_HIPAA_Compliance_Whitepaper.pdf

IRAP

The Information Security Registered Assessors Program (IRAP) enables Australian government customers to validate that appropriate controls are in place and determine the appropriate responsibility model for addressing the needs of the Australian Signals Directorate (ASD) Information Security Manual (ISM).



Amazon Web Services [has completed an independent assessment](#) that has determined all applicable ISM controls are in place relating to the processing, storage and transmission of Unclassified (DLM) for the AWS Sydney Region.

IRAP Compliance FAQs:

<https://aws.amazon.com/compliance/irap/>

For more information see: [Appendix B: AWS alignment with the Australian Signals Directorate \(ASD\) Cloud Computing Security Considerations](#)

ISO 9001

AWS has achieved ISO 9001 certification, AWS' ISO 9001 certification directly supports customers who develop, migrate and operate their quality-controlled IT systems in the AWS cloud. Customers can leverage AWS' compliance reports as evidence for their own ISO 9001 programs and industry-specific quality programs, such as GxP in life sciences, ISO 13485 in medical devices, AS9100 in aerospace, and ISO/TS 16949 in automotive. AWS customers who don't have quality system requirements will still benefit from the additional assurance and transparency that an ISO 9001 certification provides.

The ISO 9001 certification covers the quality management system over a specified scope of AWS services and Regions of operations (below) and services including:

- [AWS CloudFormation](#)
- [AWS Cloud Hardware Security Model \(HSM\)](#)
- [Amazon CloudFront](#)
- [AWS CloudTrail](#)
- [AWS Direct Connect](#)
- [AWS Directory Service](#)
- [Amazon DynamoDB](#)
- [Amazon EC2 VM Import/Export](#)
- [AWS Elastic Beanstalk](#)
- [Amazon Elastic Block Store \(EBS\)](#)
- [Amazon Elastic Cloud Compute \(EC2\)](#)
- [Amazon EC2 Container Service \(ECS\)](#)
- [Amazon Elastic File System \(EFS\)](#)
- [Elastic Load Balancing \(ELB\)](#)
- [Amazon Elastic MapReduce \(EMR\)](#)
- [Amazon ElastiCache](#)
- [Amazon Glacier](#)
- [AWS Identity and Access Management \(IAM\)](#)
- [AWS Key Management Service \(KMS\)](#)
- [Amazon Redshift](#)
- [Amazon Relational Database Service \(RDS\)](#)
- [AWS Route 53](#)
- [Amazon SimpleDB](#)
- [Amazon Simple Email Service \(SES\)](#)
- [Amazon Simple Queue Service \(SQS\)](#)
- [Amazon Simple Storage Service \(S3\)](#)
- [AWS Storage Gateway](#)
- [Amazon Simple Workflow Service \(SWF\)](#)
- [Amazon Virtual Private Cloud \(VPC\)](#)
- [AWS WAF - Web Application Firewall](#)

- [Amazon WorkDocs](#)
- [Amazon WorkMail](#)
- [Amazon WorkSpaces](#)
- The underlying physical infrastructure and the AWS Management Environment

AWS' ISO 9001 accreditation covers AWS Regions including US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US), South America (Sao Paulo), EU (Ireland), EU (Frankfurt) and Asia Pacific (Singapore), Asia Pacific (Sydney), and Asia Pacific (Tokyo).

ISO 9001:2008 is a global standard for managing the quality of products and services. The 9001 standard outlines a quality management system based on eight principles defined by the International Organization for Standardization (ISO) Technical Committee for Quality Management and Quality Assurance. They include:

- Customer focus
- Leadership
- Involvement of people
- Process approach
- System approach to management
- Continual Improvement
- Factual approach to decision-making
- Mutually beneficial supplier relationships

The AWS ISO 9001 certification can be downloaded at:

https://do.awsstatic.com/certifications/iso_9001_certification.pdf

AWS provides additional information and frequently asked questions about its ISO 9001 certification at:

<https://aws.amazon.com/compliance/iso-9001-faqs/>

ISO 27001

AWS has achieved ISO 27001 certification of our Information Security Management System (ISMS) covering AWS infrastructure, data centers, and services including:

- [AWS CloudFormation](#)
- [Amazon CloudFront](#)
- [AWS Cloudtrail](#)
- [AWS Directory Service](#)
- [Amazon DynamoDB](#)
- [AWS Elastic Beanstalk](#)
- [Amazon Elastic Block Store \(EBS\)](#)
- [Amazon Elastic Cloud Compute \(EC2\)](#)
- [Amazon EC2 Container Service \(ECS\)](#)
- [AWS Direct Connect](#)
- [Amazon EC2 VM Import/Export](#)
- [AWS Cloud Hardware Security Model \(HSM\)](#)
- [Elastic Load Balancing \(ELB\)](#)
- [Amazon Elastic File System \(EFS\)](#)
- [Amazon Elastic MapReduce \(EMR\)](#)
- [Amazon ElastiCache](#)
- [Amazon Glacier](#)
- [AWS Identity and Access Management \(IAM\)](#)



- [AWS Key Management Service \(KMS\)](#)
- [Amazon Redshift](#)
- [Amazon Relational Database Service \(RDS\)](#)
- [AWS Route 53](#)
- [Amazon SimpleDB](#)
- [Amazon Simple Email Service \(SES\)](#)
- [Amazon Simple Queue Service \(SQS\)](#)
- [Amazon Simple Storage Service \(S3\)](#)
- [Amazon Simple Workflow Service \(SWF\)](#)
- [AWS Storage Gateway](#)
- [Amazon Virtual Private Cloud \(VPC\)](#)
- [AWS WAF - Web Application Firewall](#)
- [Amazon WorkDocs](#)
- [Amazon WorkMail](#)
- [Amazon WorkSpaces](#)
- The underlying physical infrastructure (including GovCloud) and the AWS Management Environment

ISO 27001/27002 is a widely-adopted global security standard that sets out requirements and best practices for a systematic approach to managing company and customer information that's based on periodic risk assessments appropriate to ever-changing threat scenarios. In order to achieve the certification, a company must show it has a systematic and ongoing approach to managing information security risks that affect the confidentiality, integrity, and availability of company and customer information. This certification reinforces Amazon's commitment to providing significant information regarding our security controls and practices.

AWS' ISO 27001 accreditation covers AWS Regions including US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US), South America (Sao Paulo), EU (Ireland), EU (Frankfurt), Asia Pacific (Singapore), Asia Pacific (Sydney), and Asia Pacific (Tokyo).

The AWS ISO 27001 certification can be downloaded at:

https://do.awsstatic.com/certifications/iso_27001_global_certification.pdf

AWS provides additional information and frequently asked questions about its ISO 27001 certification at:

<https://aws.amazon.com/compliance/iso-27001-faqs/>

ISO 27017

ISO 27017 is the newest code of practice released by the International Organization for Standardization (ISO). It provides implementation guidance on information security controls that specifically relate to cloud services.

AWS has achieved ISO 27017 certification of our Information Security Management System (ISMS) covering AWS infrastructure, data centers, and services including:

- [Amazon CloudFront](#)
- [Amazon DynamoDB](#)
- [Amazon EC2 Container Service \(ECS\)](#)
- [Amazon Elastic Block Store \(EBS\)](#)
- [Amazon Elastic Compute Cloud \(EC2\)](#)
- [Amazon Elastic File System \(EFS\)](#)
- [Amazon Elastic MapReduce \(EMR\)](#)
- [Amazon ElastiCache](#)
- [Amazon Glacier](#)



- [Amazon Redshift](#)
- [Amazon Relational Database Service \(RDS\)](#)
- [Amazon Route 53](#)
- [Amazon Simple Email Service \(SES\)](#)
- [Amazon Simple Queue Service \(SQS\)](#)
- [Amazon Simple Storage Service \(S3\)](#)
- [Amazon Simple Workflow Service \(SWF\)](#)
- [Amazon SimpleDB](#)
- [Amazon Virtual Private Cloud \(VPC\)](#)
- [Amazon WorkDocs](#)
- [Amazon WorkMail](#)
- [Amazon WorkSpaces](#)
- [AWS CloudFormation](#)
- [AWS CloudHSM](#)
- [AWS CloudTrail](#)
- [AWS Direct Connect](#)
- [AWS Directory Service](#)
- [AWS Elastic Beanstalk](#)
- [AWS Identity and Access Management \(IAM\)](#)
- [AWS Key Management Service \(KMS\)](#)
- [AWS Storage Gateway](#)
- [AWS WAF \(Web Application Firewall\)](#)
- [Elastic Load Balancing](#)
- [VM Import/Export](#)

The AWS ISO 27017 certification can be downloaded at:

https://do.awsstatic.com/certifications/iso_27017_certification.pdf

AWS provides additional information and frequently asked questions about its ISO 27017 certification at:

<https://aws.amazon.com/compliance/iso-27017-faqs/>

ISO 27018

ISO 27018 is the first International code of practice that focuses on protection of personal data in the cloud. It is based on ISO information security standard 27002 and provides implementation guidance on ISO 27002 controls applicable to public cloud Personally Identifiable Information (PII). It also provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements not addressed by the existing ISO 27002 control set.

AWS has achieved ISO 27018 certification of our Information Security Management System (ISMS) covering AWS infrastructure, data centers, and services including:

- [Amazon CloudFront](#)
- [Amazon DynamoDB](#)
- [Amazon EC2 Container Service \(ECS\)](#)
- [Amazon Elastic Block Store \(EBS\)](#)
- [Amazon Elastic Compute Cloud \(EC2\)](#)
- [Amazon Elastic File System \(EFS\)](#)
- [Amazon Elastic MapReduce \(EMR\)](#)
- [Amazon ElastiCache](#)
- [Amazon Glacier](#)



- [Amazon Redshift](#)
- [Amazon Relational Database Service \(RDS\)](#)
- [Amazon Route 53](#)
- [Amazon Simple Email Service \(SES\)](#)
- [Amazon Simple Queue Service \(SQS\)](#)
- [Amazon Simple Storage Service \(S3\)](#)
- [Amazon Simple Workflow Service \(SWF\)](#)
- [Amazon SimpleDB](#)
- [Amazon Virtual Private Cloud \(VPC\)](#)
- [Amazon WorkDocs](#)
- [Amazon WorkMail](#)
- [Amazon WorkSpaces](#)
- [AWS CloudFormation](#)
- [AWS CloudHSM](#)
- [AWS CloudTrail](#)
- [AWS Direct Connect](#)
- [AWS Directory Service](#)
- [AWS Elastic Beanstalk](#)
- [AWS Identity and Access Management \(IAM\)](#)
- [AWS Key Management Service \(KMS\)](#)
- [AWS Storage Gateway](#)
- [AWS WAF \(Web Application Firewall\)](#)
- [Elastic Load Balancing](#)
- [VM Import/Export](#)

The AWS ISO 27018 certification can be downloaded at:

https://do.awsstatic.com/certifications/iso_27018_certification.pdf

AWS provides additional information and frequently asked questions about its ISO 27018 certification at:

<https://aws.amazon.com/compliance/iso-27018-faqs/>

ITAR

The **AWS GovCloud (US)** region supports US International Traffic in Arms Regulations (**ITAR**) compliance. As a part of managing a comprehensive ITAR compliance program, companies subject to ITAR export regulations must control unintended exports by restricting access to protected data to US Persons and restricting physical location of that data to the US. AWS GovCloud (US) provides an environment physically located in the US and where access by AWS Personnel is limited to US Persons, thereby allowing qualified companies to transmit, process, and store protected articles and data subject to ITAR restrictions. The AWS GovCloud (US) environment has been audited by an independent third-party to validate the proper controls are in place to support customer export compliance programs for this requirement.

MPAA

The Motion Picture Association of America (MPAA) has established a set of best practices for securely storing, processing and delivering protected media and content (<http://www.fightfilmtheft.org/facility-security-program.html>). Media companies use these best practices as a way to assess risk and security of their content and infrastructure. AWS has demonstrated alignment with the MPAA best practices and the AWS infrastructure is compliant with all applicable MPAA infrastructure controls. While the MPAA does not offer a “certification,” media industry customers can use the AWS MPAA documentation to augment their risk assessment and evaluation of MPAA-type content on AWS.

See the [AWS Compliance MPAA hub page](https://aws.amazon.com/compliance/mpaa/) for additional details:
<https://aws.amazon.com/compliance/mpaa/>

MTCS Tier 3 Certification

The [Multi-Tier Cloud Security \(MTCS\)](#) is an operational Singapore security management Standard (SPRING SS 584:2013), based on ISO 27001/02 Information Security Management System (ISMS) standards. The certification assessment requires us to:

- Systematically evaluate our information security risks, taking into account the impact of company threats and vulnerabilities
- Design and implement a comprehensive suite of information security controls and other forms of risk management to address company and architecture security risks
- Adopt an overarching management process to ensure that the information security controls meet the our information security needs on an ongoing basis

View the MTCS Hub Page at:

<https://aws.amazon.com/compliance/aws-multitiered-cloud-security-standard-certification/>

NIST

In June 2015 The National Institute of Standards and Technology (NIST) released guidelines [800-171](#), "Final Guidelines for Protecting Sensitive Government Information Held by Contractors". This guidance is applicable to the protection of Controlled Unclassified Information (CUI) on nonfederal systems.

AWS is already compliant with these guidelines, and customers can effectively comply with NIST 800-171 immediately. NIST 800-171 outlines a subset of the NIST 800-53 requirements, a guideline under which AWS has already been audited under the FedRAMP program. The FedRAMP Moderate security control baseline is more rigorous than the recommended requirements established in Chapter 3 of 800-171, and includes a significant number of security controls above and beyond those required of FISMA Moderate systems that protect CUI data. A detailed mapping is available in the [NIST Special Publication 800-171](#), starting on page D2 (which is page 37 in the PDF).

PCI DSS Level 1

AWS is Level 1 compliant under the Payment Card Industry (PCI) Data Security Standard (DSS). Customers can run applications on our PCI-compliant technology infrastructure for storing, processing, and transmitting credit card information in the cloud. In February 2013, the PCI Security Standards Council released PCI DSS Cloud Computing Guidelines. These guidelines provide customers who are managing a cardholder data environment with considerations for maintaining PCI DSS controls in the cloud. AWS has incorporated the PCI DSS Cloud Computing Guidelines into the AWS PCI Compliance Package for customers. The AWS PCI Compliance Package includes the AWS PCI Attestation of Compliance (AoC), which shows that AWS has been successfully validated against standards applicable to a Level 1 service provider under PCI DSS Version 3.1, and the AWS PCI Responsibility Summary, which explains how compliance responsibilities are shared between AWS and our customers in the cloud.

The following services are in scope for PCI DSS Level 1:



- [Auto Scaling](#)
- [AWS CloudFormation](#)
- [Amazon CloudFront](#)
- [AWS CloudHSM](#)
- [AWS CloudTrail](#)
- [AWS Direct Connect](#)
- [Amazon DynamoDB](#)
- [AWS Elastic Beanstalk](#)
- [Amazon Elastic Block Store \(EBS\)](#)
- [Amazon Elastic Compute Cloud \(EC2\)](#)
- [Elastic Load Balancing \(ELB\)](#)
- [Amazon Elastic MapReduce \(EMR\)](#)
- [Amazon Glacier](#)
- [AWS Key Management Service \(KMS\)](#)
- [AWS Identity and Access Management \(IAM\)](#)
- [Amazon Redshift](#)
- [Amazon Relational Database Service \(RDS\)](#)
- [Amazon Route 53](#)
- [Amazon SimpleDB](#)
- [Amazon Simple Storage Service \(S3\)](#)
- [Amazon Simple Queue Service \(SQS\)](#)
- [Amazon Simple Workflow Service SWF](#)
- [Amazon Virtual Private Cloud \(VPC\)](#)
- The underlying physical infrastructure (including GovCloud) and the AWS Management Environment

The latest scope of services and regions for the AWS PCI DSS Level 1 certification can be found at:

<https://aws.amazon.com/compliance/pci-dss-level-1-faqs/>

SOC 1/ISAE 3402

Amazon Web Services publishes a Service Organization Controls 1 (SOC 1), Type II report. The audit for this report is conducted in accordance with American Institute of Certified Public Accountants (AICPA): AT 801 (formerly SSAE 16) and the International Standards for Assurance Engagements No. 3402 (ISAE 3402). This dual-standard report is intended to meet a broad range of financial auditing requirements for U.S. and international auditing bodies. The SOC 1 report audit attests that AWS' control objectives are appropriately designed and that the individual controls defined to safeguard customer data are operating effectively. This report is the replacement of the Statement on Auditing Standards No. 70 (SAS 70) Type II Audit report.

The AWS SOC 1 control objectives are provided here. The report itself identifies the control activities that support each of these objectives and the independent auditor's results of their testing procedures of each control.

Objective Area	Objective Description
Security Organization	Controls provide reasonable assurance that information security policies have been implemented and communicated throughout the organization.
Employee User Access	Controls provide reasonable assurance that procedures have been established so that Amazon employee user accounts are added, modified and deleted in a timely manner and reviewed on a periodic basis.

Logical Security	Controls provide reasonable assurance that policies and mechanisms are in place to appropriately restrict unauthorized internal and external access to data and customer data is appropriately segregated from other customers.
Secure Data Handling	Controls provide reasonable assurance that data handling between the customer's point of initiation to an AWS storage location is secured and mapped accurately.
Physical Security and Environmental Protection	Controls provide reasonable assurance that physical access to data centers is restricted to authorized personnel and that mechanisms are in place to minimize the effect of a malfunction or physical disaster to data center facilities.
Change Management	Controls provide reasonable assurance that changes (including emergency / non-routine and configuration) to existing IT resources are logged, authorized, tested, approved and documented.
Data Integrity, Availability and Redundancy	Controls provide reasonable assurance that data integrity is maintained through all phases including transmission, storage and processing.
Incident Handling	Controls provide reasonable assurance that system incidents are recorded, analyzed, and resolved.

The SOC 1 reports are designed to focus on controls at a service organization that are likely to be relevant to an audit of a user entity's financial statements. As AWS' customer base is broad, and the use of AWS services is equally as broad, the applicability of controls to customer financial statements varies by customer. Therefore, the AWS SOC 1 report is designed to cover specific key controls likely to be required during a financial audit, as well as covering a broad range of IT general controls to accommodate a wide range of usage and audit scenarios. This allows customers to leverage the AWS infrastructure to store and process critical data, including that which is integral to the financial reporting process. AWS periodically reassesses the selection of these controls to consider customer feedback and usage of this important audit report.

AWS' commitment to the SOC 1 report is ongoing, and AWS will continue the process of periodic audits. The SOC 1 report scope covers:

- [AWS CloudFormation](#)
- [AWS CloudHSM](#)
- [AWS CloudTrail](#)
- [AWS Direct Connect](#)
- [Amazon DynamoDB](#)
- [Amazon EC2 VM Import/Export](#)
- [Amazon Elastic Beanstalk](#)
- [Amazon Elastic Block Store \(EBS\)](#)
- [Amazon ElastiCache](#)
- [Amazon Elastic Compute Cloud \(EC2\)](#)
- [Amazon Elastic Load Balancing \(ELB\)](#)
- [Amazon Elastic MapReduce \(EMR\)](#)
- [Amazon Glacier](#)
- [AWS Identity and Access Management \(IAM\)](#)
- [AWS Key Management Service \(KMS\)](#)
- [Amazon Redshift](#)
- [Amazon Relational Database Service \(RDS\)](#)
- [Amazon Route 53](#)
- [Amazon SimpleDB](#)
- [Amazon Simple Email Service \(SES\)](#)

- [Amazon Simple Storage Service \(S3\)](#)
- [Amazon Simple Workflow \(SWF\)](#)
- [Amazon Simple Queue Service \(SQS\)](#)
- [AWS Storage Gateway](#)
- [Amazon Virtual Private Cloud \(VPC\)](#)
- [Amazon Workspaces](#)

SOC 2

In addition to the SOC 1 report, AWS publishes a Service Organization Controls 2 (SOC 2), Type II report. Similar to the SOC 1 in the evaluation of controls, the SOC 2 report is an attestation report that expands the evaluation of controls to the criteria set forth by the American Institute of Certified Public Accountants (AICPA) Trust Services Principles. These principles define leading practice controls relevant to security, availability, processing integrity, confidentiality, and privacy applicable to service organizations such as AWS. The AWS SOC 2 is an evaluation of the design and operating effectiveness of controls that meet the criteria for the security and availability principles set forth in the AICPA's Trust Services Principles criteria. This report provides additional transparency into AWS security and availability based on a pre-defined industry standard of leading practices and further demonstrates AWS' commitment to protecting customer data. The SOC 2 report scope covers the same services covered in the SOC 1 report. See the SOC 1 description above for the in-scope services.

SOC 3

AWS publishes a Service Organization Controls 3 (SOC 3) report. The SOC 3 report is a publically-available summary of the AWS SOC 2 report. The report includes the external auditor's opinion of the operation of controls (based on the [AICPA's Security Trust Principles](#) included in the SOC 2 report), the assertion from AWS management regarding the effectiveness of controls, and an overview of AWS Infrastructure and Services. The AWS SOC 3 report includes all AWS data centers worldwide that support in-scope services. This is a great resource for customers to validate that AWS has obtained external auditor assurance without going through the process to request a SOC 2 report. The SOC 3 report scope covers the same services covered in the SOC 1 report. See the SOC 1 description above for the in-scope services. [View the AWS SOC 3 report here.](#)

Key Compliance Questions and AWS

This section addresses generic cloud computing compliance questions specifically for AWS. These common compliance questions listed may be of interest when evaluating and operating in a cloud computing environment and may assist in AWS customers' control management efforts.

Ref	Cloud Computing Question	AWS Information
1	Control ownership. Who owns which controls for cloud-deployed infrastructure?	For the portion deployed into AWS, AWS controls the physical components of that technology. The customer owns and controls everything else, including control over connection points and transmissions. To help customers better understand what controls we have in place and how effectively they are operating, we publish a SOC 1 Type II report with controls defined around EC2, S3 and VPC, as well as detailed physical security and environmental controls. These controls are defined at a high level of specificity that should meet most customer needs. AWS customers that have signed a non-disclosure agreement with AWS may request a copy of the SOC 1 Type II report.
2	Auditing IT. How can auditing of the cloud provider be accomplished?	Auditing for most layers and controls above the physical controls remains the responsibility of the customer. The definition of AWS-defined logical and physical controls is documented in the SOC 1 Type II report, and the report is available for review by audit and compliance teams. AWS ISO 27001 and other certifications are also available for auditors to review.
3	Sarbanes-Oxley compliance. How is SOX compliance achieved if in-scope systems are deployed in the cloud provider environment?	If a customer processes financial information in the AWS cloud, the customer's auditors may determine that some AWS systems come into scope for Sarbanes-Oxley (SOX) requirements. The customer's auditors must make their own determination regarding SOX applicability. Because most of the logical access controls are managed by customer, the customer is best positioned to determine if its control activities meet relevant standards. If the SOX auditors request specifics regarding AWS' physical controls, they can reference the AWS SOC 1 Type II report which details the controls that AWS provides.
4	HIPAA compliance. Is it possible to meet HIPAA compliance requirements while deployed in the cloud provider environment?	HIPAA requirements apply to and are controlled by the AWS customer. The AWS platform allows for the deployment of solutions that meet industry-specific certification requirements such as HIPAA. Customers can use AWS services to maintain a security level that is equivalent or greater than those required to protect electronic health records. Customers have built healthcare applications compliant with HIPAA's Security and Privacy Rules on AWS. AWS provides additional information about HIPAA compliance on its web site, including a whitepaper on this topic .
5	GLBA compliance. Is it possible to meet GLBA certification requirements while deployed in the cloud provider environment?	Most GLBA requirements are controlled by the AWS customer. AWS provides means for customers to protect data, manage permissions, and build GLBA-compliant applications on AWS infrastructure. If the customer requires specific assurance that physical security controls are operating effectively, they can reference the AWS SOC 1 Type II report as relevant.
6	Federal regulation compliance. Is it possible for a US Government agency to be compliant with security and privacy regulations while deployed in the cloud provider environment?	US Federal agencies can be compliant under a number of compliance standards, including the Federal Information Security Management Act (FISMA) of 2002, Federal Risk and Authorization Management Program (FedRAMP sm), the Federal Information Processing Standard (FIPS) Publication 140-2, and the International Traffic in Arms Regulations (ITAR). Compliance with other laws and statutes may also be accommodated depending on the requirements set forth in the applicable legislation.

Ref	Cloud Computing Question	AWS Information
7	Data location. Where does customer data reside?	AWS customers designate in which physical region their data and their servers will be located. Data replication for S3 data objects is done within the regional cluster in which the data is stored and is not replicated to other data center clusters in other regions. AWS customers designate in which physical region their data and their servers will be located. AWS will not move customers' content from the selected Regions without notifying the customer, unless required to comply with the law or requests of governmental entities. As of this writing, there are eleven regions: US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US) (Oregon), EU (Frankfurt), EU (Ireland), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), China (Beijing), and South America (Sao Paulo).
8	E-Discovery. Does the cloud provider meet the customer's needs to meet electronic discovery procedures and requirements?	AWS provides infrastructure, and customers manage everything else, including the operating system, the network configuration, and the installed applications. Customers are responsible for responding appropriately to legal procedures involving the identification, collection, processing, analysis, and production of electronic documents they store or process using AWS. Upon request, AWS may work with customers who require AWS' assistance in legal proceedings.
9	Data center tours. Are data center tours by customers allowed by the cloud provider?	No. Due to the fact that our data centers host multiple customers, AWS does not allow data center tours by customers, as this exposes a wide range of customers to physical access of a third party. To meet this customer need, an independent and competent auditor validates the presence and operation of controls as part of our SOC 1 Type II report. This broadly accepted third-party validation provides customers with the independent perspective of the effectiveness of controls in place. AWS customers that have signed a non-disclosure agreement with AWS may request a copy of the SOC 1 Type II report. Independent reviews of data center physical security is also a part of the ISO 27001 audit, the PCI assessment, ITAR audit, and the FedRAMP sm testing programs.
10	Third-party access. Are third parties allowed access to the cloud provider data centers?	AWS strictly controls access to data centers, even for internal employees. Third parties are not provided access to AWS data centers except when explicitly approved by the appropriate AWS data center manager per the AWS access policy. See the SOC 1 Type II report for specific controls related to physical access, data center access authorization, and other related controls.
11	Privileged actions. Are privileged actions monitored and controlled?	Controls in place limit access to systems and data and provide that access to systems or data is restricted and monitored. In addition, customer data is and server instances are logically isolated from other customers by default. Privileged user access control is reviewed by an independent auditor during the AWS SOC 1, ISO 27001, PCI, ITAR, and FedRAMP sm audits.
12	Insider access. Does the cloud provider address the threat of inappropriate insider access to customer data and applications?	AWS provides specific SOC 1 controls to address the threat of inappropriate insider access, and the public certification and compliance initiatives covered in this document address insider access. All certifications and third-party attestations evaluate logical access preventative and detective controls. In addition, periodic risk assessments focus on how insider access is controlled and monitored.

Ref	Cloud Computing Question	AWS Information
13	Multi-tenancy. Is customer segregation implemented securely?	The AWS environment is a virtualized, multi-tenant environment. AWS has implemented security management processes, PCI controls, and other security controls designed to isolate each customer from other customers. AWS systems are designed to prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software. This architecture has been validated by an independent PCI Qualified Security Assessor (QSA) and was found to be in compliance with all requirements of PCI DSS version 3.1 published in April 2015. Note that AWS also has single-tenancy options. Dedicated Instances are Amazon EC2 instances launched within your Amazon Virtual Private Cloud (Amazon VPC) that run hardware dedicated to a single customer. Dedicated Instances let you take full advantage of the benefits of Amazon VPC and the AWS cloud while isolating your Amazon EC2 compute instances at the hardware level.
14	Hypervisor vulnerabilities. Has the cloud provider addressed known hypervisor vulnerabilities?	Amazon EC2 currently utilizes a highly customized version of the Xen hypervisor. The hypervisor is regularly assessed for new and existing vulnerabilities and attack vectors by internal and external penetration teams, and is well suited for maintaining strong isolation between guest virtual machines. The AWS Xen hypervisor security is regularly evaluated by independent auditors during assessments and audits. See the AWS security whitepaper for more information on the Xen hypervisor and instance isolation.
15	Vulnerability management. Are systems patched appropriately?	AWS is responsible for patching systems supporting the delivery of service to customers, such as the hypervisor and networking services. This is done as required per AWS policy and in accordance with ISO 27001, NIST, and PCI requirements. Customers control their own guest operating systems, software and applications and are therefore responsible for patching their own systems.
16	Encryption. Do the provided services support encryption?	Yes. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS, SimpleDB, and EC2. IPSec tunnels to VPC are also encrypted. Amazon S3 also offers Server Side Encryption as an option for customers. Customers may also use third-party encryption technologies. Refer to the AWS Security white paper for more information.
17	Data ownership. What are the cloud provider's rights over customer data?	AWS customers retain control and ownership of their data. AWS errs on the side of protecting customer privacy and is vigilant in determining which law enforcement requests we must comply with. AWS does not hesitate to challenge orders from law enforcement if we think the orders lack a solid basis.
18	Data isolation. Does the cloud provider adequately isolate customer data?	All data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. Amazon S3 provides advanced data access controls. Please see the AWS security whitepaper for more information about specific data services' security.
19	Composite services. Does the cloud provider layer its service with other providers' cloud services?	AWS does not leverage any third-party cloud providers to deliver AWS services to customers.

Ref	Cloud Computing Question	AWS Information
20	Physical and environmental controls. Are these controls operated by the cloud provider specified?	Yes. These are specifically outlined in the SOC 1 Type II report. In addition, other certifications AWS supports such as ISO 27001 and FedRAMP sm require best practice physical and environmental controls.
21	Client-side protection. Does the cloud provider allow customers to secure and manage access from clients, such as PC and mobile devices?	Yes. AWS allows customers to manage client and mobile applications to their own requirements.
22	Server security. Does the cloud provider allow customers to secure their virtual servers?	Yes. AWS allows customers to implement their own security architecture. See the AWS security whitepaper for more details on server and network security.
23	Identity and Access Management. Does the service include IAM capabilities?	AWS has a suite of identity and access management offerings, allowing customers to manage user identities, assign security credentials, organize users in groups, and manage user permissions in a centralized way. Please see the AWS web site for more information.
24	Scheduled maintenance outages. Does the provider specify when systems will be brought down for maintenance?	AWS does not require systems to be brought offline to perform regular maintenance and system patching. AWS' own maintenance and system patching generally do not impact customers. Maintenance of instances themselves is controlled by the customer.
25	Capability to scale. Does the provider allow customers to scale beyond the original agreement?	The AWS cloud is distributed, highly secure and resilient, giving customers massive scale potential. Customers may scale up or down, paying for only what they use.
26	Service availability. Does the provider commit to a high level of availability?	AWS does commit to high levels of availability in its service level agreements (SLA). For example, Amazon EC2 commits to annual uptime percentage of at least 99.95% during the service year. Amazon S3 commits to monthly uptime percentage of at least 99.9%. Service credits are provided in the case these availability metrics are not met.
27	Distributed Denial Of Service (DDoS) attacks. How does the provider protect their service against DDoS attacks?	The AWS network provides significant protection against traditional network security issues and the customer can implement further protection. See the AWS Security Whitepaper for more information on this topic, including a discussion of DDoS attacks.
28	Data portability. Can the data stored with a service provider be exported by customer request?	AWS allows customers to move data as needed on and off AWS storage. AWS Import/Export service for S3 accelerates moving large amounts of data into and out of AWS using portable storage devices for transport.
29	Service provider business continuity. Does the service provider operate a business continuity program?	AWS does operate a business continuity program. Detailed information is provided in the AWS Security Whitepaper.

Ref	Cloud Computing Question	AWS Information
30	Customer business continuity. Does the service provider allow customers to implement a business continuity plan?	AWS provides customers with the capability to implement a robust continuity plan, including the utilization of frequent server instance back-ups, data redundancy replication, and multi-region/availability zone deployment architectures.
31	Data durability. Does the service specify data durability?	Amazon S3 provides a highly durable storage infrastructure. Objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 Region. Once stored, Amazon S3 maintains the durability of objects by quickly detecting and repairing any lost redundancy. Amazon S3 also regularly verifies the integrity of data stored using checksums. If corruption is detected, it is repaired using redundant data. Data stored in S3 is designed to provide 99.999999999% durability and 99.99% availability of objects over a given year.
32	Backups. Does the service provide backups to tapes?	AWS allows customers to perform their own backups to tapes using their own tape backup service provider. However, a tape backup is not a service provided by AWS. Amazon S3 service is designed to drive the likelihood of data loss to near zero percent and the durability equivalent of multi-site copies of data objects is achieved through data storage redundancy. For information on data durability and redundancy, please refer to the AWS web site.
33	Price increases. Will the service provider raise prices unexpectedly?	AWS has a history of frequently reducing prices as the cost to provide these services reduces over time. AWS has reduced prices consistently over the past several years.
34	Sustainability. Does the service provider company have long term sustainability potential?	AWS is a leading cloud provider and is a long-term business strategy of Amazon.com. AWS has very high long term sustainability potential.

AWS Contact

Customers can request the reports and certifications produced by our third-party auditors or can request more information about AWS Compliance by contacting [AWS Sales and Business Development](#). The representative will route customers to the proper team depending on nature of the inquiry. For additional information on AWS Compliance, see the [AWS Compliance site](#) or send questions directly to awscompliance@amazon.com.

Appendix A: CSA Consensus Assessments Initiative Questionnaire v3.0.1

The Cloud Security Alliance (CSA) is a “not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing.” [Reference

<https://cloudsecurityalliance.org/about/>] A wide range of industry security practitioners, corporations, and associations participate in this organization to achieve its mission.

The CSA Consensus Assessments Initiative Questionnaire provides a set of questions the CSA anticipates a cloud consumer and/or a cloud auditor would ask of a cloud provider. It provides a series of security, control, and process questions which can then be used for a wide range of uses, including cloud provider selection and security evaluation. AWS has completed this questionnaire with the answers below.

Control Group	CID	Consensus Assessment Questions	AWS Response
Application & Interface Security <i>Application Security</i>	AIS-01.1	Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?	The AWS system development lifecycle incorporates industry best practices which include formal design reviews by the AWS Security Team, threat modeling and completion of a risk assessment. Refer to the AWS Overview of Security Processes for further details. AWS has in place procedures to manage new development of resources. Refer to ISO 27001 standard, Annex A, domain 14 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	AIS-01.2	Do you use an automated source code analysis tool to detect security defects in code prior to production?	
	AIS-01.3	Do you use manual source-code analysis to detect security defects in code prior to production?	
	AIS-01.4	Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	
	AIS-01.5	(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	

Control Group	CID	Consensus Assessment Questions	AWS Response
Application & Interface Security <i>Customer Access Requirements</i>	AIS-02.1	Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems?	AWS Customers retain responsibility to ensure their usage of AWS is in compliance with applicable laws and regulations. AWS communicates its security and control environment to customers through industry certifications and third-party attestations, white papers (available at http://aws.amazon.com/compliance) and providing certifications, reports and other relevant documentation directly to AWS Customers.
	AIS-02.2	Are all requirements and trust levels for customers' access defined and documented?	
Application & Interface Security <i>Data Integrity</i>	AIS-03.1	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	AWS data integrity controls as described in AWS SOC reports illustrates the data integrity controls maintained through all phases including transmission, storage and processing. In addition, refer to ISO 27001 standard, Annex A, domain 14 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Application & Interface Security <i>Data Security / Integrity</i>	AIS-04.1	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	AWS Data Security Architecture was designed to incorporate industry leading practices. Refer to AWS Certifications, reports and whitepapers for additional details on the various leading practices that AWS adheres to (available at http://aws.amazon.com/compliance).
Audit Assurance & Compliance <i>Audit Planning</i>	AAC-01.1	Do you produce audit assertions using a structured, industry accepted format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	AWS obtains certain industry certifications and independent third-party attestations and provides certain certifications, reports and other relevant documentation directly to AWS Customers.
Audit Assurance & Compliance <i>Independent Audits</i>	AAC-02.1	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	AWS provides third-party attestations, certifications, Service Organization Controls (SOC) reports and other relevant compliance reports directly to our customers under NDA. The AWS ISO 27001 certification can be downloaded here: http://do.awsstatic.com/certifications/iso_27001_global_certification.pdf. The AWS SOC 3 report can be downloaded here: https://do.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf. AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. In addition, external vulnerability threat
	AAC-02.2	Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	
	AAC-02.3	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	AAC - 02.4	Do you conduct internal audits regularly as prescribed by industry best practices and guidance?	assessments are performed regularly by independent security firms. Findings and recommendations resulting from these assessments are categorized and delivered to AWS leadership.
	AAC - 02.5	Do you conduct external audits regularly as prescribed by industry best practices and guidance?	In addition, the AWS control environment is subject to regular internal and external audits and risk assessments. AWS engages with external certifying bodies and independent auditors to review and test the AWS overall control environment.
	AAC - 02.6	Are the results of the penetration tests available to tenants at their request?	
	AAC - 02.7	Are the results of internal and external audits available to tenants at their request?	
	AAC - 02.8	Do you have an internal audit program that allows for cross-functional audit of assessments?	
Audit Assurance & Compliance <i>Information System Regulatory Mapping</i>	AAC -03.1	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	All data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. Customers retain control and ownership of their data, thus it is their responsibility to choose to encrypt the data. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS, SimpleDB and EC2. IPSec tunnels to VPC are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security
	AAC - 03.2	Do you have capability to recover data for a specific customer in the case of a failure or data loss?	
	AAC - 03.3	Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	AWS allows customers to perform their own backups to tapes using their own tape backup service provider. However, a tape backup is not a service provided by AWS. Amazon S3 and Glacier services are designed to drive the likelihood of data loss to near zero percent and the durability equivalent of multi-site copies of data objects is achieved through data storage redundancy. For information on data durability and redundancy, please refer to the AWS website. AWS Customers designate in which physical region their content will be located. AWS will not move customers' content from the selected regions without notifying the customer, unless required to comply with the law or requests of governmental entities. As of this writing, there are eleven regions: US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US)(Oregon), EU (Ireland), EU (Frankfurt), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), China (Beijing) Region, and South America (Sao Paulo).

Control Group	CID	Consensus Assessment Questions	AWS Response
	AAC - 03.4	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	AWS monitors relevant legal and regulatory requirements. Refer to ISO 27001 standard Annex 18 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Business Continuity Management & Operational Resilience <i>Business Continuity Planning</i>	BCR -01.1	Do you provide tenants with geographically resilient hosting options?	Data centers are built in clusters in various global regions. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Customers should architect their AWS usage to take advantage of multiple Regions and Availability Zones. Refer to AWS Overview of Cloud Security whitepaper for additional details - available at http://aws.amazon.com/security .
	BCR -01.2	Do you provide tenants with infrastructure service failover capability to other providers?	
Business Continuity Management & Operational Resilience <i>Business Continuity Testing</i>	BCR -02.1	Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	AWS Business Continuity Policies and Plans have been developed and tested in alignment with ISO 27001 standards. Refer to ISO 27001 standard, annex A domain 17 for further details on AWS and business continuity.
Business Continuity Management & Operational Resilience <i>Power / Telecommunications</i>	BCR -03.1	Do you provide tenants with documentation showing the transport route of their data between your systems?	AWS Customers designate in which physical region their data and servers will be located. AWS will not move customers' content from the selected regions without notifying the customer, unless required to comply with the law or requests of governmental entities. AWS SOC reports provides additional details. Customers can also choose their network path to AWS facilities, including over dedicated, private networks where the customer controls the traffic routing.
	BCR - 03.2	Can tenants define how their data is transported and through which legal jurisdictions?	
Business Continuity Management & Operational Resilience Documentation	BCR -04.1	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	Information System Documentation is made available internally to AWS personnel through the use of Amazon's Intranet site. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security/ . Refer to ISO 27001 Appendix A Domain 12.
Business Continuity Management & Operational Resilience <i>Environmental Risks</i>	BCR -05.1	Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied?	AWS data centers incorporate physical protection against environmental risks. AWS' physical protection against environmental risks has been validated by an independent auditor and has been certified as being in alignment with ISO 27002 best practices. Refer to ISO 27001 standard, Annex A domain 11.

Control Group	CID	Consensus Assessment Questions	AWS Response
Business Continuity Management & Operational Resilience <i>Equipment Location</i>	BCR -06.1	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?	AWS data centers incorporate physical protection against environmental risks. AWS' physical protection against environmental risks has been validated by an independent auditor and has been certified as being in alignment with ISO 27002 best practices. Refer to ISO 27001 standard, Annex A domain 11.
Business Continuity Management & Operational Resilience <i>Equipment Maintenance</i>	BCR -07.1	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	EBS Snapshot functionality allows customers to capture and restore virtual machine images at any time. Customers can export their AMIs and use them on premise or at another provider (subject to software licensing restrictions). Refer to the AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security .
	BCR -07.2	If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?	
	BCR -07.3	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	
	BCR -07.4	If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	
	BCR -07.5	Does your cloud solution include software/provider independent restore and recovery capabilities?	
Business Continuity Management & Operational Resilience <i>Equipment Power Failures</i>	BCR -08.1	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	AWS equipment is protected from utility service outages in alignment with ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. AWS SOC reports provides additional details on controls in place to minimize the effect of a malfunction or physical disaster to the computer and data center facilities. In addition, refer to the AWS Cloud Security Whitepaper - available at http://aws.amazon.com/security.

Control Group	CID	Consensus Assessment Questions	AWS Response
Business Continuity Management & Operational Resilience <i>Impact Analysis</i>	BCR-09.1	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	AWS CloudWatch provides monitoring for AWS cloud resources and the applications customers run on AWS. Refer to aws.amazon.com/cloudwatch for additional details. AWS also publishes our most up-to-the-minute information on service availability on the Service Health Dashboard. Refer to status.aws.amazon.com .
	BCR-09.2	Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	
	BCR-09.3	Do you provide customers with ongoing visibility and reporting of your SLA performance?	
Business Continuity Management & Operational Resilience <i>Policy</i>	BCR-10.1	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	Policies and Procedures have been established through AWS Security framework based upon NIST 800-53, ISO 27001, ISO 27017, ISO 27018, ISO 9001 standard and the PCI DSS requirements. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/compliance.
Business Continuity Management & Operational Resilience <i>Retention Policy</i>	BCR-11.1	Do you have technical control capabilities to enforce tenant data retention policies?	AWS provide customers with the ability to delete their data. However, AWS Customers retain control and ownership of their data so it is the customer's responsibility to manage data retention to their own requirements. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security. AWS errs on the side of protecting customer privacy and is vigilant in determining which law enforcement requests we must comply with. AWS does not hesitate to challenge orders from law enforcement if we think the orders lack a solid basis. For additional information refer to https://aws.amazon.com/compliance/data-privacy-faq/. AWS backup and redundancy mechanisms have been developed and tested in alignment with ISO 27001 standards. Refer to ISO 27001 standard, annex A domain 12 and the AWS SOC 2 report for additional information on AWS backup and redundancy mechanisms.
	BCR-11.2	Do you have a documented procedure for responding to requests for tenant data from governments or third parties?	
	BCR-11.4	Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	
	BCR-11.5	Do you test your backup or redundancy mechanisms at least annually?	
Change Control & Configuration Management <i>New Development / Acquisition</i>	CCC-01.1	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	Policies and Procedures have been established through AWS Security framework based upon NIST 800-53, ISO 27001, ISO 27017, ISO 27018, ISO 9001 standard and the PCI DSS requirements. Whether a customer is new to AWS or an advanced user, useful information about the services, ranging from introductions to advanced features, can be found on the AWS Documentation section of our website at https://aws.amazon.com/documentation/.
	CCC-01.2	Is documentation available that describes the installation, configuration and use of products/services/features?	

Control Group	CID	Consensus Assessment Questions	AWS Response
Change Control & Configuration Management <i>Outsourced Development</i>	CCC-02.1	Do you have controls in place to ensure that standards of quality are being met for all software development?	AWS does not generally outsource development of software. AWS incorporates standards of quality as part of the system development lifecycle (SDLC) processes.
	CCC-02.2	Do you have controls in place to detect source code security defects for any outsourced software development activities?	Refer to ISO 27001 standard, Annex A, domain 12 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Change Control & Configuration Management <i>Quality Testing</i>	CCC-03.1	Do you provide your tenants with documentation that describes your quality assurance process?	AWS maintains an ISO 9001 certification. This is an independent validation of AWS quality system and determined that AWS activities comply with ISO 9001 requirements. AWS Security Bulletins notify customers of security and privacy events. Customers can subscribe to the AWS Security Bulletin RSS feed on our website. Refer to aws.amazon.com/security/security-bulletins/ .
	CCC-03.2	Is documentation describing known issues with certain products/services available?	AWS also publishes our most up-to-the-minute information on service availability on the Service Health Dashboard. Refer to status.aws.amazon.com .
	CCC-03.3	Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	The AWS system development lifecycle (SDLC) incorporates industry best practices which include formal design reviews by the AWS Security Team, threat modeling and completion of a risk assessment. Refer to the AWS Overview of Security Processes for further details.
	CCC-03.4	Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	In addition, refer to ISO 27001 standard, Annex A, domain 14 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Change Control & Configuration Management <i>Unauthorized Software Installations</i>	CCC-04.1	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	AWS' program, processes and procedures for managing malicious software is in alignment with ISO 27001 standards. Refer to ISO 27001 standard, Annex A, domain 12 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Change Control & Configuration Management <i>Production Changes</i>	CCC-05.1	Do you provide tenants with documentation that describes your production change management procedures and their roles / rights / responsibilities within it?	AWS SOC reports provides an overview of the controls in place to manage change management in the AWS environment. In addition, refer to ISO 27001 standard, Annex A, domain 14 for further details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.

Control Group	CID	Consensus Assessment Questions	AWS Response
Data Security & Information Lifecycle Management <i>Classification</i>	DSI-01.1	Do you provide a capability to identify virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?	Virtual Machines are assigned to customers as a part of the EC2 service. Customers retain control over what resources are being used and where resources reside. Refer to the AWS website for additional details - http://aws.amazon.com .
	DSI-01.2	Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?	AWS provides the ability to tag EC2 resources. A form of metadata, EC2 tags can be used to create user-friendly names, enhance searchability, and improve coordination between multiple users. The AWS Management Console has also supports tagging.
	DSI-01.3	Do you have a capability to use system geographic location as an authentication factor?	AWS provides the capability of conditional user access based on IP address. Customers can add conditions to control how users can use AWS, such as time of day, their originating IP address, or whether they are using SSL.
	DSI-01.4	Can you provide the physical location/geography of storage of a tenant's data upon request?	AWS provides customers the flexibility to place instances and store data within multiple geographic Regions. AWS Customers designate in which physical region their data and their servers will be located. AWS will not move customers' content from the selected Regions without notifying the customer, unless required to comply with the law or requests of governmental entities. As of this writing, there are eleven regions: US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US) (Oregon), EU (Ireland), EU (Frankfurt), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), China (Beijing) Region and South America (Sao Paulo).
	DSI-01.5	Can you provide the physical location/geography of storage of a tenant's data in advance?	
	DSI-01.6	Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	AWS Customers retain control and ownership of their data and may implement a structured data-labeling standard to meet their requirements.
	DSI-01.7	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	AWS provides customers the flexibility to place instances and store data within multiple geographic regions. AWS Customers designate in which physical region their data and their servers will be located. AWS will not move customers' content from the selected Regions without notifying the customer, unless required to comply with the law or requests of governmental entities. As of this writing, there are eleven regions: US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US) (Oregon), EU (Ireland), EU (Frankfurt), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), China (Beijing) Region and South America (Sao Paulo).
Data Security & Information Lifecycle Management <i>Data Inventory / Flows</i>	DSI-02.1	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?	AWS Customers designate in which physical region their content will be located. AWS will not move customers' content from the selected regions without notifying the customer, unless required to comply with the law or requests of governmental entities. As of this writing, there are eleven regions: US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US)(Oregon), EU (Ireland), EU (Frankfurt), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), China (Beijing) Region, and South America (Sao Paulo).

Control Group	CID	Consensus Assessment Questions	AWS Response
	DSI-02.2	Can you ensure that data does not migrate beyond a defined geographical residency?	
Data Security & Information Lifecycle Management <i>eCommerce Transactions</i>	DSI-03.1	Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	All of the AWS APIs are available via SSH-protected endpoints which provide server authentication. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS, SimpleDB and EC2. IPSec tunnels to VPC are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Customers may also use third-party encryption technologies.
	DSI-03.2	Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security .
Data Security & Information Lifecycle Management <i>Handling / Labeling / Security Policy</i>	DSI-04.1	Are policies and procedures established for labeling, handling and the security of data and objects that contain data?	AWS Customers retain control and ownership of their data and may implement a labeling and handling policy and procedures to meet their requirements.
	DSI-04.2	Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?	
Data Security & Information Lifecycle Management <i>Nonproduction Data</i>	DSI-05.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	AWS Customers retain control and ownership of their own data. AWS provides customers the ability to maintain and develop production and non-production environments. It is the responsibility of the customer to ensure that their production data is not replicated to non-production environments.
Data Security & Information Lifecycle Management <i>Ownership / Stewardship</i>	DSI-06.1	Are the responsibilities regarding data stewardship defined, assigned, documented and communicated?	AWS Customers retain control and ownership of their own data. Refer to the AWS Customer Agreement for additional information.
Data Security & Information Lifecycle Management <i>Secure Disposal</i>	DSI-07.1	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?	When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. If a hardware device is unable to be

Control Group	CID	Consensus Assessment Questions	AWS Response
	DSI-07.2	Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security. Amazon EBS volumes are presented to you as raw unformatted block devices that have been wiped prior to being made available for use. Wiping occurs immediately before reuse so that you can be assured that the wipe process completed. If you have procedures requiring that all data be wiped via a specific method, such as those detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual") or NIST 800-88 ("Guidelines for Media Sanitization"), you have the ability to do so on Amazon EBS. You should conduct a specialized wipe procedure prior to deleting the volume for compliance with your established requirements. Encryption of sensitive data is generally a good security practice, and AWS provides the ability to encrypt EBS volumes and their snapshots with AES-256. The encryption occurs on the servers that host the EC2 instances, providing encryption of data as it moves between EC2 instances and EBS storage. In order to be able to do this efficiently and with low latency, the EBS encryption feature is only available on EC2's more powerful instance types (e.g., M3, C3, R3, G2).
Datacenter Security <i>Asset Management</i>	DCS-01.1	Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?	In alignment with ISO 27001 standards, AWS Hardware assets are assigned an owner, tracked and monitored by the AWS personnel with AWS proprietary inventory management tools. AWS procurement and supply chain team maintain relationships with all AWS suppliers. Refer to ISO 27001 standards; Annex A, domain 8 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	DCS-01.2	Do you maintain a complete inventory of all of your critical supplier relationships?	
Datacenter Security <i>Controlled Access Points</i>	DCS-02.1	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented?	Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means. The AWS SOC reports provides additional details on the specific control activities executed by AWS. Refer to ISO 27001 standards; Annex A, domain 11 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Datacenter Security <i>Equipment Identification</i>	DCS-03.1	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	AWS manages equipment identification in alignment with ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.

Control Group	CID	Consensus Assessment Questions	AWS Response
Datacenter Security <i>Offsite Authorization</i>	DCS -04.1	Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another? (e.g., offsite backups, business continuity failovers, replication)	AWS Customers can designate which physical region their data will be located. AWS will not move customers' content from the selected Regions without notifying the customer unless required to comply with the law or requests of governmental entities. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security .
Datacenter Security <i>Offsite equipment</i>	DCS -05.1	Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment?	In alignment with ISO 27001 standards, when a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices. Refer to ISO 27001 standards; Annex A, domain 8 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Datacenter Security <i>Policy</i>	DCS -06.1	Can you provide evidence that policies, standards and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?	AWS engages with external certifying bodies and independent auditors to review and validate our compliance with compliance frameworks. AWS SOC reports provides additional details on the specific physical security control activities executed by AWS. Refer to ISO 27001 standards; Annex A, domain 11 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	DCS -06.2	Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards and procedures?	In alignment with ISO 27001 standard, all AWS employees complete periodic Information Security training which requires an acknowledgement to complete. Compliance audits are periodically performed to validate that employees understand and follow the established policies. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security . AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification. In addition AWS SOC 1 and SOC 2 reports provides further information.
Datacenter Security <i>Secure Area Authorization</i>	DCS -07.1	Do you allow tenants to specify which of your geographic locations their data is allowed to move into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?	AWS Customers designate which physical region their data will be located. AWS will not move customers' content from the selected Regions without notifying the customer unless required to comply with the law or requests of governmental entities. As of this writing, there are eleven regions: US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US)(Oregon), EU (Ireland), EU (Frankfurt), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), China (Beijing) Region, and South America (Sao Paulo).

Control Group	CID	Consensus Assessment Questions	AWS Response
Datacenter Security <i>Unauthorized Persons Entry</i>	DCS -08.1	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	Physical access is strictly controlled both at the perimeter and at building ingress points and includes, but is not limited to, professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. Physical access points to server locations are recorded by closed circuit television camera (CCTV) as defined in the AWS Data Center Physical Security Policy.
Datacenter Security <i>User Access</i>	DCS -09.1	Do you restrict physical access to information assets and functions by users and support personnel?	AWS Physical Security Mechanisms are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.
Encryption & Key Management <i>Entitlement</i>	EKM -01.1	Do you have key management policies binding keys to identifiable owners?	AWS provides customers the ability to use their own encryption mechanism for nearly all services including S3, EBS and EC2. VPC sessions are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Internally, AWS establishes and manages cryptographic keys for required cryptography employed within the AWS infrastructure. An AWS developed secure key and credential manager is used to create, protect and distribute symmetric keys and is used to secure and distribute: AWS credentials needed on hosts, RSA public/private keys and X.509 Certifications. AWS cryptographic processes are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP.
Encryption & Key Management <i>Key Generation</i>	EKM -02.1	Do you have a capability to allow creation of unique encryption keys per tenant?	AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. IPSec tunnels to VPC are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/).
	EKM -02.2	Do you have a capability to manage encryption keys on behalf of tenants?	Refer to AWS SOC reports for more details on KMS.
	EKM -02.3	Do you maintain key management procedures?	In addition, refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security .
	EKM -02.4	Do you have documented ownership for each stage of the lifecycle of encryption keys?	Internally, AWS establishes and manages cryptographic keys for required cryptography employed within the AWS infrastructure. AWS produces, controls and distributes symmetric cryptographic keys using NIST approved key management technology and processes in the AWS information system. An AWS developed secure key and credential manager is used to create, protect and distribute symmetric keys and is used to secure and distribute: AWS credentials needed on hosts, RSA public/private keys and X.509 Certifications.
	EKM -02.5	Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	AWS cryptographic processes are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP.
Encryption & Key	EKM -03.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?	AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. IPSec tunnels to VPC are also encrypted. In addition, customers can leverage AWS Key

Control Group	CID	Consensus Assessment Questions	AWS Response
Management Encryption	EKM - 03.2	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS SOC reports for more details on KMS. In addition, refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
	EKM - 03.3	Do you support tenant-generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate (e.g. identity-based encryption)?	
	EKM - 03.4	Do you have documentation establishing and defining your encryption management policies, procedures and guidelines?	
Encryption & Key Management Storage and Access	EKM - 04.1	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS SOC reports for more details on KMS.
	EKM - 04.2	Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	AWS establishes and manages cryptographic keys for required cryptography employed within the AWS infrastructure. AWS produces, controls and distributes symmetric cryptographic keys using NIST approved key management technology and processes in the AWS information system. An AWS developed secure key and credential manager is used to create, protect and distribute symmetric keys and is used to secure and distribute: AWS credentials needed on hosts, RSA public/private keys and X.509 Certifications.
	EKM - 04.3	Do you store encryption keys in the cloud?	
	EKM - 04.4	Do you have separate key management and key usage duties?	AWS cryptographic processes are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP.
Governance and Risk Management Baseline Requirements	GR M- 01.1	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	In alignment with ISO 27001 standards, AWS maintains system baselines for critical components. Refer to ISO 27001 standards, Annex A, domain 14 and 18 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. Customers can provide their own virtual machine image. VM Import enables customers to easily import virtual machine images from your existing environment to Amazon EC2 instances.
	GR M- 01.2	Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	
	GR M- 01.3	Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?	

Control Group	CID	Consensus Assessment Questions	AWS Response
Governance and Risk Management <i>Risk Assessments</i>	GR M-02.1	Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status)?	AWS does publish independent auditor reports and certifications to provide customers with considerable information regarding the policies, processes, and controls established and operated by AWS. The relevant certifications and reports can be provided to AWS Customers. Continuous Monitoring of logical controls can be executed by customers on their own systems.
	GR M-02.2	Do you conduct risk assessments associated with data governance requirements at least once a year?	In alignment with ISO 27001 standard, AWS maintains a Risk Management program to mitigate and manage risk. In addition AWS maintains an AWS ISO 27018 certification. Alignment with ISO 27018 demonstrates to customers that AWS has a system of controls in place that specifically address the privacy protection of their content. For more information refer to the AWS Compliance ISO 27018 FAQ http://aws.amazon.com/compliance/iso-27018-faqs/ .
Governance and Risk Management <i>Management Oversight</i>	GR M-03.1	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	The Control environment at Amazon begins at the highest level of the Company. Executive and senior leadership play important roles in establishing the Company's tone and core values. Every employee is provided with the Company's Code of Business Conduct and Ethics and completes periodic training. Compliance audits are performed so that employees understand and follow the established policies. Refer to AWS Risk & Compliance whitepaper for additional details - available at http://aws.amazon.com/compliance .
Governance and Risk Management <i>Management Program</i>	GR M-04.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	AWS provides our customers with our ISO 27001 certification. The ISO 27001 certification is specifically focused on the AWS ISMS and measures how AWS internal processes follow the ISO standard. Certification means a third party accredited independent auditor has performed an assessment of our processes and controls and confirms they are operating in alignment with the ISO 27001 certification standard. For additional information refer to the AWS Compliance ISO 27001 FAQ website: http://aws.amazon.com/compliance/iso-27001-faqs/ .
	GR M-04.2	Do you review your Information Security Management Program (ISMP) least once a year?	
Governance and Risk Management <i>Management Support / Involvement</i>	GR M-05.1	Do you ensure your providers adhere to your information security and privacy policies?	AWS has established information security framework and policies which have integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, PCI DSS v3.1 and National Institute of Standards and Technology (NIST) Publication 800-53 (Recommended Security Controls for Federal Information Systems).
Governance and Risk Management <i>Policy</i>	GR M-06.1	Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?	AWS manages third-party relationships in alignment with ISO 27001 standards. AWS Third Party requirements are reviewed by independent external

Control Group	CID	Consensus Assessment Questions	AWS Response
	GR M-06.2	Do you have agreements to ensure your providers adhere to your information security and privacy policies?	auditors during audits for our PCI DSS, ISO 27001 and FedRAMP compliance. Information about the AWS Compliance programs is published publicly on our website at http://aws.amazon.com/compliance/.
	GR M-06.3	Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?	
	GR M-06.4	Do you disclose which controls, standards, certifications and/or regulations you comply with?	
Governance and Risk Management <i>Policy Enforcement</i>	GR M-07.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	AWS provides security policies and security training to employees to educate them as to their role and responsibilities concerning information security. Employees who violate Amazon standards or protocols are investigated and appropriate disciplinary action (e.g. warning, performance plan, suspension, and/or termination) is followed.
	GR M-07.2	Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	Refer to the AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security . Refer to ISO 27001 Annex A, domain 7 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Governance and Risk Management <i>Business / Policy Change Impacts</i>	GR M-08.1	Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective?	Updates to AWS security policies, procedures, standards and controls occur on an annual basis in alignment with the ISO 27001 standard. Refer to ISO 27001 for additional information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification.
Governance and Risk Management <i>Policy Reviews</i>	GR M-09.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	Our AWS Cloud Security Whitepaper and Risk and Compliance whitepapers, available at http://aws.amazon.com/security and http://aws.amazon.com/compliance , are updated on a regular basis to reflect updates to the AWS policies.
	GR M-09.2	Do you perform, at minimum, annual reviews to your privacy and security policies?	The AWS SOC reports provide details related to privacy and security policy review.
Governance and Risk Management <i>Assessments</i>	GR M-10.1	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	In alignment with ISO 27001 AWS has developed a Risk Management program to mitigate and manage risk. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification. Refer to AWS Risk and Compliance Whitepaper (available at aws.amazon.com/security) for additional details on AWS Risk Management Framework.

Control Group	CID	Consensus Assessment Questions	AWS Response
	GR M-10.2	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?	
Governance and Risk Management Program	GR M-11.1	Do you have a documented, organization-wide program in place to manage risk?	In alignment with ISO 27001, AWS maintains a Risk Management program to mitigate and manage risk.
	GR M-11.2	Do you make available documentation of your organization-wide risk management program?	AWS management has a strategic business plan which includes risk identification and the implementation of controls to mitigate or manage risks. AWS management re-evaluates the strategic business plan at least biannually. This process requires management to identify risks within its areas of responsibility and to implement appropriate measures designed to address those risks. AWS Risk Management program is reviewed by independent external auditors during audits for our PCI DSS, ISO 27001 and FedRAMP compliance.
Human Resources Asset Returns	HRS -01.1	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	AWS Customers retain the responsibility to monitor their own environment for privacy breaches. The AWS SOC reports provides an overview of the controls in place to monitor AWS managed environment.
	HRS -01.2	Is your Privacy Policy aligned with industry standards?	
Human Resources Background Screening	HRS -02.1	Pursuant to local laws, regulations, ethics and contractual constraints, are all employment candidates, contractors and involved third parties subject to background verification?	AWS conducts criminal background checks, as permitted by applicable law, as part of pre-employment screening practices for employees commensurate with the employee's position and level of access to AWS facilities. The AWS SOC reports provides additional details regarding the controls in place for background verification.
Human Resources Employment Agreements	HRS -03.1	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	In alignment with ISO 27001 standard, all AWS employees complete periodic role based training that includes AWS Security training and requires an acknowledgement to complete. Compliance audits are periodically performed to validate that employees understand and follow the established policies. Refer to SOC reports for additional details.
	HRS -03.2	Do you document employee acknowledgment of training they have completed?	All personnel supporting AWS systems and devices must sign a non-disclosure agreement prior to being granted access. Additionally, upon hire, personnel are required to read and accept the Acceptable Use Policy and the Amazon Code of Business Conduct and Ethics (Code of Conduct) Policy.
	HRS -03.3	Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	HRS - 03.4	Is successful and timed completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems?	
	HRS - 03.5	Are personnel trained and provided with awareness programs at least once a year?	
Human Resources <i>Employment Termination</i>	HRS -04.1	Are documented policies, procedures and guidelines in place to govern change in employment and/or termination?	AWS Human Resources team defines internal management responsibilities to be followed for termination and role change of employees and vendors. AWS SOC reports provide additional details.
	HRS - 04.2	Do the above procedures and guidelines account for timely revocation of access and return of assets?	Access is automatically revoked when an employee's record is terminated in Amazon's Human Resources system. When changes in an employee's job function occur, continued access must be explicitly approved to the resource or it will be automatically revoked. AWS SOC reports provide further details on User access revocation. In addition the AWS Security White paper, section "Employee Lifecycle" provides additional information. Refer to ISO 27001 Annex A, domain 7 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Human Resources <i>Portable / Mobile Devices</i>	HRS -05.1	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g. laptops, cell phones and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to manage mobile security devices and the access to the customer's content.
Human Resources <i>Nondisclosure Agreements</i>	HRS -06.1	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented and reviewed at planned intervals?	Amazon Legal Counsel manages and periodically revises the Amazon NDA to reflect AWS business needs.
Human Resources <i>Roles / Responsibilities</i>	HRS -07.1	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	The AWS Cloud Security Whitepaper and the AWS Risk and Compliance Whitepaper provide details on the roles and responsibilities of AWS and those of our Customers. The whitepapers area available at: http://aws.amazon.com/security and http://aws.amazon.com/compliance .

Control Group	CID	Consensus Assessment Questions	AWS Response
Human Resources <i>Acceptable Use</i>	HRS -08.1	Do you provide documentation regarding how you may or access tenant data and metadata?	AWS has a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy). The policy addresses purpose, scope, roles, responsibilities and management commitment. AWS employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function. Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to manage mobile security devices and the access to the customer's content. Refer to the ISO 27001 standard and 27018 code of practice for additional information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 and ISO 27018.
	HRS -08.2	Do you collect or create metadata about tenant data usage through inspection technologies (search engines, etc.)?	
	HRS -08.3	Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?	
Human Resources <i>Training / Awareness</i>	HRS -09.1	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model segregation of duties implications and conflicts of interest) for all persons with access to tenant data?	In alignment with ISO 27001 standard, all AWS employees complete periodic Information Security training which requires an acknowledgement to complete. Compliance audits are periodically performed to validate that employees understand and follow the established policies. AWS roles and responsibilities are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.
	HRS -09.2	Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	
Human Resources <i>User Responsibility</i>	HRS -10.1	Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory requirements?	AWS has implemented various methods of internal communication at a global level to help employees understand their individual roles and responsibilities and to communicate significant events in a timely manner. These methods include orientation and training programs for newly hired employee as well as electronic mail messages and the posting of information via the Amazon intranet. Refer to ISO 27001 standard, Annex A, domain 7 and 8. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. In addition the AWS Cloud Security Whitepaper provides further details - available at http://aws.amazon.com/security.
	HRS -10.2	Are users made aware of their responsibilities for maintaining a safe and secure working environment?	
	HRS -10.3	Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?	
Human Resources <i>Workspace</i>	HRS -11.1	Do your data management policies and procedures address tenant and service level conflicts of interests?	AWS data management policies are in alignment with ISO 27001 standard. Refer to ISO 27001 standard, Annex A, domain 8 and 9. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. AWS SOC reports

Control Group	CID	Consensus Assessment Questions	AWS Response
	HRS-11.2	Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?	provides additional details on the specific control activities executed by AWS to prevent unauthorized access to AWS resources. AWS has identified auditable event categories across systems and devices within the AWS system. Service teams configure the auditing features to record continuously the security-related events in accordance with requirements. Audit records contain a set of data elements in order to support necessary analysis requirements. In addition, audit records are available for AWS Security team or other appropriate teams to perform inspection or analysis on demand, and in response to security-related or business-impacting events.
	HRS-11.3	Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	
Identity & Access Management <i>Audit Tools Access</i>	IAM-01.1	Do you restrict, log and monitor access to your information security management systems? (E.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)	In alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources. AWS SOC reports outlines the controls in place to manage access provisioning to AWS resources. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
	IAM-01.2	Do you monitor and log privileged access (administrator level) to information security management systems?	AWS has identified auditable event categories across systems and devices within the AWS system. Service teams configure the auditing features to record continuously the security-related events in accordance with requirements. The log storage system is designed to provide a highly scalable, highly available service that automatically increases capacity as the ensuing need for log storage grows. Audit records contain a set of data elements in order to support necessary analysis requirements. In addition, audit records are available for AWS Security team or other appropriate teams to perform inspection or analysis on demand, and in response to security-related or business-impacting events. Designated personnel on AWS teams receive automated alerts in the event of an audit processing failure. Audit processing failures include, for example, software/hardware errors. When alerted, on-call personnel issue a trouble ticket and track the event until it is resolved. AWS logging and monitoring processes are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP compliance.
Identity & Access Management <i>User Access Policy</i>	IAM-02.1	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	AWS SOC reports provides further details on User access revocation. In addition the AWS Security White paper, section "Employee Lifecycle" provides additional information. Refer to ISO 27001 Annex A, domain 9 for additional details. AWS has

Control Group	CID	Consensus Assessment Questions	AWS Response
	IAM - 02.2	Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?	been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Identity & Access Management <i>Diagnostic / Configuration Ports Access</i>	IAM -03.1	Do you use dedicated secure networks to provide management access to your cloud service infrastructure?	Controls in place limit access to systems and data and provide that access to systems or data is restricted and monitored per the AWS access policy. In addition, customer data is and server instances are logically isolated from other customers by default. Privileged user access controls are reviewed by an independent auditor during the AWS SOC, ISO 27001, PCI, ITAR, and FedRAMP audits.
Identity & Access Management <i>Policies and Procedures</i>	IAM -04.1	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	
	IAM - 04.2	Do you manage and store the user identity of all personnel who have network access, including their level of access?	
Identity & Access Management <i>Segregation of Duties</i>	IAM -05.1	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	Customers retain the ability to manage segregations of duties of their AWS resources. Internally, AWS aligns with ISO 27001 standards for managing segregation of duties. Refer to ISO 27001 standard, Annex A, domain 6.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Identity & Access Management <i>Source Code Access Restriction</i>	IAM -06.1	Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?	In alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources. AWS SOC reports outlines the controls in place to manage access provisioning to AWS resources. Refer to AWS Overview of Security Processes for additional details - available at http://aws.amazon.com/security .
	IAM - 06.2	Are controls in place to prevent unauthorized access to tenant application, program or object source code, and assure it is restricted to authorized personnel only?	
Identity & Access Management <i>Third Party Access</i>	IAM -07.1	Do you provide multi-failure disaster recovery capability?	AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. In case of failure, automated processes move customer data traffic away from the affected area. AWS SOC reports provides further details. ISO 27001 standard Annex A, domain 15 provides additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification.
	IAM - 07.2	Do you monitor service continuity with upstream providers in the event of provider failure?	
	IAM - 07.3	Do you have more than one provider for each service you depend on?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	IAM - 07.4	Do you provide access to operational redundancy and continuity summaries, including the services you depend on?	
	IAM -07.5	Do you provide the tenant the ability to declare a disaster?	
	IAM - 07.6	Do you provided a tenant-triggered failover option?	
	IAM -07.7	Do you share your business continuity and redundancy plans with your tenants?	
Identity & Access Management <i>User Access Restriction / Authorization</i>	IAM -08.1	Do you document how you grant and approve access to tenant data?	AWS Customers retain control and ownership of their data. Controls in place limit access to systems and data and provide that access to systems or data is restricted and monitored. In addition, customer data and server instances are logically isolated from other customers by default. Privileged user access controls are reviewed by an independent auditor during the AWS SOC, ISO 27001, PCI, ITAR, and FedRAMP audits.
	IAM - 08.2	Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	
Identity & Access Management <i>User Access Authorization</i>	IAM -09.1	Does your management provision the authorization and restrictions for user access (e.g. employees, contractors, customers (tenants), business partners and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	Unique user identifiers are created as part of the onboarding workflow process in the AWS human resources management system. The device provisioning process helps ensure unique identifiers for devices. Both processes include manager approval to establish the user account or device. Initial authenticators are delivered to user's in-person and to devices as part of the provisioning process. Internal users can associate SSH public keys with their account. System account authenticators are provided to the requestor as part of the account creation process after the identity of the requestor is verified.
	IAM - 09.2	Do you provide upon request user access (e.g. employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	AWS has established controls to address the threat of inappropriate insider access. All certifications and third-party attestations evaluate logical access preventative and detective controls. In addition, periodic risk assessments focus on how insider access is controlled and monitored.
Identity & Access Management <i>User Access Reviews</i>	IAM -10.1	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?	In alignment with ISO 27001 standard, all access grants are reviewed on a periodic basis; explicit re-approval is required or access to the resource is automatically revoked. Controls specific to User Access reviews are outlined in the SOC reports. Exceptions in the User entitlement controls are documented in the SOC reports. Refer to ISO 27001 standards, Annex A, domain 9 for additional details.

Control Group	CID	Consensus Assessment Questions	AWS Response
	IAM-10.2	If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?	AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	IAM-10.3	Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?	
Identity & Access Management <i>User Access Revocation</i>	IAM-11.1	Is timely deprovisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or involved third parties?	Access is automatically revoked when an employee's record is terminated in Amazon's Human Resources system. When changes in an employee's job function occur, continued access must be explicitly approved to the resource or it will be automatically revoked. AWS SOC reports provides further details on User access revocation. In addition the AWS Security White paper, section "Employee Lifecycle" provides additional information. Refer to ISO 27001 Annex A, domain 9 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	IAM-11.2	Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	
Identity & Access Management <i>User ID Credentials</i>	IAM-12.1	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	The AWS Identity and Access Management (IAM) service provides identity federation to the AWS Management Console. Multi-factor authentication is an optional feature that a customer can utilize. Refer to the AWS website for additional details - http://aws.amazon.com/mfa . AWS Identity and Access Management (IAM) supports identity federation for delegated access to the AWS Management Console or AWS APIs. With identity federation, external identities (federated users) are granted secure access to resources in your AWS account without having to create IAM users. These external identities can come from your corporate identity provider (such as Microsoft Active Directory or from the AWS Directory Service) or from a web identity provider, such as Amazon Cognito, Login with Amazon, Facebook, Google or any OpenID Connect (OIDC) compatible provider.
	IAM-12.2	Do you use open standards to delegate authentication capabilities to your tenants?	
	IAM-12.3	Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	
	IAM-12.4	Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?	
	IAM-12.5	Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	IAM -12.6	Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometrics, etc.) for user access?	AWS Identity and Access Management (IAM) enables customers to securely control access to AWS services and resources for their users. Additional information about IAM can be found on website at https://aws.amazon.com/iam/ . AWS SOC reports provides details on the specific control activities executed by AWS.
	IAM -12.7	Do you allow tenants to use third-party identity assurance services?	
	IAM -12.8	Do you support password (minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) policy enforcement?	
	IAM -12.9	Do you allow tenants/customers to define password and account lockout policies for their accounts?	
	IAM -12.10	Do you support the ability to force password changes upon first logon?	
	IAM -12.11	Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	
Identity & Access Management <i>Utility Programs Access</i>	IAM -13.1	Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored?	In alignment with ISO 27001 standards, system utilities are appropriately restricted and monitored. AWS SOC reports provides details on the specific control activities executed by AWS. Refer to AWS Overview of Security Processes for additional details - available at http://aws.amazon.com/security .
	IAM -13.2	Do you have a capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)?	
	IAM -13.3	Are attacks that target the virtual infrastructure prevented with technical controls?	

Control Group	CID	Consensus Assessment Questions	AWS Response
Infrastructure & Virtualization Security <i>Audit Logging / Intrusion Detection</i>	IVS-01.1	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents?	AWS Incident response program (detection, investigation and response to incidents) have been developed in alignment with ISO 27001 standards, system utilities are appropriately restricted and monitored. AWS SOC reports provides additional details on controls in place to restrict system access. Refer to AWS Overview of Security Processes for additional details - available at http://aws.amazon.com/security .
	IVS-01.2	Is physical and logical user access to audit logs restricted to authorized personnel?	
	IVS-01.3	Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?	
	IVS-01.4	Are audit logs centrally stored and retained?	In alignment with ISO 27001 standards, AWS information systems utilize internal system clocks synchronized via NTP (Network Time Protocol). AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	IVS-01.5	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	AWS utilizes automated monitoring systems to provide a high level of service performance and availability. Proactive monitoring is available through a variety of online tools both for internal and external use. Systems within AWS are extensively instrumented to monitor key operational metrics. Alarms are configured to notify operations and management personnel when early warning thresholds are crossed on key operational metrics. An on-call schedule is used such that personnel are always available to respond to operational issues. This includes a pager system so alarms are quickly and reliably communicated to operations personnel. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security .
Infrastructure & Virtualization Security <i>Change Detection</i>	IVS-02.1	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g. dormant, off or running)?	Virtual Machines are assigned to customers as a part of the EC2 service. Customers retain control over what resources are being used and where resources reside. Refer to the AWS website for additional details - http://aws.amazon.com .
	IVS-02.2	Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g. portals or alerts)?	

Control Group	CID	Consensus Assessment Questions	AWS Response
Infrastructure & Virtualization Security <i>Clock Synchronization</i>	IVS-03.1	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	In alignment with ISO 27001 standards, AWS information systems utilize internal system clocks synchronized via NTP (Network Time Protocol). AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	IVS-04.1	Do you provide documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?	Details regarding AWS Service Limits and how to request an increase for specific services is available on the AWS website at http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html . AWS manages capacity and utilization data in alignment with ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	IVS-04.2	Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	
	IVS-04.3	Do your system capacity requirements take into account current, projected and anticipated capacity needs for all systems used to provide services to the tenants?	
	IVS-04.4	Is system performance monitored and tuned in order to continuously meet regulatory, contractual and business requirements for all the systems used to provide services to the tenants?	
Infrastructure & Virtualization Security <i>Management - Vulnerability Management</i>	IVS-05.1	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g. virtualization aware)?	Amazon EC2 currently utilizes a highly customized version of the Xen hypervisor. The hypervisor is regularly assessed for new and existing vulnerabilities and attack vectors by internal and external penetration teams, and is well suited for maintaining strong isolation between guest virtual machines. The AWS Xen hypervisor security is regularly evaluated by independent auditors during assessments and audits. Regular internal and external vulnerability scans are performed on the host operating system, web application and databases in the AWS environment utilizing a variety of tools. Vulnerability scanning and remediation practices are regularly reviewed as a part of AWS continued compliance with PCI DSS and FedRAMP.
Infrastructure & Virtualization Security <i>Network Security</i>	IVS-06.1	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?	AWS website provides guidance on creating a layered security architecture in a number of white papers available via the AWS public website - http://aws.amazon.com/documentation/ .
	IVS-06.2	Do you regularly update network architecture diagrams that include data flows between security domains/zones?	Boundary protection devices that employ rule sets, access control lists (ACL), and configurations enforce the flow of information between network fabrics. Several network fabrics exist at Amazon, each separated by devices that

Control Group	CID	Consensus Assessment Questions	AWS Response
	IVS-06.3	Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	control the flow of information between fabrics. The flow of information between fabrics is established by approved authorizations, which exist as access control lists (ACL) which reside on these devices. These devices control the flow of information between fabrics as mandated by these ACLs. ACLs are defined, approved by appropriate personnel, managed and deployed using AWS ACL-manage tool.
	IVS-06.4	Are all firewall access control lists documented with business justification?	Amazon's Information Security team approves these ACLs. Approved firewall rule sets and access control lists between network fabrics restrict the flow of information to specific information system services. Access control lists and rule sets are reviewed and approved, and are automatically pushed to boundary protection devices on a periodic basis (at least every 24 hours) to ensure rule-sets and access control lists are up-to-date.
Infrastructure & Virtualization Security <i>OS Hardening and Base Controls</i>	IVS-07.1	Are operating systems hardened to provide only the necessary ports, protocols and services to meet business needs using technical controls (i.e antivirus, file integrity monitoring and logging) as part of their baseline build standard or template?	AWS Network Management is regularly reviewed by independent third-party auditors as a part of AWS ongoing compliance with SOC, PCI DSS, ISO 27001 and FedRAMPsm. AWS implements least privilege throughout its infrastructure components. AWS prohibits all ports and protocols that do not have a specific business purpose. AWS follows a rigorous approach to minimal implementation of only those features and functions that are essential to use of the device. Network scanning is performed and any unnecessary ports or protocols in use are corrected. Regular internal and external vulnerability scans are performed on the host operating system, web application and databases in the AWS environment utilizing a variety of tools. Vulnerability scanning and remediation practices are regularly reviewed as a part of AWS continued compliance with PCI DSS and FedRAMP.
	IVS-08.1	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	AWS Customers retain the ability and the responsibility to create and maintain production and test environments. AWS website provides guidance on creating an environment utilizing the AWS services - http://aws.amazon.com/documentation/ .
Infrastructure & Virtualization Security <i>Production / Nonproduction Environments</i>	IVS-08.2	For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	
	IVS-08.3	Do you logically and physically segregate production and non-production environments?	AWS Customers retain responsibility to manage their own network segmentation in adherence with their defined requirements. Internally, AWS network segmentation is aligned with ISO 27001 standards. Refer to ISO 27001 standard, Annex A. domain 13 for further detail. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Infrastructure & Virtualization Security <i>Segmentation</i>	IVS-09.1	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	
	IVS-09.2	Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legislative, regulatory and contractual requirements?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	IVS-09.3	Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?	
	IVS-09.4	Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	
Infrastructure & Virtualization Security <i>VM Security - vMotion Data Protection</i>	IVS-10.1	Are secured and encrypted communication channels used when migrating physical servers, applications or data to virtual servers?	AWS provides customers the ability to use their own encryption mechanism for nearly all services including S3, EBS and EC2. VPC sessions are also encrypted.
	IVS-10.2	Do you use a network segregated from production-level networks when migrating physical servers, applications or data to virtual servers?	AWS Customers retain control and ownership of their own data. AWS provides customers the ability to maintain and develop production and non-production environments. It is the responsibility of the customer to ensure that their production data is not replicated to non-production environments.
Infrastructure & Virtualization Security <i>VMM Security - Hypervisor Hardening</i>	IVS-11.1	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g. two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	AWS employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function. When user accounts are created, user accounts are created to have minimal access. Access above these least privileges requires appropriate authorization. Refer to AWS SOC reports for more information on Access Controls.
Infrastructure & Virtualization Security <i>Wireless Security</i>	IVS-12.1	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?	Policies, procedures and mechanisms to protect AWS network environment are in place. AWS security controls are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.
	IVS-12.2	Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings)	

Control Group	CID	Consensus Assessment Questions	AWS Response
	IVS-12.3	Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	
Infrastructure & Virtualization Security <i>Network Architecture</i>	IVS-13.1	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?	AWS Customers retain responsibility to manage their own network segmentation in adherence with their defined requirements. Internally, AWS network segmentation is aligned with the ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	IVS-13.2	Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?	AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. In addition, external vulnerability threat assessments are performed regularly by independent security firms. Findings and recommendations resulting from these assessments are categorized and delivered to AWS leadership. In addition, the AWS control environment is subject to regular internal and external risk assessments. AWS engages with external certifying bodies and independent auditors to review and test the AWS overall control environment. AWS security controls are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.
Interoperability & Portability APIs	IPY-01	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	Details regarding AWS APIs can be found on the AWS website at https://aws.amazon.com/documentation/. In alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources. AWS SOC reports outlines the controls in place to manage access provisioning to AWS resources.
Interoperability & Portability Data Request	IPY-02	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
Interoperability & Portability Policy & Legal	IPY-03.1	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	
	IPY-03.2	Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?	Customer retain control and ownership of their content. Customers can choose how they migrate applications and content both on and off the AWS platform at their discretion.

Control Group	CID	Consensus Assessment Questions	AWS Response
Interoperability & Portability <i>Standardized Network Protocols</i>	IPY-04.1	Can data import, data export and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	AWS allows customers to move data as needed on and off AWS storage. Refer to http://aws.amazon.com/choosing-a-cloud-platform for more information on Storage options.
	IPY-04.2	Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	
Interoperability & Portability <i>Virtualization</i>	IPY-05.1	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?	Amazon EC2 currently utilizes a highly customized version of the Xen hypervisor. The hypervisor is regularly assessed for new and existing vulnerabilities and attack vectors by internal and external penetration teams, and is well suited for maintaining strong isolation between guest virtual machines. The AWS Xen hypervisor security is regularly evaluated by independent auditors during assessments and audits. Refer to the AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security .
	IPY-05.2	Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?	
Mobile Security <i>Anti-Malware</i>	MOS-01	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?	AWS' program, processes and procedures to managing antivirus / malicious software is in alignment with ISO 27001 standards. Refer to ISO 27001 standard, Annex A, domain 12 for additional information.
Mobile Security <i>Application Stores</i>	MOS-02	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?	AWS has established an information security framework and policies and has effectively integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, the PCI DSS v3.1 and the National Institute of Standards and Technology (NIST) Publication 800-53 (Recommended Security Controls for Federal Information Systems). Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to manage mobile security devices and the access to the customer's content.
Mobile Security <i>Approved Applications</i>	MOS-03	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores be loaded onto a mobile device?	
Mobile Security <i>Approved Software for BYOD</i>	MOS-04	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?	

Control Group	CID	Consensus Assessment Questions	AWS Response
Mobile Security <i>Awareness and Training</i>	MOS-05	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?	
Mobile Security <i>Cloud Based Services</i>	MOS-06	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?	
Mobile Security <i>Compatibility</i>	MOS-07	Do you have a documented application validation process for testing device, operating system and application compatibility issues?	
Mobile Security <i>Device Eligibility</i>	MOS-08	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?	
Mobile Security <i>Device Inventory</i>	MOS-09	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (os system and patch levels, lost or decommissioned, device assignee)?	
Mobile Security <i>Device Management</i>	MOS-10	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?	
Mobile Security <i>Encryption</i>	MOS-11	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?	
Mobile Security <i>Jailbreaking and Rooting</i>	MOS-12.1	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	MOS -12.2	Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?	
Mobile Security <i>Legal</i>	MOS -13.1	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery and legal holds?	Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to manage mobile security devices and the access to the customer's content.
	MOS -13.2	Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?	
Mobile Security <i>Lockout Screen</i>	MOS -14	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?	
Mobile Security <i>Operating Systems</i>	MOS -15	Do you manage all changes to mobile device operating systems, patch levels and applications via your company's change management processes?	
Mobile Security <i>Passwords</i>	MOS -16.1	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?	
	MOS -16.2	Are your password policies enforced through technical controls (i.e. MDM)?	
	MOS -16.3	Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?	
Mobile Security <i>Policy</i>	MOS -17.1	Do you have a policy that requires BYOD users to perform backups of specified corporate data?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	MOS -17.2	Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?	
	MOS -17.3	Do you have a policy that requires BYOD users to use anti-malware software (where supported)?	
Mobile Security <i>Remote Wipe</i>	MOS -18.1	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?	
	MOS -18.2	Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?	
Mobile Security <i>Security Patches</i>	MOS -19.1	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?	
	MOS -19.2	Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?	
Mobile Security <i>Users</i>	MOS -20.1	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?	AWS maintains contacts with industry bodies, risk and compliance organizations, local authorities and regulatory bodies as required by the ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	MOS -20.2	Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?	
Security Incident Management, E-Discovery & Cloud Forensics <i>Contact / Authority Maintenance</i>	SEF-01.1	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	
	SEF-02.1	Do you have a documented security incident response plan?	
Security Incident Management, E-Discovery & Cloud Forensics <i>Incident Management</i>	SEF-02.2	Do you integrate customized tenant requirements into your security incident response plans?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	SEF-02.3	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	The AWS Cloud Security Whitepaper (available at http://aws.amazon.com/security) provides additional details.
	SEF-02.4	Have you tested your security incident response plans in the last year?	
Security Incident Management, E-Discovery & Cloud Forensics <i>Incident Reporting</i>	SEF-03.1	Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?	
	SEF-03.2	Does your logging and monitoring framework allow isolation of an incident to specific tenants?	
Security Incident Management, E-Discovery & Cloud Forensics <i>Incident Response Legal Preparation</i>	SEF-04.1	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	
	SEF-04.2	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	
	SEF-04.3	Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	
	SEF-04.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	
Security Incident Management, E-Discovery & Cloud Forensics <i>Incident Response Metrics</i>	SEF-05.1	Do you monitor and quantify the types, volumes and impacts on all information security incidents?	
	SEF-05.2	Will you share statistical information for security incident data with your tenants upon request?	

Control Group	CID	Consensus Assessment Questions	AWS Response
Supply Chain Management, Transparency and Accountability <i>Data Quality and Integrity</i>	STA-01.1	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	Customers retain control and ownership over the quality of their data and potential quality errors that may arise through their usage of AWS services. Refer to AWS SOC report for specific details in relation to Data Integrity and Access Management (including least privilege access)
	STA-01.2	Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	
Supply Chain Management, Transparency and Accountability <i>Incident Reporting</i>	STA-02.1	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals)?	AWS' incident response program, plans and procedures have been developed in alignment with ISO 27001 standard. The AWS SOC reports provides details on the specific control activities executed by AWS. The AWS Cloud Security Whitepaper (available at http://aws.amazon.com/security) provides additional details.
Supply Chain Management, Transparency and Accountability <i>Network / Infrastructure Services</i>	STA-03.1	Do you collect capacity and use data for all relevant components of your cloud service offering?	AWS manages capacity and utilization data in alignment with ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	STA-03.2	Do you provide tenants with capacity planning and use reports?	
Supply Chain Management, Transparency and Accountability <i>Provider Internal Assessments</i>	STA-04.1	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	AWS procurement and supply chain team maintain relationships with all AWS suppliers. Refer to ISO 27001 standards; Annex A, domain 8 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Supply Chain Management, Transparency and Accountability <i>Third Party Agreements</i>	STA-05.1	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored and transmitted?	Personnel security requirements for third-party providers supporting AWS systems and devices are established in a Mutual Non-Disclosure Agreement between AWS' parent organization, Amazon.com, and the respective third-party provider. The Amazon Legal Counsel and the AWS Procurement team define AWS third party provider personnel security requirements in contract agreements with the third party provider. All persons working with AWS information must at a minimum, meet the screening process for pre-employment background checks and sign a Non-Disclosure Agreement (NDA) prior to being granted access to AWS information. AWS does not generally outsource development of AWS services to subcontractors.
	STA-05.2	Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?	
	STA-05.3	Does legal counsel review all third-party agreements?	
	STA-05.4	Do third-party agreements include provision for the security and protection of information and assets?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	STA-05.5	Do you provide the client with a list and copies of all sub processing agreements and keep this updated?	
Supply Chain Management, Transparency and Accountability <i>Supply Chain Governance Reviews</i>	STA-06.1	Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?	AWS maintains formal agreements with key third party suppliers and implements appropriate relationship management mechanisms in line with their relationship to the business. AWS' third party management processes are reviewed by independent auditors as part of AWS ongoing compliance with SOC and ISO 27001.
Supply Chain Management, Transparency and Accountability <i>Supply Chain Metrics</i>	STA-07.1	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	
	STA-07.2	Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?	
	STA-07.3	Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	
	STA-07.4	Do you review all agreements, policies and processes at least annually?	
Supply Chain Management, Transparency and Accountability <i>Third Party Assessment</i>	STA-08.1	Do you assure reasonable information security across your information supply chain by performing an annual review?	
	STA-8.2	Does your annual review include all partners/third-party providers upon which your information supply chain depends?	
Supply Chain Management, Transparency	STA-09.1	Do you permit tenants to perform independent vulnerability assessments?	

Control Group	CID	Consensus Assessment Questions	AWS Response
and Accountability <i>Third Party Audits</i>	STA-09.2	Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	these types of scans can be initiated by submitting a request via the AWS Vulnerability / Penetration Testing Request Form . AWS Security regularly engages independent security firms to perform external vulnerability threat assessments. The AWS SOC reports provides additional details on the specific control activities executed by AWS.
Threat and Vulnerability Management <i>Antivirus / Malicious Software</i>	TVM-01.1	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?	AWS' program, processes and procedures to managing antivirus / malicious software is in alignment with ISO 27001 standards. Refer to AWS SOC reports provides further details. In addition, refer to ISO 27001 standard, Annex A, domain 12 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	TVM-01.2	Do you ensure that security threat detection systems using signatures, lists or behavioral patterns are updated across all infrastructure components within industry accepted time frames?	
Threat and Vulnerability Management <i>Vulnerability / Patch Management</i>	TVM-02.1	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	Customers retain control of their own guest operating systems, software and applications and are responsible for performing vulnerability scans and patching of their own systems. Customers can request permission to conduct scans of their cloud infrastructure as long as they are limited to the customer's instances and do not violate the AWS Acceptable Use Policy. AWS Security regularly scans all Internet-facing service endpoint IP addresses for vulnerabilities. AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. AWS' own maintenance and system patching generally do not impact customers. Refer to AWS Cloud Security Whitepaper for further information - available at http://aws.amazon.com/security . Refer to ISO 27001 standard, Annex A, domain 12 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	TVM-02.2	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	
	TVM-02.3	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	
	TVM-02.4	Will you make the results of vulnerability scans available to tenants at their request?	
	TVM-02.5	Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications and systems?	
	TVM-02.6	Will you provide your risk-based systems patching time frames to your tenants upon request?	
Threat and Vulnerability Management <i>Mobile Code</i>	TVM-03.1	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?	AWS allows customers to manage client and mobile applications to their own requirements.

Control Group	CID	Consensus Assessment Questions	AWS Response
	TVM - 03.2	Is all unauthorized mobile code prevented from executing?	

Appendix B: AWS alignment with the Australian Signals Directorate (ASD) Cloud Computing Security Considerations

The Cloud Computing Security Considerations was created to assist agencies in performing a risk assessment of services offered by Cloud Service Providers. The following provides AWS alignment to the Security Considerations, published on September 2012. For additional details refer to:

http://www.asd.gov.au/publications/csocprotect/Cloud_Computing_Security_Considerations.pdf

Key Area	Questions	AWS RESPONSE
Maintaining Availability and Business Functionality	a. Business criticality of data or functionality. Am I moving business critical data or functionality to the cloud?	AWS customers retain control and ownership of their content. Customers are responsible for the classification and use of their content.
	b. Vendor's business continuity and disaster recovery plan. Can I thoroughly review a copy of the vendor's business continuity and disaster recovery plan that covers the availability and restoration of both my data and the vendor's services that I use? How much time does it take for my data and the services that I use to be recovered after a disaster, and do the vendor's other customers that are larger and pay more money than me get prioritization?	AWS customers retain control and ownership of their data. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. In case of failure, automated processes move customer data traffic away from the affected area. AWS SOC 1 Type 2 report provides further details. ISO 27001 standard Annex A, domain 11. 2 provides additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification. Customers utilize AWS to enable faster disaster recovery of their critical IT systems without incurring the infrastructure expense of a second physical site. The AWS cloud supports many popular disaster recovery (DR) architectures from "pilot light" environments that are ready to scale up at a moment's notice to "hot standby" environments that enable rapid failover. To learn more about Disaster Recovery on AWS visit https://aws.amazon.com/disaster-recovery/. AWS provides customers with the capability to implement a robust continuity plan, including the utilization of frequent server instance back-ups, data redundancy replication, and multi-region/availability zone deployment architectures. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. In case of failure, automated processes move customer data traffic away from the affected area. AWS data centers incorporate physical protection against environmental risks. AWS' physical protection against environmental risks has been validated by an independent auditor and has been certified as being in alignment with ISO 27002 best practices. Refer to ISO 27001 standard, Annex A domain 9.1 and the AWS SOC 1 Type II report for additional information.

Key Area	Questions	AWS RESPONSE
	c. My data backup plan. Will I spend additional money to maintain an up to date backup copy of my data located either at my agency's premises, or stored with a second vendor that has no common points of failure with the first vendor?	AWS customers retain control and ownership of their content and it is the customer's responsibility to manage their data backup plans. AWS allows customers to move data as needed on and off AWS storage. AWS Import/Export service for S3 accelerates moving large amounts of data into and out of AWS using portable storage devices for transport. AWS allows customers to perform their own backups to tapes using their own tape backup service provider. However, a tape backup is not a service provided by AWS. Amazon S3 service is designed to drive the likelihood of data loss to near zero percent and the durability equivalent of multi-site copies of data objects is achieved through data storage redundancy. For information on data durability and redundancy, please refer to the AWS website. AWS offers a range of cloud computing services to support Disaster Recovery. To learn more about Disaster Recovery on AWS visit https://aws.amazon.com/disaster-recovery/.
	d. My business continuity and disaster recovery plan. Will I spend additional money to replicate my data or business functionality with a second vendor that uses a different data center and ideally has no common points of failure with the first vendor? This replication should preferably be configured to automatically "failover", so that if one vendor's services become unavailable, control is automatically and smoothly transitioned to the other vendor.	Customers retain control and ownership of their data. Customers can export their AMIs and use them on premise or at another provider (subject to software licensing restrictions). Refer to the AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security. AWS allows customers to move data as needed on and off AWS storage. AWS Import/Export service for S3 accelerates moving large amounts of data into and out of AWS using portable storage devices for transport. AWS allows customers to perform their own backups to tapes using their own tape backup service provider. However, a tape backup is not a service provided by AWS. AWS data centers are built in clusters in various global regions. All data centers are online and serving customers; no data center is "cold." In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. This means that Availability Zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by Region). In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, they are each fed via different grids from independent utilities to further reduce single points of failure. Availability Zones are all redundantly connected to multiple tier-1 transit providers. Customers should architect their AWS usage to take advantage of multiple Regions and Availability Zones. Distributing applications across multiple Availability Zones provides the ability to remain resilient in the face of most failure modes including natural disasters or system failures. AWS SOC 1 Type 2 report provides further details. ISO 27001 standard Annex A, domain 11. 2 provides additional details. AWS has been validated

Key Area	Questions	AWS RESPONSE
		and certified by an independent auditor to confirm alignment with ISO 27001 certification.
	e. My network connectivity to the cloud. Is the network connectivity between my agency's users and the vendor's network adequate in terms of availability, traffic throughput (bandwidth), delays (latency) and packet loss?	Customers can also choose their network path to AWS facilities, including multiple VPN endpoints in each AWS Region. In addition, AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your data center, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.

Key Area	Questions	AWS RESPONSE
	f. Vendor's guarantee of availability. Does the Service Level Agreement (SLA guarantee that the vendor will provide adequate system availability and quality of service, using their robust system architecture and business processes?	AWS does commit to high levels of availability in its service level agreements (SLAs). For example, Amazon EC2 commits to annual uptime percentage of at least 99.95% during the service year. Amazon S3 commits to monthly uptime percentage of at least 99.99% Service credits are provided in the case these availability metrics are not met. Customers should architect their AWS usage to take advantage of multiple Regions and Availability Zones. Distributing applications across multiple Availability Zones provides the ability to remain resilient in the face of most failure modes including natural disasters or system failures. AWS utilizes automated monitoring systems to provide a high level of service performance and availability. Proactive monitoring is available through a variety of online tools both for internal and external use. Systems within AWS are extensively instrumented to monitor key operational metrics. Alarms are configured to notify operations and management personnel when early warning thresholds are crossed on key operational metrics. An on-call schedule is used such that personnel are always available to respond to operational issues. This includes a pager system so alarms are quickly and reliably communicated to operations personnel. AWS Network Management is regularly reviewed by independent third-party auditors as a part of AWS ongoing compliance with SOC, PCI DSS, ISO 27001 and FedRAMPsm.
	g. Impact of outages. Can I tolerate the maximum possible downtime of the SLA? Are the scheduled outage windows acceptable both in duration and time of day, or will scheduled outages interfere with my critical business processes?	AWS does not require systems to be brought offline to perform regular maintenance and system patching. AWS' own maintenance and system patching generally do not impact customers. Maintenance of instances themselves is controlled by the customer.
	h. SLA inclusion of scheduled outages. Does the SLA guaranteed availability percentage include scheduled outages?	AWS does not operate an environment with scheduled outage as AWS provides customers the ability to architect their environment to take advantage of multiple Availability Zones and regions.
	i. SLA compensation. Does the SLA adequately reflect the actual damage caused by a breach of the SLA such as unscheduled downtime or data loss?	AWS provides customer remuneration for losses they may incur due to outages in alignment with AWS' Service Level Agreement.

Key Area	Questions	AWS RESPONSE
	j. Data integrity and availability. How does the vendor implement mechanisms such as redundancy and offsite backups to prevent corruption or loss of my data, and guarantee both the integrity and the availability of my data?	AWS data integrity controls as described in AWS SOC 1 Type II report provides reasonable assurance that data integrity is maintained through all phases including transmission, storage and processing. In addition, refer to ISO 27001 standard, Annex A, domain 12.2 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. Data centers are built in clusters in various global regions. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Customers should architect their AWS usage to take advantage of multiple Regions and Availability Zones. You choose where to store your data by specifying a region (for Amazon S3) or an availability zone within a region (for EBS). Data stored in Amazon Elastic Block Store (Amazon EBS) is redundantly stored in multiple physical locations as part of normal operation of those services and at no additional charge. However, Amazon EBS replication is stored within the same availability zone, not across multiple zones. Amazon S3 provides a highly durable storage infrastructure. Objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 Region. Once stored, Amazon S3 maintains the durability of objects by quickly detecting and repairing any lost redundancy. Amazon S3 also regularly verifies the integrity of data stored using checksums. If corruption is detected, it is repaired using redundant data. Data stored in S3 is designed to provide 99.99999999% durability and 99.99% availability of objects over a given year. Refer to AWS Overview of Security Processes whitepaper for additional details - available at http://aws.amazon.com/security
	k. Data restoration. If I accidentally delete a file, email or other data, how much time does it take for my data to be partially or fully restored from backup, and is the maximum acceptable time captured in the SLA?	AWS customers retain control and ownership of their data. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region.
	l. Scalability. How much available spare computing resources does the vendor provide to enable my usage of the vendor's services to scale at short notice?	The AWS cloud is distributed, highly secure and resilient, giving customers large scaling potential. Customers may scale up or down, paying for only what they use.

Key Area	Questions	AWS RESPONSE
	m. Changing vendor. If I want to move my data to my agency or to a different vendor, or if the vendor suddenly becomes bankrupt or otherwise quits the cloud business, how do I get access to my data in a vendor-neutral format to avoid vendor lock-in? How cooperative will the vendor be? How do I ensure that my data is permanently deleted from the vendor's storage media? For Platform as a Service, which standards does the vendor use that facilitate portability and interoperability to easily move my application to a different vendor or to my agency?	Customers retain control and ownership of their data. Customers can export their AMIs and use them on premise or at another provider (subject to software licensing restrictions). Refer to the AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security. AWS allows customers to move data as needed on and off AWS storage. AWS Import/Export service for S3 accelerates moving large amounts of data into and out of AWS using portable storage devices for transport. AWS allows customers to perform their own backups to tapes using their own tape backup service provider. However, a tape backup is not a service provided by AWS.
Protecting Data from Unauthorized Access by a Third Party	a. Choice of cloud deployment model. Am I considering using a potentially less secure public cloud, a potentially more secure hybrid cloud or community cloud, or a potentially most secure private cloud?	AWS' Compliance and Security teams have established an information security framework and policies based on the Control Objectives for Information and related Technology (COBIT) framework. The AWS security framework integrates the ISO 27002 best practices and the PCI Data Security Standard. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security. AWS provides third-party attestations, certifications, Service Organization Controls 1 (SOC 1) Type II report and other relevant compliance reports directly to our customers under NDA. Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the Amazon Web Services (AWS) Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can easily customize the network configuration for your Amazon VPC. For example, you can create a public-facing subnet for your web servers that has access to the Internet, and place your backend systems such as databases or application servers in a private-facing subnet with no Internet access. You can leverage multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet. Additionally, you can create a Hardware Virtual Private Network (VPN) connection between your corporate data center and your VPC and leverage the AWS cloud as an extension of your corporate data center

Key Area	Questions	AWS RESPONSE
	b. Sensitivity of my data. Is my data to be stored or processed in the cloud classified, sensitive, private, or data that is publicly available such as information from my public web site? Does the aggregation of my data make it more sensitive than any individual piece of data? For example, the sensitivity may increase if storing a significant amount of data, or storing a variety of data that if compromised would facilitate identity theft. If there is a data compromise, could I demonstrate my due diligence to senior management, government officials and the public?	AWS customers retain control and ownership of their data and may implement a structured data-classification program to meet their requirements.
	c. Legislative obligations. What obligations do I have to protect and manage my data under various legislation, for example the Privacy Act, the Archives Act, as well as other legislation specific to the type of data? Will the vendor contractually accept adhering to these obligations to help me ensure that the obligations are met to the satisfaction of the Australian Government?	AWS customers retain responsibility to ensure their usage of AWS is within compliance of applicable laws and regulations. AWS communicates its security and control environment to customers through industry certifications and third-party attestations, white papers (available at http://aws.amazon.com/security) and providing certifications, reports and other relevant documentation directly to AWS customers. AWS has published a whitepaper on using AWS in the context of Australian privacy considerations, available here.

Key Area	Questions	AWS RESPONSE
	d. Countries with access to my data. In which countries is my data stored, backed up and processed? Which foreign countries does my data transit? In which countries is the failover or redundant data centers? Will the vendor notify me if the answers to these questions change?	AWS customers choose the AWS Region or regions in which their content and servers will be located. This allows customers with geographic specific requirements to establish environments in a location of their choice. AWS customers in Australia can choose to deploy their AWS services exclusively in the Asia Pacific (Sydney) region and store their content onshore in Australia. If the customer makes this choice, their content will be located in Australia unless the customer chooses to move the data. Customers can replicate and back up content in more than one region, but AWS does not move or replicate customer content outside of the customer's chosen region or regions. AWS is vigilant about customers' security and does not disclose or move data in response to a request from the Australian, U.S. or other government unless legally required to do so in order to comply with a legally valid and binding order, such as a subpoena or a court order, or as is otherwise required by applicable law. Non-U.S. governmental or regulatory bodies typically must use recognized international processes, such as Mutual Legal Assistance Treaties with the U.S. government, to obtain valid and binding orders. Additionally, our practice is to notify customers where practicable before disclosing their content so they can seek protection from disclosure, unless we are legally prevented from doing so.

Key Area	Questions	AWS RESPONSE
	e. Data encryption technologies. Are hash algorithms, encryption algorithms and key lengths deemed appropriate by the DSD ISM used to protect my data when it is in transit over a network, and stored on both the vendor's computers and on backup media? The ability to encrypt data while it is being processed by the vendor's computers is still an emerging technology and is an area of current research by industry and academia. Is the encryption deemed strong enough to protect my data for the duration of time that my data is sensitive?	AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS, SimpleDB and EC2. VPC sessions are also encrypted. Amazon S3 also offers Server Side Encryption as an option for customers. Customers may also use third-party encryption technologies. Internally, AWS establishes and manages cryptographic keys for required cryptography employed within the AWS infrastructure. AWS produces, controls and distributes symmetric cryptographic keys using NIST approved key management technology and processes in the AWS information system. An AWS developed secure key and credential manager is used to create, protect and distribute symmetric keys and is used to secure and distribute: AWS credentials needed on hosts, RSA public/private keys and X.509 Certifications. AWS cryptographic processes are reviewed by independent third-party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMPsm. The AWS CloudHSM service allows you to protect your encryption keys within HSMs designed and validated to government standards for secure key management. You can securely generate, store, and manage the cryptographic keys used for data encryption such that they are accessible only by you. AWS CloudHSM helps you comply with strict key management requirements without sacrificing application performance. The AWS CloudHSM service works with Amazon Virtual Private Cloud (VPC). CloudHSMs are provisioned inside your VPC with an IP address that you specify, providing simple and private network connectivity to your Amazon Elastic Compute Cloud (EC2) instances. Placing CloudHSMs near your EC2 instances decreases network latency, which can improve application performance. AWS provides dedicated and exclusive access to CloudHSMs, isolated from other AWS customers. Available in multiple Regions and Availability Zones (AZs), AWS CloudHSM allows you to add secure and durable key storage to your Amazon EC2 applications.
	f. Media sanitization. What processes are used to sanitize the storage media storing my data at its end of life, and are the processes deemed appropriate by the DSD ISM?	When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.

Key Area	Questions	AWS RESPONSE
	g. Vendor's remote monitoring and management. Does the vendor monitor, administer or manage the computers that store or process my data? If yes, is this performed remotely from foreign countries or from Australia? Can the vendor provide patch compliance reports and other details about the security of workstations used to perform this work, and what controls prevent the vendor's employees from using untrustworthy personally owned laptops?	Moving IT infrastructure to AWS services creates a model of shared responsibility between the customer and AWS. This shared model can help relieve customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall.
	h. My monitoring and management. Can I use my existing tools for integrity checking, compliance checking, security monitoring and network management, to obtain visibility of all my systems regardless of whether these systems are located locally or in the cloud? Do I have to learn to use additional tools provided by the vendor? Does the vendor even provide such a mechanism for me to perform monitoring?	AWS Cloudwatch provides monitoring for AWS cloud resources and the applications customers run on AWS. Refer to aws.amazon.com/cloudwatch for additional details. AWS also publishes our most up-to-the-minute information on service availability on the Service Health Dashboard. Refer to status.aws.amazon.com. The AWS Trusted Advisor inspects your AWS environment and makes recommendations when opportunities exist to save money, improve system performance and reliability, or help close security gap.
	i. Data ownership. Do I retain legal ownership of my data, or does it belong to the vendor and may be considered an asset for sale by liquidators if the vendor declares bankruptcy?	AWS customers retain ownership and control of their data. AWS only uses each customer's content to provide the AWS services selected by each customer to that customer and does not use customer content for any secondary purposes. AWS treats all customer content the same and has no insight as to what type of content the customer chooses to store in AWS. AWS simply makes available the compute, storage, database and networking services selected by customer – AWS does not require access to customer content to provide its services.

Key Area	Questions	AWS RESPONSE
	j. Gateway technologies. What technologies does the vendor use to create a secure gateway environment? Examples include firewalls, traffic flow filters, content filters, and antivirus software and data diodes where appropriate.	The AWS network provides significant protection against traditional network security issues and customers can implement further protection. Refer to the AWS Overview of Security whitepaper (available at http://aws.amazon.com/security) for additional details. Amazon assets (e.g. laptops) are configured with anti-virus software that includes e-mail filtering and malware detection. AWS Network Firewall management and Amazon's anti-virus program are reviewed by independent third-party auditors as a part of AWS ongoing compliance with SOC, PCI DSS, ISO 27001 and FedRAMPsm.
	k. Gateway certification. Is the vendor's gateway environment certified against government security standards and regulations?	AWS obtains certain industry certifications and independent third-party attestations which include the AWS Gateway environment.
	l. Email content filtering. For email Software as a Service, does the vendor provide customizable email content filtering that can enforce my agency's email content policy?	A Customer can utilize a system to host e-mail capabilities, however in that case it is the Customer's responsibility to employ the appropriate levels of spam and malware protection at e-mail entry and exit points and update spam and malware definitions when new releases are made available.

Key Area	Questions	AWS RESPONSE
	m. Policies and processes supporting the vendor's IT security posture. Can I have details of how the vendor's computer and network security posture is supported by policies and processes including threat and risk assessments, ongoing vulnerability management, a change management process that incorporates security, penetration testing, logging and regular log analysis, use of security products endorsed by the Australian Government, and compliance with Australian government security standards and regulations?	Policies and procedures have been established by AWS Information Security based upon the COBIT framework, ISO 27001 standards and the PCI DSS requirements. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. In addition AWS publishes a SOC 1 Type II report. Refer to the SOC 1 report for further details. The AWS Risk and Compliance whitepaper for additional details - available at http://aws.amazon.com/security. AWS customers are able to identify key controls managed by AWS. Key controls are critical to the customer's control environment and require an external attestation of the operating effectiveness of these key controls in order to comply with compliance requirements—such as the annual financial audit. For this purpose, AWS publishes a wide range of specific IT controls in its Service Organization Controls 1 (SOC 1) Type II report. The SOC 1 report, formerly the Statement on Auditing Standards (SAS) No. 70, Service Organizations report and formerly referred to as the Statement on Standards for Attestation Engagements No. 16 (SSAE 16) report, is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). The SOC 1 audit is an in-depth audit of both the design and operating effectiveness of AWS' defined control objectives and control activities (which include control objectives and control activities over the part of the infrastructure AWS manages). "Type II" refers to the fact that each of the controls described in the report are not only evaluated for adequacy of design, but are also tested for operating effectiveness by the external auditor. Because of the independence and competence of AWS' external auditor, controls identified in the report should provide customers with a high level of confidence in AWS' control environment.
	n. Technologies supporting the vendor's IT security posture. Can I have details of how the vendor's computer and network security posture is supported by direct technical controls including timely application of security patches, regularly updated antivirus software, defense in depth mechanisms to protect against unknown vulnerabilities, hardened operating systems and software applications configured with the strongest possible security settings, intrusion detection and prevention systems,	AWS provides third-party attestations, certifications, Service Organization Controls 1 (SOC 1) Type II report and other relevant compliance reports directly to our customers under NDA. AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. In addition, external vulnerability threat assessments are performed regularly by independent security firms. Findings and recommendations resulting from these assessments are categorized and delivered to AWS leadership. In addition, the AWS control environment is subject to regular internal and external risk assessments. AWS engages with external certifying bodies and independent auditors to review and test the AWS overall control environment.

Key Area	Questions	AWS RESPONSE
	and data loss prevention mechanisms?	
	o. Auditing the vendor's IT security posture. Can I audit the vendor' implementation of security measures, including performing scans and other penetration testing of the environment provided to me? If there is justifiable reason why auditing is not possible, which reputable third party has performed audits and other vulnerability assessments? What sort of internal audits does the vendor perform, and which compliance standards and other recommended practices from organization's such as the Cloud Security Alliance are used for these assessments? Can I thoroughly review a copy of recent resulting reports?	AWS provides third-party attestations, certifications, Service Organization Controls 1 (SOC 1) Type II report and other relevant compliance reports directly to our customers under NDA. Customers can request permission to conduct scans of their cloud infrastructure as long as they are limited to the customer's instances and do not violate the AWS Acceptable Use Policy. Advance approval for these types of scans can be initiated by submitting a request via the AWS Vulnerability / Penetration Testing Request Form. AWS Security regularly engages independent security firms to perform external vulnerability threat assessments. The AWS SOC 1 Type 2 report provides additional details on the specific control activities executed by AWS.

Key Area	Questions	AWS RESPONSE
	p. User authentication. What identity and access management systems does the vendor support for users to log in to use Software as a Service?	AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users. Using IAM, you can create and manage AWS users and groups and use permissions to allow and deny their access to AWS resources. AWS supports identity federation that makes it easier to manage users by maintaining their identities in a single place. AWS IAM includes support for the Security Assertion Markup Language (SAML) 2.0, an open standard used by many identity providers. This new feature enables federated single sign-on, or SSO, empowering users to log into the AWS Management Console or make programmatic calls to AWS APIs, by using assertions from a SAML-compliant identity provider, such as Shibboleth and Windows Active Directory Federation Services.
	q. Centralized control of data. What user training, policies and technical controls prevent my agency's users from using unapproved or insecure computing devices without a trusted operating environment to store or process sensitive data accessed using Software as a Service?	N/A

Key Area	Questions	AWS RESPONSE
	r. Vendor's physical security posture. Does the vendor use physical security products and devices that are endorsed by the Australian Government? How is the vendor's physical data center designed to prevent the tampering or theft of servers, infrastructure and the data stored thereon? Is the vendor's physical data center accredited by an authoritative third party?	The definition of AWS-defined logical and physical controls is documented in the SOC 1 Type II report, and the report is available for review by audit and compliance teams. AWS ISO 27001 and other certifications are also available for auditors to review. Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means. Physical access is strictly controlled both at the perimeter and at building ingress points and includes, but is not limited to, professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. Physical access points to server locations are recorded by closed circuit television camera (CCTV) as defined in the AWS Data Center Physical Security Policy. Images are retained for 90 days, unless limited to 30 days by legal or contractual obligations AWS provides data center physical access and information to approved employees and contractors who have a legitimate business need for such privileges. All visitors are required to present identification and are signed in and escorted by authorized staff. See the SOC 1 Type II report for specific controls related to physical access, data center access authorization, and other related controls. Refer to ISO 27001 standard, Annex A, domain 9.1 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	s. Software and hardware procurement. What procurement process is used to ensure that cloud infrastructure software and hardware has been supplied by a legitimate source and has not been maliciously modified in transit?	In alignment with ISO 27001 standards, AWS Hardware assets are assigned an owner, tracked and monitored by the AWS personnel with AWS proprietary inventory management tools. AWS procurement and supply chain team maintain relationships with all AWS suppliers. Refer to ISO 27001 standard, Annex A, domain 7.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.

Key Area	Questions	AWS RESPONSE
Protecting Data from Unauthorized Access by the Vendor's Customers	a. Customer segregation. What assurance do I have that the virtualization and "multi-tenancy" mechanisms guarantee adequate logical and network segregation between multiple tenants, so that a malicious customer using the same physical computer as me cannot access my data?	Amazon EC2 currently utilizes a highly customized version of the Xen hypervisor. The hypervisor is regularly assessed for new and existing vulnerabilities and attack vectors by internal and external penetration teams, and is well suited for maintaining strong isolation between guest virtual machines. The AWS Xen hypervisor security is regularly evaluated by independent auditors during assessments and audits. All data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. Customers retain control and ownership of their data, thus it is their responsibility to choose to encrypt the data. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. VPC sessions are also encrypted. Amazon S3 also offers Server Side Encryption as an option for customers. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security.
	b. Weakening my security posture. How would using the vendor's cloud infrastructure weaken my agency's existing network security posture? Would the vendor advertise me as one of their customers without my explicit consent, thereby assisting an adversary that is specifically targeting me?	AWS customers are considered confidential and would not advertise customer details without explicit consent. Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the Amazon Web Services (AWS) Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.
	c. Dedicated servers. Do I have some control over which physical computer runs my virtual machines? Can I pay extra to ensure that no other customer can use the same physical computer as me e.g. dedicated servers or virtual private cloud?	VPC allows customers to launch Amazon EC2 instances that are physically isolated at the host hardware level; they will run on single tenant hardware. A VPC can be created with 'dedicated' tenancy, in which case all instances launched into the VPC will utilize this feature. Alternatively, a VPC may be created with 'default' tenancy, but customers may specify 'dedicated' tenancy for particular instances launched into the VPC.
	d. Media sanitization. When I delete portions of my data, what processes are used to sanitize the storage media before it is made available to another customer, and are the processes deemed appropriate by the DSD ISM?	Customers retain ownership and control of their content and provide customers with the ability to delete their data. When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.

Key Area	Questions	AWS RESPONSE
Protecting Data from Unauthorized Access by Rogue Vendor Employees	a. Data encryption key management. Does the vendor know the password or key used to decrypt my data, or do I encrypt and decrypt the data on my computer so the vendor only ever has encrypted data?	AWS Customers manage their own encryption unless they are utilizing AWS server side encryption service. In this case, AWS does create a unique encryption key per tenant. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security .
	b. Vetting of vendor's employees. What personnel employment checks and vetting processes does the vendor perform to ensure that employees are trustworthy?	AWS conducts criminal background checks, as permitted by applicable law, as part of pre-employment screening practices for employees commensurate with the employee's position and level of access to AWS facilities.
	c. Auditing vendor's employees. What robust identity and access management system do the vendor's employees use? What auditing process is used to log and review the actions performed by the vendor's employees?	In alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources. AWS SOC 1 Type 2 report outlines the controls in place to manage access provisioning to AWS resources. Refer to AWS Overview of Security Processes whitepaper for additional details - available at http://aws.amazon.com/security .
	d. Visitors to data center. Are visitors to data centers escorted at all times, and is the name and other personal details of every visitor verified and recorded?	All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is routinely logged and audited.
	e. Physical tampering by vendor's employees. Is network cabling professionally installed to Australian standards or internationally acceptable standards, to help avoid the vendor's employees from accidentally connecting cables to the wrong computers, and to help readily highlight any deliberate attempts by the vendor's employees to tamper with the cabling?	Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means. This includes appropriate protection for network cables. The AWS SOC 1 Type 2 report provides additional details on the specific control activities executed by AWS. Refer to ISO 27001 standard, Annex A, domain 9.1 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.

Key Area	Questions	AWS RESPONSE
	f. Vendor's subcontractors. Do the answers to these questions apply equally to all of the vendor's subcontractors?	Provisioning contractor / vendor access is managed the same for both employees and contractors, with responsibility shared across Human Resources (HR), Corporate Operations and Service Owners. Vendors are subject to the same access requirements as employees.
Handling Security Incidents	a. Timely vendor support. Is the vendor readily contactable and responsive to requests for support, and is the maximum acceptable response time captured in the SLA or simply a marketing claim that the vendor will try their best? Is the support provided locally, or from a foreign country, or from several foreign countries using an approach that follows the sun? What mechanism does the vendor use to obtain a real-time understanding of the security posture of my use of the vendor's services so that the vendor can provide support?	AWS Support is a one-on-one, fast-response support channel that is staffed 24x7x365 with experienced and technical support engineers. The service helps customers of all sizes and technical abilities to successfully utilize the products and features provided by Amazon Web Services. All AWS Support tiers offer customers of AWS Infrastructure Services an unlimited number of support cases with pay-by-the-month pricing and no long-term contracts. The four tiers provide developers and businesses the flexibility to choose the support tiers that meet their specific needs.
	b. Vendor's incident response plan. Does the vendor have a security incident response plan that specifies how to detect and respond to security incidents, in a way that is similar to incident handling procedures detailed in the DSD ISM? Can I thoroughly review a copy?	The Amazon Incident Management team employs industry-standard diagnostic procedures to drive resolution during business-impacting events. Staff operators provide 24 x 7 x 365 coverage to detect incidents and to manage the impact and resolution. AWS' incident response program, plans and procedures have been developed in alignment with ISO 27001 standard. The AWS SOC 1 Type 2 report provides details on the specific control activities executed by AWS. The AWS Overview of Security Processes whitepaper (available at http://aws.amazon.com/security) provides additional details.
	c. Training of vendor's employees. What qualifications, certifications and regular information security awareness training do the vendor's employees require, to know how to use the vendor's systems in a secure manner and to identify potential security incidents?	In alignment with ISO 27001 standard, all AWS employees complete periodic Information Security training which requires an acknowledgement to complete. Compliance audits are periodically performed to validate that employees understand and follow the established policies. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security .

Key Area	Questions	AWS RESPONSE
	d. Notification of security incidents. Will the vendor notify me via secure communications of security incidents that are more serious than an agreed threshold, especially in cases where the vendor might be liable? Will the vendor automatically notify law enforcement or other authorities, who may confiscate computing equipment used to store or process my data?	Notification of security incidents are handled on a case-by-case basis and as required by applicable law. Any notification is performed via secure communications.
	e. Extent of vendor support. How much assistance will the vendor provide me with investigations if there is a security breach such as an unauthorized disclosure of my data, or if there is a need to perform legal electronic discovery of evidence?	AWS provides infrastructure and customers manage everything else, including the operating system, the network configuration and the installed applications. Customers are responsible for responding appropriately to legal procedures involving the identification, collection, processing, analysis and production of electronic documents they store or process using AWS. Upon request, AWS may work with customers who require AWS' assistance in legal proceedings.
	f. My access to logs. How do I obtain access to time synchronized audit logs and other logs to perform a forensic investigation, and how are the logs created and stored to be suitable evidence for a court of law?	Customers retain control of their own guest operating systems, software and applications and are responsible for developing logical monitoring of the conditions of these systems. In alignment with ISO 27001 standards, AWS information systems utilize internal system clocks synchronized via NTP (Network Time Protocol). AWS CloudTrail provides a simple solution to log user activity that helps alleviate the burden of running a complex logging system. Refer to aws.amazon.com/cloudtrail for additional details. AWS Cloudwatch provides monitoring for AWS cloud resources and the applications customers run on AWS. Refer to aws.amazon.com/cloudwatch for additional details. AWS also publishes our most up-to-the-minute information on service availability on the Service Health Dashboard. Refer to status.aws.amazon.com.
	g. Security incident compensation. How will the vendor adequately compensate me if the vendor's actions, faulty software or hardware contributed to a security breach?	AWS' incident response program, plans and procedures have been developed in alignment with ISO 27001 standard. The AWS SOC 1 Type 2 report provides details on the specific control activities executed by AWS. The AWS Overview of Security Processes whitepaper (available at http://aws.amazon.com/security) provides additional details.

Key Area	Questions	AWS RESPONSE
	h. Data spills. If data that I consider is too sensitive to be stored in the cloud is accidentally placed into the cloud, referred to as a data spill, how can the spilled data be deleted using forensic sanitization techniques? Is the relevant portion of physical storage media zeroed whenever data is deleted? If not, how long does it take for deleted data to be overwritten by customers as part of normal operation, noting that clouds typically have significant spare unused storage capacity? Can the spilled data be forensically deleted from the vendor's backup media? Where else is the spilled data stored, and can it be forensically deleted?	Customers retain ownership and control of their content. All data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. IPsec tunnels to VPC are also encrypted. Amazon S3 also offers Server Side Encryption as an option for customers. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security.

Appendix C: Glossary of Terms

Authentication: Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be.

Availability Zone: Amazon EC2 locations are composed of regions and Availability Zones. Availability Zones are distinct locations that are engineered to be insulated from failures in other Availability Zones and provide inexpensive, low latency network connectivity to other Availability Zones in the same region.

DSS: The Payment Card Industry Data Security Standard (DSS) is a worldwide information security standard assembled and managed by the Payment Card Industry Security Standards Council.

EBS: Amazon Elastic Block Store (EBS) provides block level storage volumes for use with Amazon EC2 instances. Amazon EBS volumes are off-instance storage that persists independently from the life of an instance.

FedRAMPsm: The Federal Risk and Authorization Management Program (FedRAMPsm) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMPsm is mandatory for Federal Agency cloud deployments and service models at the low and moderate risk impact levels.

FISMA: The Federal Information Security Management Act of 2002. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

FIPS 140-2: The Federal Information Processing Standard (FIPS) Publication 140-2 is a US government security standard that specifies the security requirements for cryptographic modules protecting sensitive information.

GLBA: The Gramm–Leach–Bliley Act (GLB or GLBA), also known as the Financial Services Modernization Act of 1999, sets forth requirements for financial institutions with regard to, among other things, the disclosure of nonpublic customer information and the protection of threats in security and data integrity.

HIPAA: The Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The Administration Simplification provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the U.S. health care system.

Hypervisor: A hypervisor, also called Virtual Machine Monitor (VMM), is software/hardware platform virtualization software that allows multiple operating systems to run on a host computer concurrently.

IAM: AWS Identity and Access Management (IAM) enables a customer to create multiple Users and manage the permissions for each of these Users within their AWS Account.

ITAR: International Traffic in Arms Regulations (ITAR) is a set of United States government regulations that control the export and import of defense-related articles and services on the United States Munitions List (USML). Government agencies and contractors must comply with ITAR and restrict access to protected data.

ISAE 3402: The International Standards for Assurance Engagements No. 3402 (ISAE 3402) is the international standard on assurance engagements. It was put forth by the International Auditing and Assurance Standards Board (IAASB), a standard-setting board within the International Federation of Accountants (IFAC). ISAE 3402 is now the new globally recognized standard for assurance reporting on service organizations.

ISO 9001: AWS' ISO 9001 certification directly supports customers who develop, migrate and operate their quality-controlled IT systems in the AWS cloud. Customers can leverage AWS' compliance reports as evidence for their own ISO 9001 programs and industry-specific quality programs, such as GxP in life sciences, ISO 13485 in medical devices, AS9100 in aerospace, and ISO/TS 16949 in automotive. AWS customers who don't have quality system requirements will still benefit from the additional assurance and transparency that an ISO 9001 certification provides.

ISO 27001: ISO/IEC 27001 is an Information Security Management System (ISMS) standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO 27001 formally specifies a management system that is intended to bring information security under explicit management control. Being a formal specification means that it mandates specific requirements. Organizations that claim to have adopted ISO/IEC 27001 can therefore be audited and certified compliant with the standard.

NIST: National Institute of Standards and Technology. This agency sets detailed security standards as needed by industry or government programs. Compliance with FISMA requires agencies to adhere to NIST standards.

Object: The fundamental entities stored in Amazon S3. Objects consist of object data and metadata. The data portion is opaque to Amazon S3. The metadata is a set of name-value pairs that describe the object. These include some default metadata such as the date last modified and standard HTTP metadata such as Content-Type. The developer can also specify custom metadata at the time the Object is stored.

PCI: Refers to the Payment Card Industry Security Standards Council, an independent council originally formed by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, with the goal of managing the ongoing evolution of the Payment Card Industry Data Security Standard.

QSA: The Payment Card Industry (PCI) Qualified Security Assessor (QSA) designation is conferred by the PCI Security Standards Council to those individuals that meet specific qualification requirements and are authorized to perform PCI compliance assessments.

SAS 70: Statement on Auditing Standards No. 70: Service Organizations is an auditing statement issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA). SAS 70 provides guidance to service auditors when assessing the internal controls of a service organization (such as AWS) and issuing a service auditor's report. SAS 70 also provides guidance to auditors of financial statements of an entity that uses one or more service organizations. The SAS 70 report has been replaced by the Service Organization Controls 1 report.

Service: Software or computing ability provided across a network (e.g., EC2, S3, VPC, etc.).

Service Level Agreement (SLA): A service level agreement is a part of a service contract where the level of service is formally defined. The SLA is used to refer to the contracted delivery time (of the service) or performance.

SOC 1: Service Organization Controls 1 (SOC 1) Type II report, formerly the Statement on Auditing Standards (SAS) No. 70, Service Organizations report (formerly referred to as the SSAE 16 report), is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). The



international standard is referenced as the International Standards for Assurance Engagements No. 3402 (ISAE 3402).

SSAE 16 [deprecated]: The Statement on Standards for Attestation Engagements No. 16 (SSAE 16) is an attestation standard published by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). The standard addresses engagements undertaken by a service auditor for reporting on controls at organizations that provide services to user entities, for which a service organization's controls are likely to be relevant to a user entities internal control over financial reporting (ICFR). SSAE 16 effectively replaces Statement on Auditing Standards No. 70 (SAS 70) for service auditor's reporting periods ending on or after June 15, 2011.

SOC 2: Service Organization Controls 2 (SOC 2) reports are intended to meet the needs of a broad range of users that need to understand internal control at a service organization as it relates to security, availability, processing integrity, confidentiality and privacy. These reports are performed using the AICPA Guide: Reporting on Controls at a Service Organizations Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy and are intended for use by stakeholders (e.g., customers, regulators, business partners, suppliers, directors) of the service organization that have a thorough understanding of the service organization and its internal controls.

SOC 3: Service Organization Controls 3 (SOC 3) reports are designed to meet the needs of users who want assurance on the controls at a service organization related to security, availability, processing integrity, confidentiality, or privacy but do not have the need for or the knowledge necessary to make effective use of a SOC 2 Report. These reports are prepared using the AICPA/Canadian Institute of Chartered Accountants (CICA) Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy. Because they are general use reports, SOC 3 Reports can be freely distributed or posted on a website as a seal.

Virtual Instance: Once an AMI has been launched, the resulting running system is referred to as an instance. All instances based on the same AMI start out identical and any information on them is lost when the instances are terminated or fail.

Version History

December 2015

- Updates to certifications and third-party attestations summaries
- Added ISO 27017 certification
- Added ISO 27018 certification
- Eleventh region added (China Beijing)

November 2015

- Update to CSA v3.0.1

August 2015

- Updates to in-scope services for PCI 3.1
- Updates to regions in-scope for PCI 3.1

May 2015

- Tenth region added (EU Frankfurt)
- Updates to in-scope services for SOC 3
- SSAE 16 language deprecated

Apr 2015

- Updates to in-scope services for: FedRAMPsm, HIPAA, SOC 1, ISO 27001, ISO 9001

Feb 2015

- Updates to FIPS 140-2 VPN endpoints and SSL-terminating load balancers
- Updates to PCI DSS verbiage

Dec 2014

- Updates to certifications and third-party attestations summaries

Nov 2013 version

- Edits to IPsec tunnel encryption verbiage

Jun 2013 version

- Updates to certifications and third-party attestations summaries
- Updates to Appendix C: Glossary of Terms
- Minor changes to formatting

Jan 2013 version

- Edits to certifications and third-party attestations summaries

Nov 2012 version

- Edits to content and updated certification scope
- Added reference to the SOC 2 and MPAA

Jul 2012 version

- Edits to content and updated certification scope
- Addition of the CSA Consensus Assessments Initiative Questionnaire (Appendix A)

Jan 2012 version

- Minor edits to content based on updated certification scope
- Minor grammatical edits

Dec 2011 version

- Change to Certifications and Third-party Attestation section to reflect SOC 1/SSAE 16, FISMA Moderate, International Traffic in Arms Regulations, and FIPS 140-2
- Addition of S3 Server Side Encryption
- Added additional cloud computing issue topics

May 2011 version

- Initial release

Notices

© 2010-2016 Amazon.com, Inc., or its affiliates. This document is provided for informational purposes only. It represents AWS' current product offerings as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS' products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Appendix B

TCC Service Level Agreement Template



Managed Infrastructure Support Service Level Agreement

Version 0.1

Customer
Logo

Effective Date: [Effective Date]

Termination Date: [Termination Date]

Document Approval

Reviewers' Signatures

Your signature indicates that, as a content expert, you have reviewed this document and that it accurately reflects the level of detail needed for the relevant systems.

Name	Title	Signature	Date

Approvers' Signatures

Your signature indicates that you acknowledge your responsibilities, agree with the purpose and scope of this document, and that the document has been reviewed by appropriate personnel to ensure successful fulfillment of this contract.

Name	Title	Signature	Date

Customer's Signatures

Your signature indicates that you acknowledge your responsibilities as stated within this document, agree with the purpose and scope of this document, and that you, as a representative of your company, obligate it to the terms listed within.

Name	Title	Signature	Date

Document Version History

This Version History documents changes to this document. Any differences between this version and previous ones are resolved in favor of the present document.

Ver.	Date	Author	Section changed/ Description

Table of Contents

1. Introduction	5
1.1. Intent.....	5
1.2. Scope	5
1.3. Terminology.....	6
1.4. Reference Documents	6
1.5. Periodic Review	6
2. Roles and Responsibilities	7
2.1. Customer Responsibilities.....	7
2.2. Service Provider Responsibilities	8
3. Service Agreement	9
3.1. Service Assumptions	9
3.2. Service Scope.....	9
3.3. Service Availability	9
3.4. Availability Restrictions	10
4. Service Management	11
4.1. Service Environment.....	11
4.2. Equipment, software and services covered	11
4.3. Service Maintenance	12
4.3.1. Service Exceptions	Error! Bookmark not defined.
4.4. Uptime Levels	13
4.4.1. Uptime Measurement.....	13
4.5. Response Times.....	13
4.5.1. Response Time Measurement	Error! Bookmark not defined.
4.6. Severity Levels	15
4.7. Service Level Reporting.....	15
5. Exclusions.....	16
Appendix A: Associated Policies, Processes and Procedures.....	17
Appendix B: Service Performance Reviews	18
Appendix C: Business Continuity Management.....	19
Appendix D: Third Party Contracts	20
Appendix E: Amendments.....	21

1. Introduction

This Agreement represents a Service Level Agreement (“SLA” or “Agreement”) between the TCC **Network Operations Group** and **[Customer]** for the provisioning of IT services required to support and sustain **[System and/or Service Name]**.

This SLA should be read alongside the IT support contract between the client and the supplier. This Agreement remains valid until superseded by a revised agreement mutually endorsed by the stakeholders. Changes are recorded in the Document Version History section of this Agreement and are effective upon mutual endorsement by the primary stakeholders.

This Agreement outlines the parameters of all IT services covered as they are mutually understood by the primary stakeholders. This Agreement does not supersede current processes and procedures unless explicitly stated herein.

1.1. Intent

The **purpose** of this Agreement is to ensure that the proper elements and commitments are in place to provide consistent IT service support and delivery to the Customer(s) by the Service Provider(s).

The **goal** of this Agreement is to obtain mutual agreement for IT service provision between the Service Provider(s) and Customer(s).

The **objectives** of this Agreement are to:

- Provide clear reference to service ownership, accountability, roles and/or responsibilities.
- Present a clear, concise and measurable description of service provision to the customer.
- Match perceptions of expected service provision with actual service support & delivery.

1.2. Scope

It is intended for this Policy to support processes <for all current TCC contracts and task orders>. These environments include <all production and non-production environments> as applicable to a particular tool.

1.3. Terminology

This document contains the following terms, acronyms and abbreviations.

Term	Explanation
NOG	Network Operations Group
SLA	Service Level Agreement
TCC	TCC Software Solutions

1.4. Reference Documents

The following documents are referenced or associated with this document.

1.5. Periodic Review

This Agreement is valid from the Effective Date stated herein until the Termination Date of the Services Contract. This Agreement should be reviewed at a minimum once per fiscal year; however, in lieu of a review during any period specified, the current Agreement will remain in effect. It may be reviewed at any point, by mutual agreement. It may also be reviewed if there are any changes to the client's IT system.

The Business Relationship Manager is responsible for facilitating regular reviews of this document. Contents of this document may be amended as required, provided mutual agreement is obtained from the primary stakeholders and communicated to all affected parties. The Document Owner will incorporate all subsequent revisions and obtain mutual agreements / approvals as required.

Business Relationship Manager: [\[Business Relationship Manager\]](#)

Review Period: [\[Review Period\]](#) e.g. "Annually" or "Quarterly"

Previous Review Date: [\[Last or Previous Review Date\]](#)

Next Review Date: [\[Next Review Date\]](#)

This Agreement will be posted to the following location and will be made accessible to all stakeholders:

Document Location: [\[SLA Directory and/or Location\]](#)

2. Roles and Responsibilities

The following Service Provider(s) and Customer(s) are the basis of the Agreement and represent the **primary stakeholders** associated with this SLA:

IT Customer(s): [Customer(s)] ("Customer")

IT Service Provider(s): [Service Provider(s)] ("Provider")

The following stakeholders are responsible for the deployment and ongoing support of this agreement: (contact information may include E-mail address, phone number, support line, etc.)

Stakeholder	Title / Role	Contact Information

2.1. Customer Responsibilities

Customer responsibilities and/or requirements in support of this Agreement include:

- Notify the service provider of issues or problems in a timely manner.
- Provide the service provider/suppliers with access to equipment, software and services for the purposes of maintenance, updates and fault prevention.
- Maintain good communication with the service provider/suppliers at all times.
- Adherence to any related policies, processes and procedures outlined in Appendix A: Related Policies, Processes and Procedures.
- Appropriate incidents and/or request prioritization as previously outlined and/or in cooperation with the Service Provider.
- Advanced scheduling of all service related requests and other special services with the Service Provider.
- Creation and maintenance of all Customer required project documentation.
- Appropriate use of support toolsets as outlined in Appendix A: Related Policies, Process and Procedures.
- Payment for all service-related setup and/or configuration costs prior to service provision.
- Review all hours logged by Service Provider for appropriateness.
- Reasonable availability of customer representative(s) when resolving a service related incident or request.

2.2. Service Provider Responsibilities

Service Provider responsibilities and/or requirements in support of this Agreement include:

- Ensure relevant software, services and equipment are available to the client in line with the uptime levels.
- Take steps to escalate and resolve issues in an appropriate, timely manner.
- Maintain good communication with the client at all times.
- Meeting response times associated with service related incidents.
- Generating quarterly reports on service levels for Customer
- Training required staff on appropriate service support tools.
- Creation and maintenance of all Service Provider required project documentation.
- Logging all Provider resource hours associated with services provided for review by the Customer.
- Appropriate notification to Customer for all scheduled maintenance.
- Facilitation of all service support activities involving incident, problem, change, release and configuration management.

3. Service Agreement

The following detailed service parameters are the responsibility of the Service Provider in the ongoing support of this Agreement.

3.1. Service Assumptions

Assumptions related to in-scope services and/or components include:

- Services are provided to customers external to IT and are communicated through one or more assigned Business Relationship Manager(s).
- Funding for major upgrades will be provided by the Customer and treated as a project outside the scope of this Agreement.
- Changes to services will be communicated and documented to all stakeholders.

3.2. Service Scope

The following Services are covered by this Agreement; full descriptions, specifications and costs are outlined in the IT support contract.

(References to the IT support contract may be pasted into this document or added as an Appendix to the Agreement for clarification, if required.)

Reference No.	Service
	Software licensing & patching
	Minor software upgrades
	Application server backup and recovery
	User security & account management
	Application data backup and recovery
	Automated server monitoring

Effective support of in-scope services is a result of maintaining consistent service levels. The following sections provide relevant details on service availability, monitoring, measurement and reporting of in-scope services and related components.

3.3. Service Availability

Coverage parameters specific to the service(s) covered in this Agreement are as follows:

- 8:00 A.M. to 5:00 P.M. EST
- Monday - Friday, 365 days per year, excluding the Service Provider observed holidays
- If the contract between the client and Service Provider specifically includes provisions for out of hours support, off hours coverage is performed through the on-call and escalation process

Production Computing Environment

Customer Availability	Sundays, 2:00 p.m. to Sundays, 2:00 a.m. EST
Maintenance Window	Sundays, 2:00 a.m. to 2:00 p.m. EST
Automated Server Monitoring	24 x 7 365 days per year

Development Computing Environment

Customer Availability	Monday to Friday, 6:00 a.m. to 8:00 p.m. EST
Maintenance Window	Monday to Friday, 8:00 p.m. to 6:00 a.m. EST; Fridays, 8:00 p.m. to Mondays, 6:00 a.m. EST
Automated Server Monitoring	Monday to Friday, 6:00 a.m. to 8:00 p.m. EST

3.4. Availability Restrictions

This section may be used to document specific times customer requires service availability and may include specific hours or days that should be avoided when emergency changes are required.

4. Service Management

4.1. Service Environment

The following information provides detail on the users, tools, applications and/or other components supported by this SLA:

Number of End Users: [# End Users] specific to application(s), if in scope

Number of Concurrent Users: [# Concurrent Users]

Number of Registered Users: [# Registered Users]

User Base Description:	[User Base Description] e.g. internal users, external users, etc.
In-Scope Applications:	[In-Scope Applications] e.g. including versions, modules, packaged, proprietary, etc.
Infrastructure Services:	[Infrastructure Services] e.g. specific network, security, telephony requirements, etc.
SLA Dependencies:	[SLA Dependencies] e.g. Operational Level Agreements (OLAs), Underpinning Contracts (UCs), parallel SLA dependencies, etc.

4.2. Equipment, software and services covered

This SLA covers only the equipment, software and services in the table below. This list may be updated at any time, with agreement from both the client and supplier.

Please note:

- The [Service Provider(s)] guarantees response times for all items listed in this section.
- The [Service Provider(s)] guarantees uptime only for items with a tick in the Covered for uptime?

These items have been assigned a priority level, from 1 (most important) to 3 (least important). The priority levels help determine the guaranteed uptime and response time.

Sometimes this information is contained in a separate database or document and the supplier will include extra details, like hardware serial numbers or software license keys. If that is the case, include or reference said DB or document.]

Item type	# of items	Priority	Covered for uptime?
			☐
			☐
			☐

			☐
			☐
			☐
			☐
			☐
			☐

4.3. Service Maintenance

TCC shall provide scheduled and preventative maintenance with the schedule based on the balanced needs of the Customer, the software and the equipment. TCC shall use commercially reasonable efforts to limit Service Maintenance and minimize the impact on system availability.

TCC shall attempt to schedule Service Maintenance during the times as specified in Table 1 – Service Maintenance Times. However, the parties agree that it may be necessary for TCC to perform Service Maintenance during times other than those specified in Table 1, and TCC reserves the right to perform Service Maintenance during times other than those specified in Table 1.

Table 1 – Service Maintenance Times

Service Maintenance Times (Day)	Service Maintenance Times (Hours)
Monday to Friday	xx:xx pm to xx:xx am (Time Zone)
Saturday	xx:xx pm to xx:xx am (Time Zone)
Sunday	xx:xx pm to xx:xx am (Time Zone)

- i. **Disclaimer of Actions Caused by and/or Under the Control of Third Parties.** TCC does not and cannot control the flow of data to or from TCC's network and other portions of the internet. Such flow depends in large part on the performance of internet services provided or controlled by third parties. At times, actions or inactions of such third parties can impair or disrupt customer's connections to the internet (or portions thereof). Although TCC will use commercially reasonable efforts to take actions it deems appropriate to remedy and avoid such events, TCC cannot guarantee that such events will not occur. Accordingly, TCC disclaims any and all liability resulting from or related to such events.
- ii. **Limitations.** TCC cannot assume responsibility and shall not be liable for any impacts on Service Availability due to (i) any requests for non-standard environment or Customer

machine access; (ii) any downtime caused by Customer produced code; or (iii) any changes to the Service by parties other than TCC. TCC will make reasonable efforts to ensure that Service changes do not affect customers.

4.4. Uptime Levels

In order to enable the client to do business effectively, the Service Provider guarantees that certain items will be available for a certain percentage of time. These uptime levels apply to items in the Equipment, software and services covered table that show a tick in the **Covered for uptime?** column.

The level of guaranteed uptime depends on the priority level of each item:

Priority level	Guaranteed uptime
1	99.99%
2	99.5%
3	99%

4.4.1. Uptime Measurement

Uptime is measured the using Service Provider's automated systems, over each calendar month. It is calculated to the nearest minute, based on the number of minutes in the given month (for instance, a 30-day month contains 43,200 minutes).

Important note:

- o Uptime measurements exclude periods of routine maintenance. These must be agreed between the supplier and client in advance.

4.5. Response Times

- When the client raises a support issue with the supplier, the Service Provider promises to respond in a timely fashion. The response time measures how long it takes the Service Provider to respond to a support request raised via the Service Provider's online support system.
- The Service Provider is deemed to have responded when it has replied to the client's initial request. This may be in the form of an email or telephone call, to either provide a solution or request further information. Guaranteed response times depend on the priority of the item(s) affected and the severity of the issue.
- Primary incident-reporting is done via TCC's Customer Ticketing System (powered by Zoho's ManageEngine ServiceDesk+). Through this system the customer has access to all tickets on your account, both open and completed, both current information and historical. TCC prioritizes tickets by severity, so, for example, issues where a site is completely unavailable will be processed before tickets where a site is slow, and those tickets for the Production Clouds will be processed before those for the Development Clouds. Shown below is a guide to the TCC Severity Levels:

Severity Levels	Explanation	Ticket Response Goals
Level 1 - Emergency	Production is down, business operations severely impacted with no workaround; or a security issue.	Within 30 minutes during TCC Business Hours, and except as otherwise provided herein, TCC guarantees response within 8 business hours. Note that these guidelines specify the time to begin investigation of the problem, not the length of time within which such problem will be resolved.
Level 2 - High	Production is operational but significant disruption of business operations; no stable workaround.	Within 1-hour during TCC Business Hours, and except as otherwise provided herein, TCC guarantees response within 8 business hours. Note that these guidelines specify the time to begin investigation of the problem, not the length of time within which such problem will be resolved.
Level 3 - Medium	Issues causing moderate to low business disruption with a Production or Development environment or any issue for which there is a stable workaround available.	Within 2-hours during TCC Business Hours, and except as otherwise provided herein, TCC guarantees response within 8 business hours. Note that these guidelines specify the time to begin investigation of the problem, not the length of time within which such problem will be resolved.
Level 4 - Low	Production or Development Environment is operational, no significant disruption of business operations; issues with little time sensitivity such as general questions	Within 4-hours during TCC Business Hours, and except as otherwise provided herein, TCC guarantees response within 8 business hours. Note that these guidelines specify the time to begin investigation of the problem, not the length of time within which such problem will be resolved.

- iv. Response times are measured from the moment the client submits a support request via the supplier's online support system.
- v. Response times apply during standard working hours (8 am — 5 pm) only, unless the contract between the client and Service Provider specifically includes provisions for out of hours support.
- vi. Internally, the TCC support team consists of Tiers, in which some groups respond more swiftly and handle more common questions and problems, and other groups handle issues which take more time or effort or expertise to solve. TCC also has an Operations group which has daily responsibilities outside of support, but are "on call" to assist in especially difficult cases or simply to handle overload from support. These groups, the processes therein, the people therein, etc., change over time as TCC learns how to better serve its customers, and therefore they are not documented here.
- vii. The goal of the Support Team is to provide specific support around the features and functionality of the Cloud technology itself, included but not limited to the provisioning, updating, securing, or other features and processes used by TCC. While the TCC support staff may look at the implementation of the software used in a particular Cloud in

an effort to diagnose problems, and may offer help where they can in order to alleviate client issues, TCC does not guarantee support for the installed software itself. TCC will, however, do its best to help any subscriber with their issues to the best of its abilities.

- viii. TCC will always endeavor to resolve problems as swiftly as possible. It recognizes that the client's computer systems are key to its business and that any downtime can cost money. However, the supplier is unable to provide guaranteed resolution times. This is because the nature and causes of problems can vary enormously. For instance, it may be possible to resolve a fatal server issue in minutes, simply by restarting the server. But if a server fails due to disk error or a hardware fault (also classed as a fatal issue) it may take much longer to get back up and running.
- ix. In all cases, TCC will make its best efforts to resolve problems as quickly as possible. It will also provide frequent progress reports to the client.

4.6. Severity Levels

The severity levels shown in the tables above are defined as follows:

Critical:	Complete degradation — all users and critical functions affected. Item or service completely unavailable.
High:	Significant degradation — large number of users or critical functions affected.
Medium:	Limited degradation — limited number of users or functions affected. Business processes can continue.
Low:	Small degradation — few users or one user affected. Business processes can continue.

4.7. Resolution Times

The supplier will always endeavor to resolve problems as swiftly as possible. It recognizes that the client's computer systems are key to its business and that any downtime can cost money. However, the supplier is unable to provide guaranteed resolution times. This is because the nature and causes of problems can vary enormously. For instance, it may be possible to resolve a fatal server issue in minutes, simply by restarting the server. But if a server fails due to disk error or a hardware fault (also classed as a fatal issue) it may take much longer to get back up and running.

In all cases, the supplier will make its best efforts to resolve problems as quickly as possible. It will also provide frequent progress reports to the client.

4.8. Service Level Reporting

The Service Provider will supply the Customer with the following reports on the intervals indicated:

Report Name	Interval	Recipient	Responsible

5. Exclusions

This SLA is written in a spirit of partnership. The [Service Provider(s)] will always do everything possible to rectify every issue in a timely manner.

However, there are a few exclusions. This SLA does not apply to:

- Any equipment, software, services or other parts of the IT system not listed above
- Software, equipment or services not purchased via and managed by the [Service Provider(s)]

Additionally, this SLA does not apply when:

- The problem has been caused by using equipment, software or service(s) in a way that is **not recommended**.
- The client has made **unauthorized changes** to the configuration or set up of affected equipment, software or services.
- The client has prevented the [Service Provider(s)] from performing required maintenance and update tasks.
- The issue has been caused by unsupported equipment, software or other services.

This SLA does not apply in circumstances that could be reasonably said to be beyond the [Service Provider(s)]'s control. For instance: floods, war, acts of god and so on.

This SLA also does not apply if the client is in breach of its contract with the [Service Provider(s)] for any reason (e.g. late payment of fees).

Having said all that, [Service Provider(s)] aims to be helpful and accommodating at all times, and will do its absolute best to assist [Customer Name] wherever possible.

Appendix A: Associated Policies, Processes and Procedures

Change Management

Definition: Change management refers to any event that alters the existing state of a Customer's production IT services, including software, hardware, networks and facilities.

Documentation: [Documentation Location / Link(s)]

Incident Management

Definition: The process of managing unexpected operational events with the objective of returning service to customers as rapidly as possible.

Documentation: [Documentation Location / Link(s)]

Problem Management

Definition: Problem Management identifies the root cause of a single significant, multiple or reoccurring incident(s) to prevent further incident activity.

Documentation: [Documentation Location / Link(s)]

Configuration Management

Definition: Identifies, records and validates critical computing components and their relationships with other configured items, maintaining a virtual representation of the IT infrastructure.

Documentation: [Documentation Location / Link(s)]

On-call and Escalation

Definition: Set of procedures set in place to handle out of hours support and escalation.

Documentation: [Documentation Location / Link(s)]

Appendix B: Service Performance Reviews

This section may contain additional details on SLA reviews, if required.

TEMPLATE

Appendix C: Business Continuity Management

This section may contain service recovery plans and related details, if required.

TEMPLATE

Appendix D: Third Party Contracts

This section may contain information on related Underpinning Contracts (UCs) that affect service support and/or delivery.

TEMPLATE

Appendix E: Amendments

Use this Appendix to reference any subsequent amendments to this agreement.

TEMPLATE

Appendix E

Sample Project Plan and Project Schedule



Project Kick-Off: NTP + 5 Business Days (8 hours)

Task #	Task Description	Assignee(s)	Estimated Hours
1	Conduct Kick-Off Meeting	Project Manager	4 hours
2	Finalize organizational structure & project RACI Matrix	Project Manager	
3	Compile contact information for SME's, & critical Client SPOC's, project stakeholders, etc.	Project Manager	
4	Review & verify communication plan	Project Manager	
5	Review & verify issue management plan	Project Manager	
6	Review & verify change management plan	Project Manager	
7	Create project issue log & risk register	Project Manager	
8	Determine transition schedule of activities	Project Manager	4 hours
9	Compile & publish Kick-Off meeting minutes for review and approval	Project Manager	

Scheduling and Planning: NTP + 5 Business Days (20 hours)

Task #	Task Description	Assignee(s)	Estimated Hours
1	Determine number of Technical Assessment review sessions needed and identify critical participants	Project Manager, CLIENT SME (Technical), Senior System Analyst	2 hours
2	Create a detailed agenda for each Technical Assessment review session to be published, at minimum, 2 days prior to session date	Project Manager, Senior System Analyst	4 hours
3	Confirm schedule of Technical Assessment review sessions and send out invitations	Project Manager	0.5 hour
4	Determine number of Business Process review sessions needed and identify critical participants	Project Manager, CLIENT SME (Business), Documentation Specialist	2 hours
5	Create a detailed agenda for each Business Process review session to be published, at minimum, 2 days prior to session date	Project Manager, Documentation Specialist	4 hours
6	Confirm schedule of Business Process review sessions and send out invitations	Project Manager	0.5 hours
7	Determine number of Current & Planned Work Stream review sessions needed and identify critical participants	Project Manager, CLIENT SME (Operations), Documentation Specialist	1 hours

8	Create a detailed agenda for each Current & Planned Work Stream review session to be published, at minimum, 2 days prior to session date	Project Manager, Senior System Analyst	4 hours
9	Confirm schedule of Current & Planned Work Stream review sessions and send out invitations	Project Manager	0.5 hour
10	Confirm & schedule bi-weekly status meetings with project stakeholders	Project Manager	0.5 hour
11	Finalize schedule of all activities associated with the Transfer of Operational Control and Knowledge Transfer	Project Manager	0.5 hour

Transfer of Operational Control: NTP + 30 Calendar Days (100 hours)

Item #	Task	Assignee(s)	Estimated Hours
1	Identify and prioritize the Business Processes critical to the transfer of operational control	CLIENT SME (Business), Project Manager	1 hours
2	Conduct Business Process review sessions	CLIENT SME (Business), Project Manager	8 hours
3	Conduct Technical Assessment review sessions	CLIENT SME (Technical), Senior System Analyst	6 hours
4	Identify and document source/app code locations, naming conventions and code repositories	CLIENT SME (Technical), Senior System Analyst	4 hours
5	Review and document server configurations in all environments	CLIENT SME (Technical), Senior System Analyst	2 hours
6	Review and document CLIENT database schema	CLIENT SME (Technical), Senior System Analyst	4 hours
7	Perform system health check on all databases, applications and other systems	Senior System Analyst	8 hours
8	Publish baseline metrics for all databases, applications and other systems	Senior System Analyst	2 hours
9	Analyze strengths/weaknesses of all production systems, identify improvement recommendations, and publish findings	Project Manager, Senior System Analyst	4 hours
10	Obtain access to source code, application code and 3 rd party tools	CLIENT SME (Technical), Senior System Analyst	2 hours
11	Obtain access to TFS and document configurations	CLIENT SME (Technical), Senior System Analyst	2 hours

12	Obtain access to non-production & production (if applicable) environments	CLIENT SME (Technical), Senior System Analyst	2 hours
13	Conduct Current & Planned Work Stream review sessions	CLIENT SME (Operations), Project Manager, Documentation Specialist, Senior System Analyst	10 hours
14	Obtain current release schedules for System Test, UAT & Production	Project Manager, Senior System Analyst	1 hour
15	Obtain a list of proposed, upcoming, or "TBD" work (pipeline)	Project Manager, Senior System Analyst	1 hour
16	Prioritize current and planned worked streams to be transitioned in order of criticality	CLIENT SME (Operations), Project Manager, Senior System Analyst	2 hours
17	Obtain the current Issue Log and document corrective actions	CLIENT SME (Operations), Project Manager, Senior System Analyst	1 hour
18	Review list of current work and document activities to be completed during transition	CLIENT SME (Operations), Project Manager, Senior System Analyst	2 hours
19	Publish revised RACI matrix (SDLC Roles & Responsibilities)	Project Manager	1 hour
20	Identify current and planned work stream development and testing efforts, establish a LOE and make necessary task assignments	Project Manager, Senior System Analyst	8 hours
21	Obtain and review all design documentation relevant to current and planned work streams	Senior System Analyst	12 hours
22	Develop and publish proposed release schedules for planned work streams	Project Manager, Senior System Analyst	8 hours
23	Mock production release (operations) performed and results analyzed	Senior System Analyst	2 hours
24	Mock emergency release performed and results analyzed	Senior System Analyst	2 hours
25	Mock back-up recovery performed and results analyzed	Senior System Analyst	2 hours
26	Shadow the incumbent TO contractor as they perform a scheduled production release	Project Manager, Senior System Analyst	2 hours

27	Review lessons learned compiled after completion of shadowed production release	CLIENT SME (Operations), Project Manager, Senior System Analyst	1 hour
28	Perform 1 st scheduled production release with only oversight from incumbent TO contractor	Project Manager, Senior System Analyst	2 hours
29	Review lessons learned compiled after completion of 1 st scheduled production release	CLIENT SME (Operations), Project Manager, Senior System Analyst	1 hour
30	Obtain client approval of the Transfer of Operations and assume responsibility	Project Manager	0.5 hours

Knowledge Transfer: NTP + 30 Business Days (25 hours)

Item #	Task	Assignee(s)	Estimated Hours
1	Locate all current technical, business process and operational procedure documentation	Project Manager	2 hours
2	Create (and/or update existing) document repository	Documentation Specialist, Senior System Analyst	2 hours
3	Assess all current technical, business process and operational procedure documentation for accuracy and completeness	Project Manager, Senior System Analyst	4 hours
4	Perform gap analysis on all current technical, business process and operational procedure documentation	Project Manager, Senior System Analyst	2 hours
5	Create additional technical, business process, and operational procedure documentation as necessary	Project Manager, Senior System Analyst	10 hours
6	Update issue log and risk register	Project Manager	0.5 hours
7	Prepare transition efforts status reports and publish, at minimum, 2 days prior to bi-weekly status meeting	Project Manager	2 hours
8	Participate in bi-weekly transition efforts status meetings with client	Project Manager	2 hours
9	Obtain client approval of the completion of Knowledge Transfer	Project Manager	0.5 hours

MTI DRAFT Project Schedule v1.3.1.mpp
Project Schedule



ID	%	T M	Pred	Task Name	Estimated Work	Actual Work	Duration	Actual Start	Actual Finish	M
0	8%			MTI DRAFT Project Schedule v1.3.1	1,245.7 hrs	135.4 hrs	133.66 days	Thu 9/24/15	Thu 3/31/16	
1	10...			Project Manager Assigned	0 hrs	0 hrs	0 days	Thu 9/24/15	Thu 9/24/15	
2	23%		1	Initiation, Inception	144.5 hrs	78.6 hrs	30.25 days	Thu 9/24/15	Thu 11/5/15	
3	10...			Establish Project Configuration Management Env.	1 hr	1 hr	0.06 days	Thu 9/24/15	Thu 9/24/15	
4	10...			Create SharePoint Project Directory with Standard Templates	0.25 hrs	0.25 hrs	0.25 hrs	Thu 9/24/15	Thu 9/24/15	
5	10...			Create Data Management Plan	0.25 hrs	0.25 hrs	0.25 hrs	Thu 9/24/15	Thu 9/24/15	
6	10...			Create Project Codes (NOG Portfolio, SPD, MESD, PayCom)	0.5 hrs	0.5 hrs	0.5 hrs	Thu 9/24/15	Thu 9/24/15	
7	23%			Project Initiation	143 hrs	77.6 hrs	30.19 days	Thu 9/24/15	Thu 11/5/15	
8	10...			Pre-Project Kickoff Meeting	24 hrs	24 hrs	1 day	Tue 9/29/15	Tue 9/29/15	
9	50%		8	Master Service Agreement (MSA)	41 hrs	33.6 hrs	12 days	Wed 9/30/15	Thu 10/15/15	
10	55%			Create Master Service Agreement (MSA)	40 hrs	33.6 hrs	11 days	Wed 9/30/15	Wed 10/14/15	
11	0%		10	MSA Formal Approval	1 hr	0 hrs	1 day	Thu 10/15/15	Thu 10/15/15	
12	0%		11	MSA Approved	0 hrs	0 hrs	0 days	Thu 10/15/15	Thu 10/15/15	
13	17%			Charter / Statement of Work (SOW)	78 hrs	20 hrs	30.19 days	Thu 9/24/15	Thu 11/5/15	
14	33%			Create Statement of Work (SOW)	60 hrs	20 hrs	30 days	Thu 9/24/15	Wed 11/4/15	
15	0%			Develop Project Charter	16 hrs	0 hrs	30 days	Thu 9/24/15	Wed 11/4/15	
16	0%		15	Project Charter / SOW Review	1 hr	0 hrs	1 hr	Thu 11/5/15	Thu 11/5/15	
17	0%		16	Project Charter / SOW Formal Acceptance	1 hr	0 hrs	0.5 hrs	Thu 11/5/15	Thu 11/5/15	
18	0%		13	Charter / SOW Approved	0 hrs	0 hrs	0 days	Thu 11/5/15	Thu 11/5/15	
19	0%		3,7	Collect and Review Lessons Learned	0.5 hrs	0 hrs	0.5 hrs	Thu 11/5/15	Thu 11/5/15	
20	0%		19	Go / No Go Approval Check Point	0 hrs	0 hrs	0 days	Thu 11/5/15	Thu 11/5/15	
21	10%		15SS	Planning, Elaboration & Design	297.75 hrs	44.8 hrs	40 days	Wed 9/30/15	Tue 11/24/15	
22	0%			Project Planning	42 hrs	0 hrs	26 days	Wed 9/30/15	Wed 11/4/15	

MTI DRAFT Project Schedule v1.3.1.mpp
Project Schedule



ID	%	T M	Pred	Task Name	Estimated Work	Actual Work	Duration	Actual Start	Actual Finish	M
42	30%		8	Requirements	161 hrs	44.8 hrs	30.25 days	Wed 9/30/15	Wed 11/11/15	
43	30%			Develop Requirements and Design Package	161 hrs	44.8 hrs	30.25 days	Wed 9/30/15	Wed 11/11/15	
44	31%			Technical Requirements	136 hrs	44.8 hrs	30 days	Wed 9/30/15	Tue 11/10/15	
45	40%			Workstations (30)	16 hrs	6.4 hrs	15 days	Wed 9/30/15	Tue 10/20/15	
46	40%			Servers (6)	20 hrs	8 hrs	15 days	Wed 9/30/15	Tue 10/20/15	
47	40%			Network (6)	20 hrs	8 hrs	15 days	Wed 9/30/15	Tue 10/20/15	
48	20%			Security, i.e., Active Directory	24 hrs	4.8 hrs	30 days	Wed 9/30/15	Tue 11/10/15	
49	20%			Cloud Migration	40 hrs	8 hrs	30 days	Wed 9/30/15	Tue 11/10/15	
50	10...			Applications, i.e., TMT - Completed as part of the assessment.	0 hrs	0 hrs	1 emin	Wed 9/30/15	Wed 9/30/15	
51	60%			Licenses	16 hrs	9.6 hrs	10 days	Wed 9/30/15	Tue 10/13/15	
52	0%		44FF	Technical Design Document	16 hrs	0 hrs	5 days	Wed 11/4/15	Tue 11/10/15	
53	0%		52	Technical Requirements Package Peer Review	8 hrs	0 hrs	1 hr	Wed 11/11/15	Wed 11/11/15	
54	0%		53	Approval of Requirements	1 hr	0 hrs	1 hr	Wed 11/11/15	Wed 11/11/15	
55	0%		54	Requirements and Design Review and Formal Acceptance	0 hrs	0 hrs	0 days	Wed 11/11/15	Wed 11/11/15	
56	0%		55	Final Project Schedule Updates	8 hrs	0 hrs	5 days	Wed 11/11/15	Wed 11/18/15	
57	0%			Update Project Schedule Based on Approved Requirements	8 hrs	0 hrs	5 days	Wed 11/11/15	Wed 11/18/15	
58	0%		57	Project Schedule Complete	0 hrs	0 hrs	0 days	Wed 11/18/15	Wed 11/18/15	
59	0%			Procurement	86.5 hrs	0 hrs	32 days	Mon 10/12/15	Tue 11/24/15	
60	0%		12FF+1 day	Select Vendor	0.5 hrs	0 hrs	5 days	Mon 10/12/15	Fri 10/16/15	
61	0%		51,12,60	Purchase Antivirus Software	1 hr	0 hrs	10 days	Mon 10/19/15	Fri 10/30/15	
62	0%		12,60,51	Windows Licenses	1 hr	0 hrs	10 days	Mon 10/19/15	Fri 10/30/15	
63	0%		12,60,51	Purchase WUG	80 hrs	0 hrs	10 days	Mon 10/19/15	Fri 10/30/15	

MTI DRAFT Project Schedule v1.3.1.mpp
Project Schedule



ID	%	T M	Pred	Task Name	Estimated Work	Actual Work	Duration	Actual Start	Actual Finish	M
64	0%		49,12,60	Purchase Contract with Cloud Vendor	2 hrs	0 hrs	10 days	Wed 11/11/15	Tue 11/24/15	
65	0%		47,12,60	Purchase CISCO ASA for Remote Connection	2 hrs	0 hrs	20 days	Wed 10/21/15	Tue 11/17/15	
66	0%		59	Procurement Complete	0 hrs	0 hrs	0 days	Tue 11/24/15	Tue 11/24/15	
67	0%		56FF	Collect and Review Lessons Learned	0.25 hrs	0 hrs	0.25 hrs	Wed 11/18/15	Wed 11/18/15	
68	0%			Execution, Construction & Testing	665 hrs	8 hrs	116.5 days	Fri 10/2/15	Wed 3/16/16	
69	4%			VPN	100 hrs	8 hrs	41 days	Fri 10/2/15	Mon 11/30/15	
70	9%		12	Set up VPN connection for MTI Office access for TCC Using Existing Firewall	8 hrs	8 hrs	11 days	Fri 10/2/15	Fri 10/16/15	
71	0%		12	Get Current configurations off Juniper	2 hrs	0 hrs	1 day	Fri 10/16/15	Fri 10/16/15	
72	0%		12	Gather requirements such as user info, VPN scope and security requirements from Tiffany.	32 hrs	0 hrs	4 days	Fri 10/16/15	Wed 10/21/15	
73	0%		65,72	Configure Equipment	2 hrs	0 hrs	1 day	Wed 11/18/15	Wed 11/18/15	
74	0%		73	Set up VPN on-site	8 hrs	0 hrs	1 day	Thu 11/19/15	Thu 11/19/15	
75	0%		73	Test VPN	8 hrs	0 hrs	1 day	Thu 11/19/15	Thu 11/19/15	
76	0%		75	VPN Training/Documentation	8 hrs	0 hrs	3 days	Fri 11/20/15	Tue 11/24/15	
77	0%		76	VPN Support write-up	24 hrs	0 hrs	3 days	Wed 11/25/15	Mon 11/30/15	
78	0%		77FF	VPN formal acceptance	8 hrs	0 hrs	1 day	Mon 11/30/15	Mon 11/30/15	
79	0%		78	VPN Installed/Accepted	0 hrs	0 hrs	0 days	Mon 11/30/15	Mon 11/30/15	
80	0%			Deep Assessment	72 hrs	0 hrs	13 days	Tue 12/1/15	Thu 12/17/15	
81	0%		78	Confirm Inventory	1 hr	0 hrs	1 day	Tue 12/1/15	Tue 12/1/15	
82	0%		81	Create inventory script	2 hrs	0 hrs	1 day	Wed 12/2/15	Wed 12/2/15	
83	0%		82	Manual listing of add/remove programs	5 hrs	0 hrs	1 day	Thu 12/3/15	Thu 12/3/15	
84	0%		83	Support Model Creation	8 hrs	0 hrs	1 day	Fri 12/4/15	Fri 12/4/15	
85	0%		84	Capture Baseline for CPU/Memory usage	24 hrs	0 hrs	6 days	Mon 12/7/15	Mon 12/14/15	
86	0%		85	Get Current ISP and circuit utilization	3 hrs	0 hrs	1 day	Tue 12/15/15	Tue 12/15/15	
87	0%		82,85	Copy Config Files	2 hrs	0 hrs	1 day	Tue 12/15/15	Tue 12/15/15	

MTI DRAFT Project Schedule v1.3.1.mpp
Project Schedule



ID	%	T M	Pred	Task Name	Estimated Work	Actual Work	Duration	Actual Start	Actual Finish	M
88	0%		85	Run Netstat for running ports	5 hrs	0 hrs	1 day	Tue 12/15/15	Tue 12/15/15	
89	0%		85	Find OS and service pack information per server	3 hrs	0 hrs	0.5 hrs	Tue 12/15/15	Tue 12/15/15	
90	0%		85	Discover last hotfix install date	5 hrs	0 hrs	1 day	Tue 12/15/15	Tue 12/15/15	
91	0%		90	Get a dump of running services	5 hrs	0 hrs	1 day	Wed 12/16/15	Wed 12/16/15	
92	0%		91	Fill out Excel document for pre-state and future state	8 hrs	0 hrs	1 day	Thu 12/17/15	Thu 12/17/15	
93	0%		91	Formal Acceptance of resources needed for cloud migration	1 hr	0 hrs	1 hr	Thu 12/17/15	Thu 12/17/15	
94	0%		93	Deep Assessment Complete	0 hrs	0 hrs	0 days	Thu 12/17/15	Thu 12/17/15	
95	0%		69	Update Production Environment	63 hrs	0 hrs	4.13 days	Thu 12/17/15	Wed 12/23/15	
96	0%		94	Figure out delta patching level	8 hrs	0 hrs	1 day	Thu 12/17/15	Fri 12/18/15	
97	0%		96	Schedule outages	2 hrs	0 hrs	1 hr	Fri 12/18/15	Fri 12/18/15	
98	0%		46,97	Patch 6 Servers Using Internet	24 hrs	0 hrs	2 days	Fri 12/18/15	Tue 12/22/15	
99	0%		98	Patch 3 Network Devices	3 hrs	0 hrs	1 day	Tue 12/22/15	Wed 12/23/15	
100	0%		94	Install Antivirus on 30 Workstations	15 hrs	0 hrs	3 days	Thu 12/17/15	Tue 12/22/15	
101	0%		98	Install Antivirus on 6 servers	3 hrs	0 hrs	3 hrs	Tue 12/22/15	Tue 12/22/15	
102	0%		98	Install and Configure WUG Monitoring Software	8 hrs	0 hrs	1 day	Tue 12/22/15	Wed 12/23/15	
103	0%		102	Production Environment Upgraded	0 hrs	0 hrs	0 days	Wed 12/23/15	Wed 12/23/15	
104	0%		95,49	Cloud Migration	131 hrs	0 hrs	30.38 days	Wed 12/9/15	Thu 1/21/16	
105	0%		102	Installation and Configuration of Cloud	4 hrs	0 hrs	5 days	Wed 12/23/15	Thu 12/31/15	
106	0%		105	Pre-Cloud health/readiness assessment	16 hrs	0 hrs	2 days	Thu 12/31/15	Mon 1/4/16	
107	0%		106	Create Cloud Migration Test Plan	12 hrs	0 hrs	10 days	Wed 12/9/15	Tue 12/22/15	
108	0%		105FF	Create Cloud Migration Implementation Plan	12 hrs	0 hrs	10 days	Wed 12/23/15	Thu 1/7/16	
109	0%		108	Cloud Migration Implementation Plan Walkthrough	9 hrs	0 hrs	1 day	Thu 1/7/16	Fri 1/8/16	
110	0%		109	Implement vConnector for P to V	8 hrs	0 hrs	1 day	Fri 1/8/16	Mon 1/11/16	

MTI DRAFT Project Schedule v1.3.1.mpp
Project Schedule



ID	%	T M	Pred	Task Name	Estimated Work	Actual Work	Duration	Actual Start	Actual Finish	M
111	0%		110	Create a schedule for test migrations	4 hrs	0 hrs	1 day	Mon 1/11/16	Tue 1/12/16	
112	0%		111	Perform additional test migrations	16 hrs	0 hrs	2 days	Tue 1/12/16	Thu 1/14/16	
113	0%		112	Right-size recommendation	8 hrs	0 hrs	1 day	Thu 1/14/16	Fri 1/15/16	
114	0%		113	Customer signoff	1 hr	0 hrs	1 day	Fri 1/15/16	Mon 1/18/16	
115	0%		114	Schedule Migration/outage	8 hrs	0 hrs	1 day	Mon 1/18/16	Tue 1/19/16	
116	0%		115	Implementation Walk-Through	9 hrs	0 hrs	1 hr	Tue 1/19/16	Tue 1/19/16	
117	0%		116	Cloud Migration Implementation Go Live	16 hrs	0 hrs	1 day	Tue 1/19/16	Wed 1/20/16	
118	0%		117	Post-Migration Support	8 hrs	0 hrs	1 day	Wed 1/20/16	Thu 1/21/16	
119	0%		118	Cloud Migration Complete	0 hrs	0 hrs	0 days	Thu 1/21/16	Thu 1/21/16	
120	0%		50	TMT Software Upgrade	259 hrs	0 hrs	44.13 days	Thu 1/14/16	Wed 3/16/16	
121	0%		104FF	Create TMT Test Plan	16 hrs	0 hrs	5 days	Thu 1/14/16	Thu 1/21/16	
122	0%		121,104	Create Cloud TMT Test Environment Using Clone of PROD	2 hrs	0 hrs	1 day	Thu 1/21/16	Fri 1/22/16	
123	0%		122	Upgrade TMT on Test Environment	15 hrs	0 hrs	20 days	Fri 1/22/16	Fri 2/19/16	
124	0%		122	Conduct TMT Testing	40 hrs	0 hrs	20 days	Fri 1/22/16	Fri 2/19/16	
125	0%		124	Look into Double-Take feasibility	6 hrs	0 hrs	1 day	Fri 2/19/16	Mon 2/22/16	
126	0%		124FF	Create TMT Implementation Plan	15 hrs	0 hrs	5 days	Fri 2/12/16	Fri 2/19/16	
127	0%		126	Create a new clone for Prod cutover	8 hrs	0 hrs	1 day	Fri 2/19/16	Mon 2/22/16	
128	0%		127	Install Double-Take software	8 hrs	0 hrs	1 day	Mon 2/22/16	Tue 2/23/16	
129	0%		128	TMT Implementation Plan Walkthrough	9 hrs	0 hrs	1 hr	Tue 2/23/16	Tue 2/23/16	
130	0%		124,129	TMT PROD Go Live	8 hrs	0 hrs	1 day	Tue 2/23/16	Wed 2/24/16	
131	0%		130	TMT Software Upgrade Complete	0 hrs	0 hrs	0 days	Wed 2/24/16	Wed 2/24/16	
132	0%		131	Priority 2 - Monitoring	132 hrs	0 hrs	15 days	Wed 2/24/16	Wed 3/16/16	
133	0%		131	daily/week/month/year monitoring schedule creation (includes 60 pt and SLA creation)	96 hrs	0 hrs	10 days	Wed 2/24/16	Wed 3/9/16	

MTI DRAFT Project Schedule v1.3.1.mpp
Project Schedule



ID	%	T M	Pred	Task Name	Estimated Work	Actual Work	Duration	Actual Start	Actual Finish	M
134	0%		133	Communications Media (Visio/Communication Plan)	16 hrs	0 hrs	2 days	Wed 3/9/16	Fri 3/11/16	
135	0%		134	Specific application monitoring	4 hrs	0 hrs	1 day	Fri 3/11/16	Mon 3/14/16	
136	0%		135	Reporting Requirements defined	8 hrs	0 hrs	1 day	Mon 3/14/16	Tue 3/15/16	
137	0%		136	SLA Signoff	8 hrs	0 hrs	1 day	Tue 3/15/16	Wed 3/16/16	
138	0%			Monitoring Requirements Complete	0 hrs	0 hrs	0 days	Wed 2/24/16	Wed 2/24/16	
139	0%		131FF	Create Operational Maintenance Plan	40 hrs	0 hrs	60 days	Tue 12/1/15	Wed 2/24/16	
140	0%		68	Product Construction Complete	0 hrs	0 hrs	0 days	Wed 3/16/16	Wed 3/16/16	
141	0%		140	Close, Implementation & Post Implementation	45.45 hrs	0 hrs	11.16 days	Wed 3/16/16	Thu 3/31/16	
142	0%			Close	45.45 hrs	0 hrs	11.16 days	Wed 3/16/16	Thu 3/31/16	
143	0%			Product Verification and Formal Project Accept	1 hr	0 hrs	1 hr	Wed 3/16/16	Wed 3/16/16	
144	0%			Lessons Learned	2 hrs	0 hrs	5 days	Wed 3/16/16	Wed 3/23/16	
145	0%			Stakeholder Survey	1 hr	0 hrs	5 days	Wed 3/16/16	Wed 3/23/16	
146	0%			Project Team Survey	1 hr	0 hrs	5 days	Wed 3/16/16	Wed 3/23/16	
147	0%			Project Audits	17 hrs	0 hrs	5 days	Wed 3/16/16	Wed 3/23/16	
148	0%			Procurement Audit	1 hr	0 hrs	1 hr	Wed 3/16/16	Wed 3/16/16	
149	0%			Auditing and Measurements	16 hrs	0 hrs	5 days	Wed 3/16/16	Wed 3/23/16	
150	0%		144,147	Develop Final Project Report	16 hrs	0 hrs	5 days	Wed 3/23/16	Wed 3/30/16	
151	0%		150	Project Close Meeting	8 hrs	0 hrs	1 hr	Wed 3/30/16	Wed 3/30/16	
152	0%		150	Release Resources	0.25 hrs	0 hrs	0.25 hrs	Wed 3/30/16	Wed 3/30/16	
153	0%		152	Final Project Report Approval	1 hr	0 hrs	1 hr	Wed 3/30/16	Wed 3/30/16	
154	0%		153	Update and Archive Project Documentation	0.2 hrs	0 hrs	1 day	Wed 3/30/16	Thu 3/31/16	
155	0%		152	Project Completed	0 hrs	0 hrs	0 days	Wed 3/30/16	Wed 3/30/16	
156	26%		1	Monitoring and Control	93 hrs	4 hrs	105.13 days	Thu 9/24/15	Mon 2/22/16	