Contract # AR2471

STATE OF UTAH COOPERATIVE CONTRACT

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

ATOS IT Solutions & Services,Inc
Name
2828 Haskell Ave
Address
Dallas | TX | 75204
City | State | Zip

LEGAL STATUS OF CONTRACTOR
- ☐ Sole Proprietor
- ☐ Non-Profit Corporation
- ☒ For-Profit Corporation
- ☐ Partnership
- ☐ Government Agency

Contact Person Karan Chetal Phone #914-733-5519 Email karan.chetal@atos.net
Vendor #94916A 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: 09/30/2016 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 the 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 and the Procurement Rules.

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 DocuSigned by: Ryan Schebler 070D23787D9642A... 12/29/2016
Contractor's signature Date

Ryan Schebler Ryan J. Schebler
Type or Print Name and Title

STATE
For Director, Division of Purchasing 1. 3. 2017
Date

Christopher Hughes	801-538-3254		christopherhughes@utah.gov
Division of Purchasing Contact Person	Telephone Number	Fax Number	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 Addendum[1] ("PA");
(2) NASPO ValuePoint Master Agreement Terms & Conditions, including the applicable Exhibits[2] to the Master Agreement; and
(3) 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, 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

[1] A Sample Participating Addendum will be published after the contracts have been awarded.
[2] The Exhibits comprise the terms and conditions for the service models: PaaS, IaaS, and PaaS.

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 or PA 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: Neither Party shall 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 other Party.

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 120 days written notice prior to the effective date of the termination. Further, any Participating Entity may terminate its participation upon 90 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.

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.

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 a material contractual requirement; or

(2) A material breach of any term or condition of this Master Agreement; or

(2) Any certification, representation or warranty by Contractor 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

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 for amounts that are subject to the dispute 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, brought by a third party 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, brought by a third party and 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.

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. Contractor shall provide evidence, upon request, of such coverage.

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 Office[3].

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.

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.

[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.

21. Payment: Unless otherwise stipulated in the Participating Addendum, Payment will be 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 electronic funds transfer. Use of a "Purchasing Card" may be agreed to in a Statement of Work.

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. Intentionally Left Blank

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 alicense to use the API for the term of the Purchasing Addendum.

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: The Contractor warrants 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. The Contractor will not interfere with a Purchasing Entity's access to and use of the Services it acquires from this Master Agreement.

c. At the time of delivery, the Services provided by the Contractor will be compatible with and will operate successfully with the environment (including web browser and operating system) specified by the Contractor in the Statement of Work.

d. 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.

Except as otherwise specifically provided in this Section or in the Master Agreement. CONTRACTOR MAKES NO WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO ANY PRODUCT, PART OR SERVICE SOLD OR SUPPLIED BY CONTRACTOR, AND CONTRACTOR EXPRESSLY DISCLAIMS ANY AND ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY, TITLE, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

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 in 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. Limitation of Liability: Except as otherwise set forth below, the limit of liability shall be as follows:

a. Contractor's liability for any claim, loss or liability arising out of, or connected with the Services provided, and whether based upon default, or other liability such as breach of contract, warranty, negligence, misrepresentation or otherwise, shall in no case exceed direct damages in: (i) an amount not to exceed a total of twelve (12) months charges payable under the applicable Purchase Order; or (ii) $1,000,000.00, whichever is greater..

b. The Purchasing Entity may retain such monies from any amount due Contractor as may be necessary to satisfy any claim for damages, costs and the like asserted against the Purchasing Entity unless Contractor at the time of the presentation of claim shall demonstrate to the Purchasing Entity's satisfaction that sufficient monies are set aside by the Contractor in the form of a bond, through insurance coverage, or through capital reserves on its balance sheet sufficient to cover associated damages and other costs.

c. Notwithstanding the above, neither the Contractor nor the Purchasing Entity shall be liable for any consequential, indirect or special damages of any kind which may result directly or indirectly from such performance, including, without limitation, damages resulting from loss of use or loss of profit by the Purchasing Entity, the Contractor, or by others.

The limitations of liability in this Section 43 will not apply to claims for bodily injury or death, breaches of Section 8 (Confidentiality, Non-disclosure and Injunctive Relief), or claims under Section 13 (Indemnification).

44. 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 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.

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.

Attachment B – Identification of Service Models Matrix

Service Model:	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered:
IaaS			X	Private Cloud
IaaS	X			Public Cloud (Hybrid hosted on Public Cloud)
PaaS			X	Private Cloud
PaaS	X			Public Cloud (Hybrid hosted on Public Cloud)
SaaS			X	Private Cloud
SaaS	X			Public Cloud (Hybrid hosted on Public Cloud)

Atos is capable of storing low-, medium-, and high-risk data in secured storage that can be encrypted at rest and in transport. Access to customer data is tightly controlled, and with access restricted to the customer only. Support staff can be restricted to not have access to customer data.

Attachment C – 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 %** 20

Infrastructure as a Service **Discount %** 20

Platform as a Services **Discount %** 20

Value Added Services **Discount %** 20

These discounts would be based on volume assessment.

For details, please see file "09b_Cost Proposal – CH16012 Cloud Solutions."

Additional Value Added Services:

Maintenance Services
Onsite Hourly Rate $ 85.06
Remote Hourly Rate $ 28.69

Professional Services

- **Deployment Services** **Onsite Hourly Rate $** 120.59
  Remote Hourly Rate $ 28.69
- **Consulting/Advisory Services** **Onsite Hourly Rate $** 168.19
  Remote Hourly Rate $ 41.21
- **Architectural Design Services** **Onsite Hourly Rate $** 168.19
  Remote Hourly Rate $ 41.21
- **Statement of Work Services** **Onsite Hourly Rate $** 168.19
  Remote Hourly Rate $ 41.21

Partner Services **Onsite Hourly Rate $** 200.00
Remote Hourly Rate $ 48.00

Training Deployment Services **Onsite Hourly Rate $** 200.00
Online Hourly Rate $ 48.00

Executive Summary

Atos, an Industry Leader in Cloud Services

Through our partnerships with industry leaders such as EMC and VMware, Atos provides a true "one-stop-shop" built upon a tight ecosystem of best-of-breed technologies. Provisioned in our data centers, our Cloud solutions are based on a secure environment and leading automation tools. They provide for ongoing seamless and predictable growth to accommodate evolving goals, enabling the State of Utah and Participating Entities to adopt Next Generation Cloud services at their own pace and speed of change.

Our Cloud solution portfolio ranges across Infrastructure as a service (IaaS), Platform as a service (PaaS), and Software as a Service (SaaS). These offerings provide the foundation for a full transformation that bring improvements in availability, speed to deployment, and a lower cost per user while delivering the following benefits:

- Greater financial transparency of IT costs and chargebacks
- Rapid application deployment capabilities
- Fully integrated solutions that can be deployed quickly

Our IaaS Cloud services include all infrastructure elements: data center facilities (floor space, power, cooling); hardware, maintenance, monitoring and management tools; operational support including incident management, problem resolution, operations and monitoring; production support; configuration/capacity/performance/change management; system administration, security operations, asset management, reporting, and account office support.

Atos' security services and security operations are integrated into Atos data centers and they conform to the State of Utah's required security policies. We propose Atos' standard global security services as a complete service package in areas such as vulnerability scanning, logs/event monitoring, and IDS/IPS. We would like to discuss your requirements more fully and understand additional areas Atos' standard global security services for Cloud environments may add value to the State of Utah in terms of potential increased efficiencies, agility, and security.

Atos can provide a comprehensive cloud backup solution for the State of Utah and Participating Entities. Tiered storage services, providing various performance classes of storage access network (SAN) and network access storage (NAS) storage to the Cloud compute services environment, are also integrated with the data center Cloud backup services. Tier 0 of storage services includes data replication to the secondary data center for disaster recovery with the ability to meet tight RTO/RPO requirements.

The data center Cloud backup solution is disk-based and includes replication to the alternate data center location to provide data protection and disc-based off-site storage. Workloads running in the secondary are also backed up to the local data center Cloud backup environment and replicated to the primary data center for off-site vaulting. This approach provides fast and efficient backup and recovery capabilities, and protection for any

workloads running in each data center through backup replication to the alternate data center.

As an overall quality program, we rely on ITIL v3 service management implementation, which includes availability, capacity, performance, service request management, and reporting. Additionally, we use standard ITIL process for incident, query, complaint, problem, change, and configuration management.

Summary

Our Cloud offerings are all about flexibility. We offer an infrastructure that is fully scalable and we have a proven track record of executing large Cloud projects in complex IT environments.

We will strive to provide the best client experience possible by implementing a specific Quality Care team led by an Account Management Office (AMO) dedicated to the State of Utah and Participating Entities. This AMO Quality Care team ensures that the best practices and service levels are being optimized for the State of Utah and Participating Entities.

The Atos solution for the State of Utah will provide key benefits such as increased service levels, reduced total cost of ownership, greater capacity (with scalability and elasticity), flexibility, agility, quality and innovation. Atos Cloud Service solutions also reduce risk by offering a completely standardized offering based on leading technologies and processes. Through this approach, we offer an enterprise class infrastructure to run critical application environments.

We engage our clients in a true spirit of partnership—one based upon growth, flexibility, and measurable IT business value. Our services approach and methodologies encourage the introduction of efficient technologies, service alignment, and scalability. As a trusted strategic partner, we firmly commit to meet the evolving needs of the State of Utah and Participating Entities.

Karan Chetal
Director, Client Services

Atos North America
2828 N. Haskell
Dallas, TX 75204

karan.chetal@atos.net

mobile: 914-733-5519

March 10, 2016

State of Utah Division of Purchasing
3150 State Office Building, Capitol Hill
Salt Lake City, UT 84114-1061

State of Utah Division of Purchasing:

Atos is pleased to respond to The State of Utah's Cloud Solutions RFP (Utah Solicitation Number CH16012).

5.2.1 Atos understands that we may be required to negotiate additional terms and conditions, including additional administrative fees, with Participating Entities when executing a Participating Addendum.

5.2.2 Atos is responsible for writing the proposal.

5.2.3 Atos is not currently suspended, debarred, or otherwise excluded from federal or state procurement and non-procurement programs.

5.2.4 Atos acknowledges that a 0.25% NASPO ValuePoint Administrative Fee and any Participating Entity Administrative fee will apply to total sales for the Master Agreement(s) awarded from the RFP.

5.2.5 Atos, under the terms of this RFP, is capable of providing IaaS, PaaS, and SaaS Service Models and deploying to all Deployment Models (i.e. Private, Community, Public, and Hybrid Clouds).

5.2.6 Atos has included a statement (below and in Attachment H) identifying the data risk categories that we are capable of storing and securing:

> Atos is capable of storing low-, medium-, and high-risk data in secured storage that can be encrypted at rest and in transport. Access to customer data is tightly controlled, and with access restricted to the customer only. Support staff can be restricted to not have access to customer data.

Atos has developed our response in accordance with the information provided. Our extensive experience, expertise, tools, and processes make Atos fully qualified to provide industry-leading cloud services, and we are committed to delivering exceptional customer service, continuous improvement of services, and competitive pricing.

Our extensive experience with cloud transformation makes Atos fully qualified to implement and provide a low-risk and sustainable value proposition over the life of the contract.

We look forward to the next phase of the evaluation process and working with The State of Utah to help achieve its objectives. If you have any questions, please contact me at 914-733-5519.

Sincerely,

Karan Chetal

Karan Chetal
Director, Client Services
Atos North America

5.3 (M) ACKNOWLEDGEMENT OF AMENDMENTS

Atos has and will acknowledge each amendment with a signature on the acknowledgement form provided with each amendment.

5.4 PLEASE SEE EXECUTIVE SUMMARY.

5.5 (M) GENERAL REQUIREMENTS

5.5.1 Atos agrees that if awarded a contract, we will provide a Usage Report Administrator responsible for the quarterly sales reporting described in the Master Agreement Terms and Conditions, and in applicable Participating Addendums.

5.5.2 Atos agrees to cooperate with NASPO ValuePoint and SciQuest (and any authorized agent or successor entity to SciQuest) with uploading an Offeror's ordering instructions, if awarded a contract.

5.5.3 Atos will, at a minimum, complete, provide, and maintain a completed CSA STAR Registry Self-Assessment, and Atos is in compliance with the Cloud Controls Matrix (CCM).

Atos represents and warrants the accuracy and currency of the information on the completed document(s) referenced above.

Additionally, Atos is committed to providing the highest levels of security globally. Atos is a member of the Cloud Security Alliance globally. Atos also maintains ISO certifications for 9000, 20000, and 27001, and has yearly SSEA-16/SAE 3402 audits. SOC 2 Reports and Certifications are available to customers who require them.

5.5.4 Atos has provided a sample of our Service Level Agreement, which would define the performance and other operating parameters within which the infrastructure must operate to meet IT System and Purchasing Entities' requirements.

5.7 RECERTIFICATION OF MANDATORY MINIMUMS AND TECHNICAL SPECIFICATIONS

Atos acknowledges that if we are awarded a contract under the RFP, we will annually certify to the Lead State that we still meet or exceed the technical capabilities discussed in our proposal.

Business Profile

This section should constitute the Offeror's response to the items described in Section 6 of the RFP. An Offeror's response must be a specific point-by-point response, in the order listed, to each requirement in the Section 6 of the RFP.

6 BUSINESS INFORMATION

6.1 (M) (E) BUSINESS PROFILE

Provide a profile of your business including: year started, organizational structure, client base (including any focus by region, market sector, etc.), growth over the last three (3) years, number of employees, employee retention rates (specific for employees that may be associated with the services related to the RFP) over the last two (2) years, etc. Businesses must demonstrate a minimum of three (3) years of experience providing cloud solutions for large scale projects, including government experience, to be eligible for award.

Atos has more than 30 years of experience and expertise providing IT services for clients. Atos Origin was formed in 2000 when Atos and Origin merged; the company is now called Atos SE. The State of Utah will have access to local, regional, and global senior leadership through Atos' organizational structure. The Atos organization model, shown in Figure 1, enables emphasis on the following areas:

- Global client focus and support with local support and service
- Innovations through the market sector and service line technology focus
- Delivery of committed service, quality level, and financial results through service lines and LEAN management processes

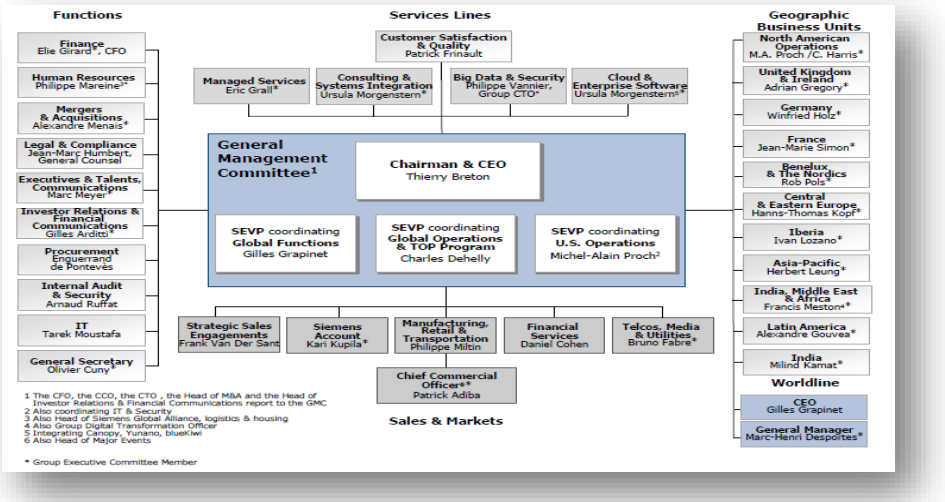


Figure 1. Atos Organizational Model

Figure 2 shows a time line of Atos' history.

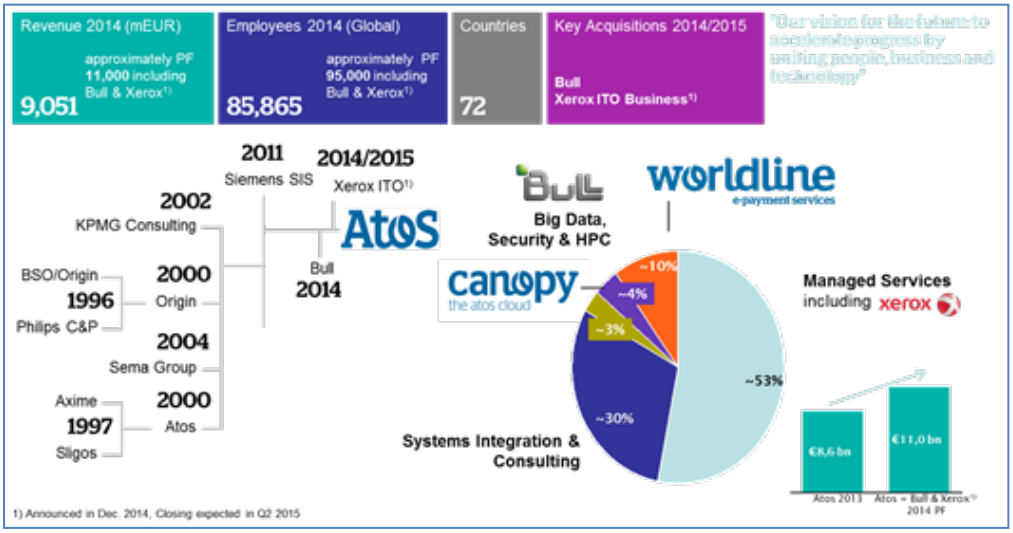


Figure 2. Atos History: Atos today is the evolution of many acquisitions and mergers that have contributed to the company's leadership in cloud, cyber-security, and other emerging technologies.

Atos Origin completed a merger with Siemens IT Solutions and Services on July 1, 2011, creating the company Atos. This combination of two strong IT leaders created one of the top IT companies in the world.

In November 2011, Atos and software services provider UFIDA International Holdings formed the joint venture Yunano. The new company provides innovative CRM and ERP cloud computing services to large and mid-size organizations in Europe, the Middle East, and Africa.

Atos joined with VMware and EMC in February 2012 to create a joint venture company, Canopy, a market-leading one-stop shop for cloud services. The strategic alliance will provide the advanced technologies upon which the new Atos cloud solutions and services will be delivered.

In April 2012, Atos acquired blueKiwi, a company that specializes in social networking technologies. The acquisition was initially made to help Atos achieve our corporate goal of zero email. blueKiwi is Europe's largest SaaS provider of enterprise social software. Since becoming an Atos company, blueKiwi has leveraged Atos' global presence and cloud technology expertise to further evolve our powerful SaaS solution. blueKiwi's focus on enterprise social networks, combined with Atos' broader product and service portfolio, creates a powerful combination that enables us to offer further value to our clients through a unique blend of consultancy, innovation, and implementation.

In May 2014, Atos announced the acquisition of Bull Group, a leading player in cloud, cyber-security, and Big Data, and the global leader in high-performance computing. The combination creates a world leader in cloud operations and a leading cyber-security solutions provider.

Bull brings critical and complementary capabilities in Big Data that, combined with Atos' solutions, will create a unique offering in this high-growth segment. As part of the Atos

"2016 Ambition," this combination of capabilities and solutions will enhance Atos' global leadership position in cloud services, and anchor its global leadership in managed services and systems integration. Complementary technologies will further increase Atos' businesses impact and the relevance of its disruptive and innovative offerings.

In December 2014, Atos announced its agreement with Xerox to acquire its Information Technology Outsourcing (ITO) business. Atos' ITO business employs approximately 9,800 employees in 45 countries, of which 4,500 are located in the United States and more than 3,800 are in global delivery countries such as India, the Philippines, and Mexico. The Atos ITO business is led by a strong and experienced management team that reinforces Atos' talent pool in the United States.

As part of the collaboration, Atos provides IT services to Xerox as a primary IT services suppliers. Atos added Atos' existing ITO clients comprising blue chip companies in the United States to its client base to accompany them on their digital transformation journey.

Acquisition of Atos was completed in June 2015. As a result of this acquisition, Atos now has a presence in 72 countries with 93,000 employees.

Table 1 and Table 2 depict key financial figures for last three years. Annual Reports and Audited Financial Statements for last three years can be viewed on the Atos website.

Table 1. Key Financial Information

In Euro Millions	FY 2014	FY 2013*	FY 2012*
Revenue	9,051	9,151	8,695
Income from Operations (Operating Margin)	701.9	645.2	566.9
Operating margin%	7.8%	7.7%	6.5%
Net Income	282.5	259.6	223.8
Earnings per share (EPS) before Goodwill (Euros)	2.67	2.98	2.66
Current Assets	4,618.7	3,509	3,615
Current Liabilities	3,663.2	2,960	3,188
Capital Employed (Total Shareholder's Equity)	3,402.1	2,939	2,379

*at constant scope and exchange rates

Table 2. Turnover History 2009 – 2014

	FY 2014	FY 2013	FY 2012	FY 2011	FY 2010	FY 2009
Turnover	15.67%	15.90%	19.50%	20.55%	21.1%	20.8%

Figure 3 is a representation of Atos' overall portfolio.

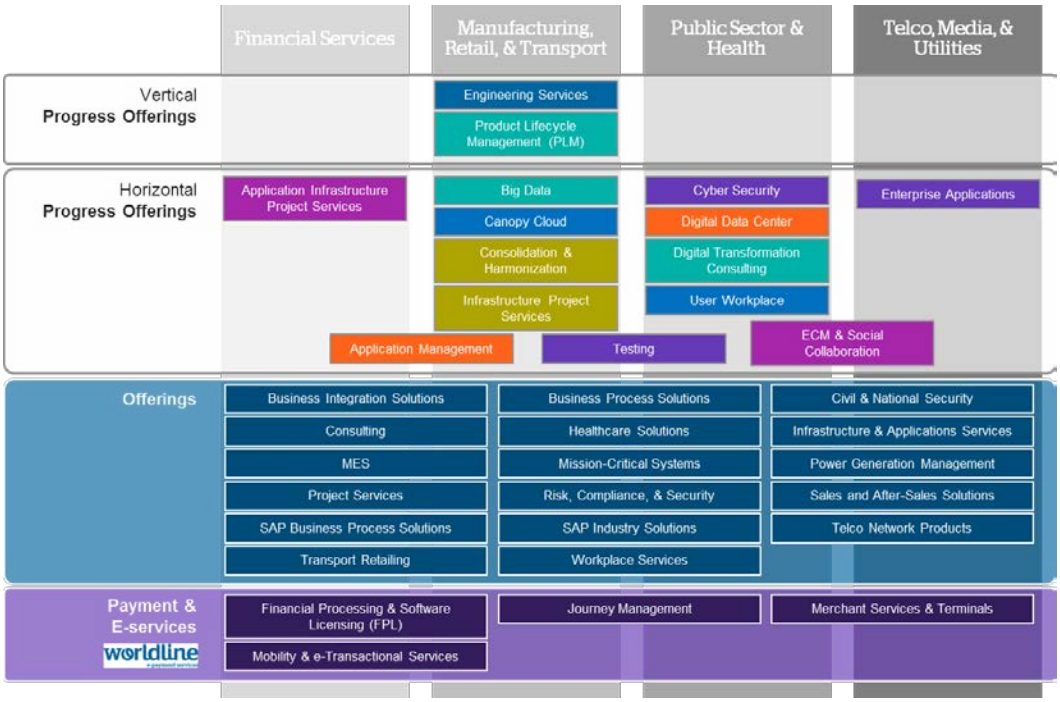


Figure 3. Markets and Portfolio Offerings: Atos has in-depth offerings targeting and spanning our target markets. As a full-service provider, Atos can provide the Lead State support beyond the in-scope services.

Atos provides a market-leading one-stop shop for cloud services, enabling organizations to easily, securely, and cost effectively accelerate their move to the cloud. As part of the strategic alliance, and in addition to providing the advanced technologies upon which the new Atos Cloud solutions and services will be delivered, Atos, EMC, and VMware jointly created Canopy to help drive innovation in the marketplace.

The strategic cloud offerings are based on open standards so customers can always choose their preferred technology, whether to run the solution off- or on-premise, and how to mix private and public cloud solutions to best meet their business needs. Atos provides the following solutions, among others:

- **Enterprise Application Store** — Powered by EMC and VMware technologies, enables customers anywhere in the world to choose, access, and download applications they require under the Software as a Service (SaaS) model. The store includes horizontal (cross-industries) and industry-specific business applications.
- **Enterprise Platform as a Service (PaaS)** — Powered by EMC and VMware technologies, and managed by Atos, provides a secure enterprise Java development environment, incorporating a standard development framework where Atos and our customers can design, create, and test new cloud applications.
- **Private Cloud** — Powered by EMC and VMware technologies, provide customers with a pre-configured, standardized, enterprise-grade cloud stack for on-premise and off-premise deployments, enabling customers to speed up their cloud readiness.
- **Cloud Strategy and Transformation Journey Design** — These consulting services range from building custom cloud strategy to shaping a cloud

transformation journey so that customers can grasp the benefits while moving to the cloud securely and at the speed that is right for them.

One example where our capabilities and reliability are major factors includes our support of the Olympic Games. For more than 20 years, Atos has been and continues to be the Worldwide Information Technology Partner for the Olympic Games. This agreement represents the extension of the largest sports-related IT contract ever awarded. As the primary IT provider to the Olympics Organizing Committee, Atos builds and delivers IT support for the Olympics. As such, the Olympics represent the size and scale of a start-up company of 200,000 employees with 4 billion customers, operating every hour of every day. Additionally, this environment relocates to a new territory every two years while technology, its fan base, and its customers' needs grow and change.

Figure 4. Atos and the Olympics: For more than 20 years, Atos has been the IT services integrator for the Olympic Games. In this role, we create a new IT environment every two years from scratch and coordinate the activities of hundreds of suppliers and support thousands of users.

6.2 (M)(E) SCOPE OF EXPERIENCE

Describe in detail the business' experience with government or large consortium contracts similar to the Master Agreements sought through this RFP. Provide the approximate dollar value of the business' five (5) largest contracts in the last two (2) years, under which the business provided offerings identical or very similar to those required by this RFP. Government experience is preferred.

While Atos does not disclose dollar values of contracts, five of our largest contracts in which we provide offerings identical or very similar to those required by this RFP are as follows:

- Texas Department of Information Resources
- Georgia Technology Authority
- City of Indianapolis, IN
- City of San Diego, CA
- Lee County, FL

To provide the best support to the Lead State, Atos applies governance that encompasses all aspects of our strategic direction, service offerings, technical integration, engagement model, relationship innovation, and market position. Our engagement model has built-in business value mapping and solution design capabilities tied to value, annuity pricing flexibility, governance, and evolution. Our ability to execute is rooted in our core focus in

the IT services market and our years of practical experience in managing complex services and infrastructures.

The Lead State's support from Atos will use a model based on assigning an Account Management Office (AMO) to be the umbrella management organization for integrating services, communications, and change throughout the contract term. The AMO is responsible for overall management of the engagement, providing a single focal point for all service delivery and daily senior management presence.

Through the AMO, the Lead State can expect the following activities:

- Relationship management that provides an interaction model for one-to-one alignment between the Lead State and Atos
- Clearly defined escalation that will apply intelligent decision-making through a chain of command approach to issue resolution
- Regular, open communication through scheduled and ad hoc meetings that will keep the Lead State's designated representatives informed, and provide transparency to IT delivery activities and performance
- Information Technology Infrastructure Library (ITIL) based process control that will ensure consistency of service delivery and measurable results

The AMO is based on the IT governance principles and alignment of key functional teams by strategic, tactical, and operational capabilities for the Lead State's demand organization and the Atos supply organization. The essence of this concept is that the Lead State retains responsibility for typical IT demand management tasks such as formulating the IT strategy and the resulting IT demands. The delivery of the agreed IT services, on the supply side, is the full responsibility of Atos.

Strategic Interaction – The Lead State can expect the vision, commitment, and behavior of senior management of both enterprises to contribute to the success of an outsourcing arrangement. Strategic activities are the topic of discussion at the senior management level. Typically, the leaders involved at this level ensure alignment between business objectives and joint initiatives. They establish the vision for the relationship. The framework agreement, which provides the overall process for each of the IT services to be delivered, is defined and monitored against key performance metrics. IT strategy and the consequences for IT demands also are defined at this level. This layer in the governance model also acts as the highest point of escalation for issues and problems.

Tactical Interaction – To ensure a successful management and delivery of services, Atos will establish an AMO for service delivery to oversee and manage the execution of support services and to direct continuous improvement activities related to these services. The AMO will work to improve workforce productivity through the implementation of established processes, tools, technology, and proven methodologies.

Operational Interaction – This level provides service delivery and the operational contacts with the Lead State's IT organization, which ensures smooth daily operations. Operational activities are meant to fulfill the IT strategy and are grouped into the following two areas:

- **Service Level Management** — Meet or exceed service level requirements in the delivery of the current services. Atos' service delivery management also uses SLAs to manage the interface with other IT suppliers.

- **Implement New Projects** — The execution of the IT strategy includes the roll-out of new services or improvement of existing ones; these changes are performed by project management professionals trained in the methodologies required for a smooth implementation.

One of the keys to successful account management is strong governance. The Lead State will have a single point of accountability for the delivery of the contracted services. The account governance model also may rely on Atos functional groups to support technology and business planning in addition to the dedicated team members.

6.3 (M) FINANCIALS

Offeror must provide audited financial statements, of the last two years, to the State that demonstrate that an Offeror meets at a minimum Dun and Bradstreet (D&B) credit rating of 3A2 or better, or a recognized equivalent rating. Please provide the Respondent's D&B Number and the composite credit rating. The State reserves the right to verify this information. If a branch or wholly owned subsidiary is bidding on this RFP, please provide the D&B Number and score for the parent company that will be financially responsible for performance of the agreement.

Table 3 and Table 4 provide the requested information at a high level. Please refer to Appendix 6.3 for a copy of Atos' FY 2014 Financial Report, which proves information on our financial status for FY 2014 and FY 2013.

Table 3. Income Statement, FY 2014 and FY 2013

	12 months ended 12/31/2014	% Margin	12 months ended 12/31/2013	% Margin
Operating Margin	701.9	7.8%	645.2	7.5%
Other Operating Income/(Expenses)	-261.6		-228.5	
Operating Income	440.3	4.9%	416.7	4.8%
Net Financial Income/ (Expenses)	-51.6		-62.7	
Tax Charge	-104.1		-95.9	
Non-controlling interests and associates	-19.4		3.5	
Net Income	265.2	2.9%	261.6	3.0%
Normalized Net Income	438.0	4.8%	415.3	4.8%

*In €millions

Table 4. Balance Sheet, FY 2014 and FY 2013

	12 months ended 12/31/2014	12 months ended 12/31/2013
ASSETS		
Intangible fixed assets	1,468	1,689
Tangible fixed assets	46	46
Participating interests	4,348,843	3,277,230
Other financial investments	791,534	775,336
Total fixed assets	5,141,891	4,054,301
Trade accounts and notes receivable	4,987	19,889
Other receivables	179,439	821,285
Cash and cash equivalent	1,002,037	836,006
Total current assets	1,186,463	1,677,180
Prepayments, deferred expenses	27,434	6,392
TOTAL ASSETS	6,355,788	5,737,873

*In €thousands

Atos IT Solutions and Services' D&B Number is 10-118-8514; our credit rating as of 2015 is 1R4.

6.4 (E) GENERAL INFORMATION

6.4.1 Provide any pertinent general information about the depth and breadth of your Solutions and their overall use and acceptance in the cloud marketplace.

Atos Enterprise Private Cloud (EPC) Service

Atos EPC is a dedicated, fully managed private cloud infrastructure solution that provides enterprises with a trusted first step to an enterprise cloud. It is an end-to-end hardware/software stack that pre-integrates industry-leading Atos, VMware, EMC, and VCE technologies. Atos EPC consists of Atos' EPC Infrastructure and EPC Managed Services. Atos EPC Managed Services enables users to provision OS via a private cloud portal. Both virtual and physical compute options are available from an Atos catalogue of supported OS's, designed and built for rapid automated infrastructure provisioning. Atos EPC provides three OS management tiers, allowing customers to access both virtual and physical OS's, with varying levels of management and SLAs.

Atos Cloud Infrastructure Service (CIS)

Atos' CIS provides computer processing, storage, and backup services in a flexible way. An appropriate secure network connection is realized, enabling customers to access the services. CIS is primarily delivered from central hub locations in each of the three regions in the world: EMEA, AMEC, and APAC. Alternatively, when local regulations or laws are in force, CIS can be delivered from satellite locations.

CIS is offered in two variants, shown in Figure 5. Depending on the chosen variant, the level of resource-sharing varies: From an environment in which resources are fully shared and connectivity is by default arranged via the Internet ("CIS – Multi-Tenant"), to a partly shared environment ("CIS – Single Tenant") where dedicated processing resources are realized for the customer. Apart from resource-sharing differences, there are differences in terms of agility as well.

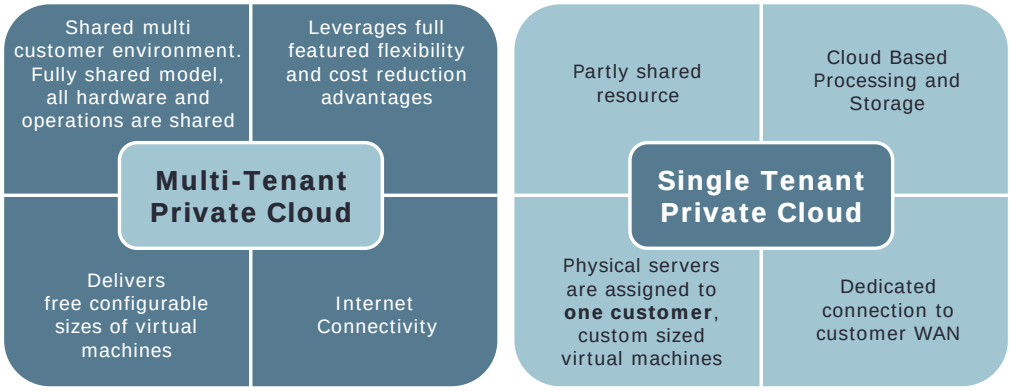


Figure 5. CIS variants: Depending on the chosen variant, the level of resource-sharing varies.

The following are important characteristics of cloud services:

- **Secure** — Customer environments are isolated from one another through the use of VLAN technology. Additionally, firewall technology is used to isolate security zones within the customer environment. Customers may share enclosures. Server blades are not shared in CIS – Single Tenant. Server blades are shared in CIS – Multi-Tenant. The system management environment is also separated by firewalls.
- **Managed** — Atos manages the entire infrastructure using remote monitoring and automatic alerting, and keeps both the underlying hardware and software up-to-date.
- **Flexible tariff structure**
- **Self-service** — A service catalogue is part of the basic CIS service, allowing customers to request and change services and allocated capacity, and to view CIS service reports.

Processing capacity is located in Atos Data Centers; customers can choose between Microsoft Windows, Red Hat Linux, and SUSE Linux Server operating systems. Each customer environment has its own separate security zone(s). This environment is accessible through a secure connection over the Internet or a dedicated WAN connection.

Atos manages the CIS computing environment in accordance to ISO 9001, ISO 27001, and ISAE3402 standards.

Atos' Trusted Agile Infrastructure Environment

With the Trusted Agile Infrastructure (TAI), Atos offers customers a secure and centrally hosted environment that meets the requirements of developers and users, yet addresses the needs of IT departments for production environments. It could also be used for other purposes, such as acceptance testing and training. The capacity provisioned can be adjusted to the customers' needs should they vary over time.

The immediate availability of infrastructure resources reduces service provisioning times significantly. This offers flexibility for test and development, and reduces internal approval processes, thereby reducing cost in the development cycles. TAI is targeted to customers who want the following:

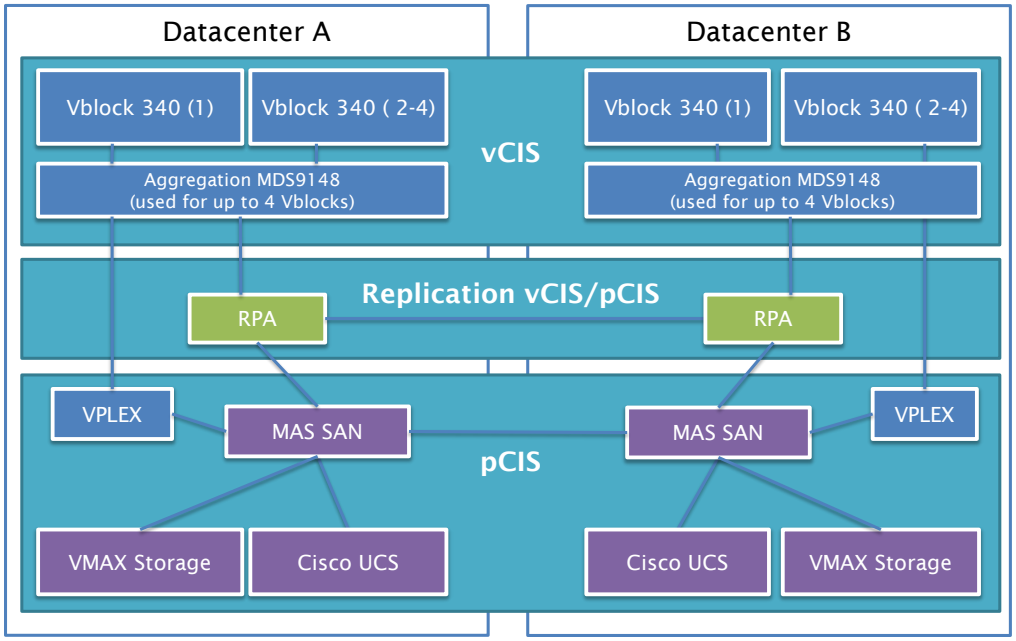
- A flexible environment that can be used for various purposes, such as development, test, acceptance, and training
- Easy self-management and responsive delivery
- A highly standardized environment to ensure quality
- Flexibility in processing hardware, storage, and network in terms of how this capacity is used
- Flexible addition or reduction of capacity
- Reduced investment compared to the customer-dedicated hardware
- Certified, compliant, and secure environments eligible to their business processes

All servers in a TAI environment are virtual machines. Standard access to the environments is via the Internet. If the demand increases, a dedicated network connection is possible.

Atos Cloud Infrastructure Platform (CCIP) Foundation

All Atos services are built using Atos' Cloud Infrastructure Platform (CCIP) foundation. The CCIP foundation comprises all the necessary environments needed for the provision of services to (XaaS) providers. The foundation itself has no direct interface to end customers. The CCIP foundation modules with a customer or an XaaS interface are as follows:

- Infrastructure
  - Data Center infrastructure
- Hardware
  - EMC Vblock (Type XXX, YYY)
- Software
  - VMware vSphere Enterprise Plus
  - VMware vCloud Automation Suite
  - VMware vCloud Networking and Security, which includes VPN, load balancing, and high-availability firewall features
  - VMware vCloud® Automation Center™
- Backup
  - EMC Avamar/Data Domain



Virtual characteristics of the CCIP include the following:

- Single standardized Vblock model chosen to scale within hub or satellite locations
- Standard compute blade to optimize virtualization ratio
- Tiered storage aligned to EMC STONE contract
- Gateway to shared storage environment for flexible capacity (via VPLEX)

CCIP physical characteristics are as follows:

- Scalable Cisco UCS solution with three blade options (Regular, Large, Performance)
- Leverages shared storage environment (MAS)
- Interconnected with vCIS environment for consistent business continuity

Satellite considerations for the CCIP include the following:

- Utilizes same building blocks as hub
- Initial deployment will allow for consolidated vCIS and pCIS on Vblock
- Scale out beyond single Vblock system will follow hub architecture

Implement standard Vblock infrastructure for virtual workloads (vCIS) aggregated with scalable Cisco and EMC components for physical workloads (pCIS), as follows:

- Provides flexible and independent scaling options for pCIS and vCIS workloads
- Leverages existing investments in storage (MAS)
- Provides common and standardized implementation and management environments across vCIS and pCIS
- Enable consistent business continuity for vCIS and pCIS workloads

Enabling technologies for CCIP include the following:

- Vblock 340 with VNX7600 for vCIS
- Cisco UCS and EMC VMAX for pCIS
- RecoverPoint for aggregated business continuity across vCIS and pCIS

Platform as a Service (PaaS)

Atos offers a full spectrum of PaaS services that enables running various types of applications in the cloud. These PaaS services enable you to focus on the business objectives of developing and running applications, with minimal distraction in infrastructure provisioning and management.

For green-field applications that take advantage of cloud-native architecture and frameworks, Atos provides fully managed Cloud Foundry as a Service. Cloud Foundry application teams can readily deploy and operate cloud native applications on Atos-managed Cloud Foundry platforms.

For brown-field applications that need to be made more cloud friendly, Atos provides a managed private PaaS for Windows and Linux applications. It removes the need to learn how to build, deploy, operate, and maintain a business-critical platform, and enables customers to simply consume and focus on the benefits derived from developing and running modern application services. It includes enterprise service levels and integrated service management with self-service capabilities. Customers also have access to flexible, private Atos hosting capabilities.

For legacy and third-party applications that simply need to be moved to the cloud, the Atos cloud application deployment automation and management PaaS platform provides a fully managed application orchestration service. Through Atos' state-of-the-art application "blueprint as code" technology and open-source based cloud brokering technology, entire legacy application landscapes can be blueprinted and deployed to multiple cloud architectures and cloud providers. Such automation ensures a high level of agility, consistency, and reusability that is compatible with the promise of cloud.

Atos PaaS offerings are fully integrated with ITSM solutions like ServiceNow to ensure PaaS-based activities are managed under your enterprise IT service management and governance framework.

6.4.2 Offeror must describe whether or not its auditing capabilities and reports are consistent with SAS 70 or later versions including, SSAE 16 6/2011, or greater.

Atos annually undergoes an SSAE audit of our central data centers, networks, and service desk services at our North American centers. The SSAE 16 requirements are an ongoing process that we continue to support based on client needs. Our audit covers a 12-month period from October 1 through September 30 each year, with the report being published in November.

The original Statement on Auditing Standards (SAS 70) was issued in 1992 by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) so that service organizations could have their internal controls periodically examined, approved, and subsequently proven to clients.

Statement on Standards for Attestation Engagements No. 16 (SSAE 16) was created with the intention of bringing the United States up to code with the International Standards for Assurance Engagements, as well as to address a number of areas not addressed in SAS 70.

As of June 15, 2011, SSAE 16 replaces SAS 70 as the authoritative guide for service organization reporting.

Activities of Atos Managed Services typically have an impact on the control environment of our customers (user entities) through information systems managed by Atos. In this case our customers may require the issuance of SOC 1 reports for the controls at Atos (for instance, for customers listed on the U.S. Stock Exchange and required to be compliant with the SOX regulation).

The ISAE3402 / SSAE16 assessments are performed on the basis of the Atos IT Control Framework (ITCF), aiming to issue "Generic assurance reports" (instead of specific reports by customer) that can meet the requirements of the in-scope customers. The Atos ITCF has been chosen as the main reference for standard controls to increase coherence and efficiency across our organization; it is an integral part of the Book of Internal Controls (BIC).

The ISAE / SSAE MS Generic report program is managed in the central level by Atos' Global MS ISAE team. An audit program is run every year in a similar approach, as follows:

- Audit program is managed and planned centrally including agreements with external auditor.
- Scope is defined locally.
- Testing period is a full year from October 1 to September 30.
- Testing is performed in two audit phases.
- Remediation of phase 1 deviations is done before phase 2 testing, and deviations of phase 2 are done prior to when the next audit cycle starts.
- Final reports are issued in October.

Scope reports include the following:

- ISAE3402/SSAE16 (SOC 1 Type II)
- ISAE3000 BCP/BCM report
- ISAE3000 report on Internal Assessment

To carry out the audit process, local coordinators have been appointed in each GBU/country. The role of the local coordinator is as follows:

- Local SPOC for ISAE / SSAE audit program and all communications
- Defines the local scope of generic ISAE 3402 / SSAE 16 reports
- Plans and coordinates the local audit activities
- Raises change request to global in case of any changes to local audit plan during the audit. All changes need to be approved by global team (Example: Extension of timeline and additional compensating testing, which has financial impact).
- Coordinates the evidence provisioning and ensures the quality and correctness of the evidence prior providing to external auditor
- Reviews deviations reported and final draft reports
- Is SPOC for deviation remediation planning and follow-up
- Distributes the final report to relevant people in their local organization and customers

6.5 (E) BILLING AND PRICING PRACTICES

DO NOT INCLUDE YOUR PRICING CATALOG, as part of your response to this question.

6.5.1 Describe your billing and pricing practices, including how your billing practices are transparent and easy to understand for Purchasing Entity's.

Atos will provide the Lead State with detailed billing and reporting. Financial and operational control objectives have been developed by Atos to provide assurance to our clients regarding the effectiveness and efficiency of operations, including reliability of invoicing and financial reporting, as well as adherence to contractual terms. The objective of our controls is to ensure the alignment of both parties' strategic intent; the financial objectives of our controls provide assurance of the following:

- Accuracy and completeness of invoices
- Sufficient invoice detail provided to support chargeback and audits
- Invoices that are consistent with contract terms
- Financial objectives consistent with strategic intent

The operational objectives of the controls provide assurance of the following:

- Accuracy and completeness of service-level reporting
- Sufficient detail provided to assess operational performance
- Contract deliverables meet contractual terms
- Efficiency and effectiveness of operations
- Operational objectives are consistent with strategic intent

The compliance objectives of Atos' controls are designed to provide assurance that both parties are adhering to the terms of the agreement as well as applicable laws and regulations. Additionally, our business relationship will be conducted in accordance with the highest ethical standards, taking into account each party's Code of Conduct and ethics guidelines. In instances where one party has a higher standard, the higher standard will prevail. Individuals involved in managing the business relationship will review and acknowledge, at least annually, that they have read and understand the other party's Code of Conduct and ethics guidelines.

Typical engagements split invoice management into the following two components:

- An invoice is submitted on the first of each month, which covers negotiated base charges for the services Atos is engaged to provide. These base charges cover a certain minimum of organizational engagement to provide services (hardware, software, focused and leveraged resource pool dedication based on forecasted volumes).
- A secondary invoice is created to address variable volume consumption over and above baselines. Both are produced by the financial and delivery arms of Atos and submitted for approvals and validation to the business unit manager prior to submission to the customer.

6.5.2 Identify any typical cost impacts that a Purchasing Entity might need to consider, if any, to implement your cloud solutions.

Atos recommends that the Lead State clearly separate out the one-time costs associated with SciQuest portal interaction efforts—such as assessment, requirements, design, and deployment of the participating providers' service catalog information—from standard recurring price structures for cloud-based compute. Furthermore, cloud consultancy services are vital to ensure success of any future adoption of cloud offerings for participating entities; therefore, service fee rate cards should be separated out to allow for flexibility and use. Finally, Atos recommends the price associated for governance of delivering solutions be isolated in order to fully understand a potential vendor's approach and price structure. Atos strongly recommends that a robust governance structure be inserted along with an Account Management Office (AMO) framework.

Atos prides itself on demonstrating a high degree of price flexibility for our Cloud Offerings and Services. We stand ready to demonstrate flexibility for the Lead State to ensure all participating entities secure the solutions required for success.

6.5.3 Offeror must describe how its Solutions are NIST compliant, as defined in NIST Special Publication 800-145, with the service models it offers.

Atos' offerings included in this response, all comply with the current NIST definitions, as published in NIST Special Publication 800-145, for Cloud Computing, in terms of the following:

- Essential Characteristics – On-Demand Self-Service, Broad Network Access, Resource Pooling, Rapid Elasticity, and Measured Service
- Service Models – IaaS, PaaS, and SaaS
- Deployment Models – Private, Community, Public and Hybrid Cloud

6.6 (E) SCOPE AND VARIETY OF CLOUD SOLUTIONS

Specify the scope and variety of the Solutions you offer under this solicitation. You may provide a list of the different SaaS, IaaS, and/or PaaS services and deployment models that you offer.

Atos intends to propose IaaS, PaaS, and SaaS offerings as part of our response.

Infrastructure as a Service (IaaS)

Atos' CIS provides an open, enterprise-standard cloud Infrastructure-as-a-Service (IaaS) technology solution, based around VMware vSphere as the key virtualization component, with Cisco and EMC providing the supporting elements. This means you can move your current workloads into the cloud with very little risk, thanks to the proven infrastructure model that VMware virtualization provides. In addition, the flexible, agile cloud-hosting model of Atos CIS means that you will be ideally placed to implement additions and new systems directly in the cloud in the future.

Atos has built and fully supports the Atos CIS infrastructure in our U.S., European, and APAC data centers.

Atos has a proven reputation for delivering business outsourcing services with the following:

- Excellent service
- A vendor-neutral and open approach to technology
- Enterprise-grade security

Atos will continue to deliver these qualities in the cloud, leveraging the extensive experience of our Managed Services group, who already manage thousands of the largest IT infrastructures for clients.

Atos are pleased to take this opportunity to offer CIS to the Lead State (through your initiative), which will provide the following:

- Consume-first/ pay-later pricing, with effective monitoring and reporting to allow you to manage costs.
- Reduced capital expenditure as Atos CIS becomes a recurrent, operational cost that varies in line with usage, rather than a fixed, up-front cost for new hardware and software.
- A fully managed service, so that:
  - You have a single point of contact for all service related issues via an online portal.
  - The service covers all managed technologies, up to and including the operating system (unlike many public clouds).
  - SLAs cover all levels of the technology stack, from the virtualization layer up to the OS.
  - Integration of Atos CIS is within your own business processes, using Atos CIS to deliver just part of your end-to-end business process.
- Flexible scale-up / scale-down capabilities (within limits to protect system stability).
- Very granular assignment of virtual capacity, so you can customize the performance and cost of resources to closely meet your requirements.
- Reduced management overheads from:
  - Automation, which increases efficiency
  - Workflow technologies, which reduce manual intervention
  - Full infrastructure management (including anti-virus and server operating system patches), which otherwise will consume your specialists' valuable time

Introduction

Atos CIS provides IaaS, which comprises enterprise-ready computing, storage, and networking capacity in the cloud. Atos CIS uses Atos' well-proven technology stack, which we host, manage, and support from Atos Data Centers in key locations across the globe (including the U.S.).

By leveraging Atos' expertise and experience, we deliver managed IT services for many of the world's largest organizations, including for the entire Olympic Games since 2006. Atos delivers a cloud environment, which is engineered to the highest standards and managed using rigorous processes for minimal risk. As a result, the Atos CIS cloud will deliver a high-

quality compute cloud to which you can trust your most important production workloads. Additionally, the Lead State can be confident that your data will remain confidential.

Unlike many public clouds, Atos CIS offers a *fully managed* private cloud. Fully managed means that Atos takes responsibility for managing the entire hardware and software stack in the cloud, up to and including the operating system. This management encompasses local networking; storage; and backup, plus the monitoring, management, and maintenance of all these components, so you don't have to. Gone are the days of setting up individual, technology-specific monitoring tool-sets, with 24x7 staff to feed and water physical servers and storage, and tend them in their hour of need. Instead, Atos takes full responsibility for their management, so that you can create and configure a virtual machine, quickly and easily in our online portal, after which Atos will ensure that this OS is provisioned, and maintained in tip-top condition over time.

In particular, Atos will do the following:

- Proactively correct error conditions, often without you being aware there is a problem
- Monitor for common over-capacity conditions, such as low disk space, high CPU levels etc., and advise you when upgrades are required
- Test, apply, and automatically update OS software patches to increase security and stability
- Provision hardware capacity headroom to ensure that should you wish to add additional capacity, it will be available, on tap (within certain limits)
- Arrange for the addition and removal of storage in line with your demands
- Manage local network traffic levels and provision additional capacity as required
- Provide clear monthly reporting on usage, to enable you to monitor and control your costs

Atos' CIS Solution

The provision of enterprise IT services is changing, with shorter business cycles and increasing pressure to deliver, which is quickly eroding the benefits of purchasing hardware for each new system that comes along. Additionally, the explosion of IT apps requiring hosting for delivery to multiple end-user devices means that the skills required to manage many servers are in increasingly short supply.

To address exactly these issues, and unlike most public cloud providers, Atos CIS offers a cloud service with a *fully managed* operating system, which can free up your highly skilled staff from the drudgery of day-to-day management of servers, operating systems, storage, backup, and network services, and for activities which are of more strategic value to your business.

Atos CIS combines our proven ability to "keep the IT lights on," with cloud flexibility to change rapidly in response to your changing needs. Key characteristics of the Atos CIS cloud include the following:

- A pre-built cloud IaaS environment hosted out of Atos Data Centers in multiple locations across the U.S.
- A variety of virtual server sizes, with different CPUs and memory to suit differing workloads.

- Multiple enterprise OS's, including Microsoft Windows Server and Red Hat Enterprise Linux.
- Built on the enterprise-standard virtualization platform that is VMware vSphere, which allows agile up-scaling and down-scaling of virtual resources.
- CIS' Dynamic Scalability option provides additional vCPU, vMEM, and storage capacity resources for volatile business demands, provisioned via the online portal.
- Comprehensive load balancing services can distribute workloads across multiple virtual machines, improving availability and security while delivering all load balancing and reverse proxy functionality.
- A portal is available where a service order catalog can be accessed to create and amend virtual resources, including a dashboard that provides an overview of your environment in near-real time where role-based access controls secure access to the portal for your business users.
- Atos Care provides a single point of contact for the efficient resolution of events, based on contracted service levels.
- Atos' CIS gives you the flexibility to mix-and-match from the following tenancy, and hardware blade types in the same environment to meet varying security, performance, and cost requirements; for example:
  - Single-tenant, physical blade with "bare-metal" OS, where your own, dedicated hardware blades provide maximum performance and enable you to arrange your own software licensing
  - Single-tenant, extra, extra large physical blade with "bare-metal" OS, providing high-performance compute capacity for extreme performance in the cloud, such as databases
  - Single-tenant, virtualized blades where a fully managed hypervisor virtualizes your dedicated hardware blades where you can run multiple virtual machines
  - Multi-tenant, virtualized OS's for maximum cost-effectiveness that securely shares all hardware components (blades, storage, and networks) among multiple clients

Atos CIS Overview

The scope of the Atos Cloud Infrastructure Service is shown in Figure 5.

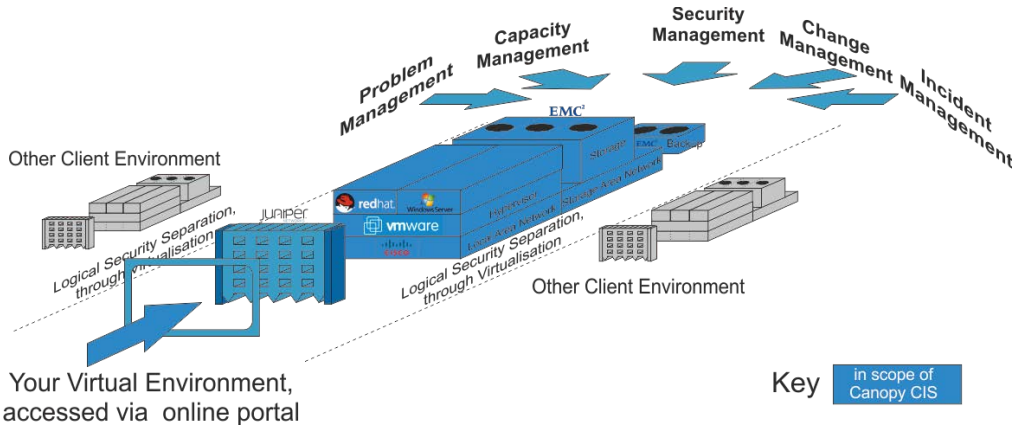


Figure 6. Scope of the Atos Cloud Infrastructure Service

The primary components of the CIS service are as follows:

- Virtualization
- Compute Capacity
- Storage Disk Arrays & Storage Area Networks
- Local Network
- Firewalls
- Load Balancers

Our proposed solution for the Lead State is built using these standard architectural building blocks above and includes the following:

- Compute (Blade) Capacity
- Operating System and Anti-Virus Licenses
- Storage
- Backup
- Data Center Local Area Network

CIS Compute Capacity

The Atos CIS solution for the Lead State uses the following servers:

- CIS Multi-Tenant Virtual Servers
- CIS Single-Tenant Virtual Servers
- CIS Single-Tenant Virtual DR Servers (on separate site)
- CIS Single-Tenant Physical Servers

Atos CIS Multi-Tenant Virtual Servers

Atos CIS Multi-Tenant Virtual Servers provide cost-effective compute capacity using VMware virtualization technology, which enables multiple Atos clients to share compute capacity in the cloud.

All multi-tenant virtual servers are protected by the standard Atos CIS cloud high-availability mechanism, using VMware HA to provide N+1 blade resilience. This means that at any one time, each VMware cluster of up to 31 blade servers has additional blade capacity of one blade, onto which virtual servers will migrate, automatically, if any of the servers in the cluster fail. This provides a high degree of resilience in the face of hardware, and many software, failures.

Atos CIS Single-Tenant Servers

For your server instances that are not suitable for running on the Atos CIS Multi-Tenant Cloud, Atos will provide CIS single-tenant servers instead.

Single-tenant servers comprise blade servers in the Atos CIS cloud that are dedicated to your use only, although storage and networking is shared with other Atos enterprise clients, but logically separated.

Single-tenant servers' pricing comprises the following three elements:

- Atos CIS Single-Tenant Virtual Environment (one or more)
- Atos CIS Single-Tenant Virtual Servers (Primary and DR sites)
- Atos CIS Single-Tenant Physical Servers

Atos CIS Single-Tenant Virtual Environment

All single-tenant virtual servers in CIS are contained within a single-tenant virtual environment, which provides a server hosting environment for the virtualization of physical servers that are dedicated to one customer only (i.e., single tenant). They also comprise a private ESX cluster in which such servers reside for management purposes.

Atos CIS Single Tenant Virtual Servers

On a primary site, single-tenant virtual servers provide the same level of service and functionality as multi-tenant servers, but on dedicated (non-shared) compute hardware blades.

At the Disaster Recovery site, Atos will provide duplicate single-tenant servers for Disaster Recovery of your critical servers, using VMware Site Recovery Manager (SRM) software in conjunction with synchronous replication of storage data between the primary and DR sites. This will allow simple, single-click recovery of virtual machines in the second site following a disaster.

Atos CIS Single-Tenant Physical Servers

CIS single-tenant physical servers can be used to run the following specific OS instances:

- Oracle production servers
- Other high-performance database and application servers
- Windows Servers running Windows Server Failover Clustering

For your critical servers that require hot-standby, high-availability across two sites, Atos proposes the use of Atos CIS Infrastructure Continuity. Infrastructure Continuity will use Windows Server Failover Clustering to provide auto-failover high availability across multiple sites.

Windows Server Failover Clustering operates at the OS level, in conjunction with synchronous Atos CIS cloud storage replication. This ensures that the complete loss of a server, or the site the server is located on, will mean that the stand-by server on the second site will automatically, and instantly, take over the role of the primary server, and continue to operate until normal service is restored.

The clustered servers will be located on a single/separate sites, as required.

Atos CIS Operating System Licenses

Microsoft Windows Server licenses will be provided as part of this service.

A Linux support contract with Red Hat/Suse will be provided as part of this service.

CIS Dynamic Scalability

CIS provides dynamic scalability to enable scale-up and scale-down for peak workloads. On-demand resizing of resources can be done by using CIS portal. It offers easily adjustable, highly scalable capacity for your business-critical applications to meet your demands supported by premium CIS cloud managed services and enterprise SLAs. This provides the following:

- Pay per use
- Zero cost for dynamic scalability until it is required
- Monthly billing using averaged resource consumption

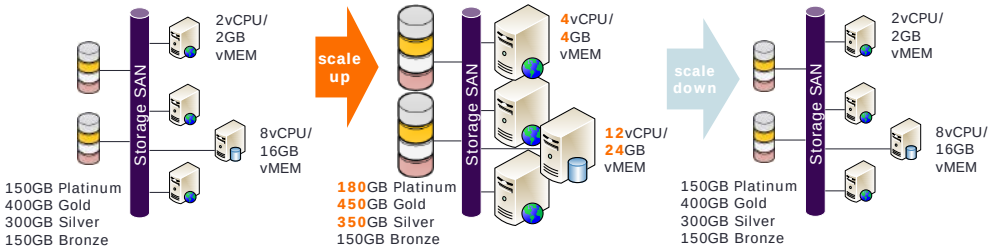


Figure 7. Dynamic Scalability – an illustration of how services can be scaled up as required

Atos CIS Storage

The Atos CIS solution will make use of the following CIS storage types:

- Platinum (Very High Performance) Storage Tier
- Gold (High Performance) Storage Tier
- Silver (Medium Performance) Storage Tier
- Bronze (Archive Performance) Storage Tier

Platinum storage is the fastest tier of storage that can be stored on a single site, where offsite backups can also be taken to provide data recovery in case of a disaster. Alternatively, where Disaster Recovery is required for single-tenant virtual servers, as described above, Platinum Storage can be replicated instantly and continuously to a second site. Such continuous, synchronous replication ensures that should a disaster strike the primary data center, a complete copy of each virtual machine image will be available in the second data center for use when a disaster situation is declared.

Gold storage is a fast tier of storage delivering the same features as the Platinum storage tier, but at slightly lower performance and, hence, lower cost. Example uses include databases and email storage, etc.

Silver Storage is lower performance storage, which is more cost-effective for applications where the high speed, and associated higher cost, of Gold storage is not appropriate.

Bronze storage in the archive tier provides low-cost, high-volume storage using commodity disks for cost-effective storage.

Note that all storage types (Platinum/Gold/Silver/Bronze & Replicated/Non-Replicated) can be flexibly provisioned on each different type of virtual machine, allowing the easy mix-and-match of storage resources to meet the differing cost and flexibility requirements of different applications.

Platinum Storage

CIS SAN Platinum storage will be used for very high-performance storage; e.g., high-performance databases, etc.

CIS NAS Platinum storage will be used for very high-performance storage—e.g., databases etc., which must be mounted on more than one physical or virtual server. NAS storage will be provisioned as NFS file systems, with CIFS is created on NFS partitions to provide Windows Servers with storage.

SAN/NAS storage will be synchronously/asynchronously replicated, dependent on distance, between CIS primary and DR sites to enable DR and/or CIS infrastructure continuity.

Gold Storage

CIS SAN Gold storage will be used for the following:

- OS partitions where high performance is essential
- High-performance storage; e.g., databases, email mailboxes, etc.

CIS NAS Gold storage will be used for high-performance NAS storage—e.g., databases, email mailboxes, etc., which must be mounted on more than one physical or virtual server.

NAS storage will be provisioned as NFS file systems, with CIFS created on NFS partitions to provide Windows Servers with storage.

SAN/NAS storage will be synchronously/asynchronously replicated, dependent on distance, between CIS primary and DR sites to enable DR and/or CIS infrastructure continuity.

Silver Storage

CIS SAN Silver storage will be used for medium-performance storage; e.g., non-database applications.

CIS NAS Silver storage will be used for medium-performance storage—e.g., non-database applications, which must be mounted on more than one system.

NAS storage will be provisioned as NFS file systems, with CIFS created on NFS partitions to provide Windows Servers with storage.

SAN/NAS storage will be synchronously/asynchronously replicated, dependent on distance, between CIS primary and DR sites to enable DR and/or CIS infrastructure continuity.

Bronze Storage

CIS SAN and NAS bronze storage will be used for data types and data volumes (GB) that require archive-performance storage; e.g., infrequently accessed data, historic archives, etc.

NAS storage will be provisioned as NFS file systems, with CIFS created on NFS partitions to provide Windows Servers with storage.

Bronze SAN/NAS storage will not be synchronously replicated between CIS primary and DR sites to enable DR and/or CIS infrastructure continuity.

Atos CIS Backup

The solution makes use of the following Atos CIS backup types:

- Active Backup
- Archive Backup

Active backup provides file-level backup and restore, including scheduling, running, and verification of routine backups. In the case of a system failure, the operating system functionality and data partitions are restored from backup media.

The default retention period of the File Level Backup is 45 days.

When requested, Atos will start the restore after receiving confirmation of the point to restore. Atos carries out regular checks of the backup procedures and backup results.

For longer term archiving, archive backup is also provided, which can be used to retain data for longer than 45 days.

Platform as a Service (PaaS)

Atos offers two distinct formats for PaaS, as follows:

- Virtualization / provisioning of legacy applications / databases, etc.
- Provisioning of cloud-ready applications

Virtualization/Provisioning of Legacy Applications

Atos can help the Lead State improve time-to-market of software products, improve software deployment reliability, and orchestrate cloud assets across a wide range of cloud providers and cloud architectures.

Driven by the need of faster time-to-market and speed-of-innovation, enterprise IT organizations continue to improve delivery efficiency and quality of service through agile processes and software automation. At the same time, it enables end-to-end agility through the application management life cycle, system provisioning, and application orchestration and management processes.

However, complexity in data center operations and network configuration, and differences in infrastructure technology have forced organizations to adopt elaborate change control and multi-discipline testing and staging mechanisms to ensure consistent application deployment quality and production performance.

Through the blueprinting technology of Atos PaaS, enterprise customers can capture and automate any system provisioning and deployment process that their IT staff already routinely performs for legacy, third-party, and green-field applications. Going far beyond just keystroke scripting, Atos is capable of connecting to all major cloud-based IaaS APIs, and provisioning VMs and networks through declarative application blueprints and policies that can be easily translated from business requirements. This enables our customers to focus on application development and operations instead of constantly trying to keep up with the rapidly changing IaaS and cloud technologies and providers. By retaining knowledge on system configuration, deployment, and management in these declarative application landscape blueprints, customers can reliably capture and document the critical knowledge of designing and operating applications for long-term re-use and automation. As blueprints are moved across cloud locations and between different IaaS technology stacks, customers can consistently reuse the same blueprints.

Compared to popular IaaS provision tools, Atos can uniquely blueprint, deploy, and manage entire landscapes of applications. Atos can capture the desired state of the complete application architecture and all of its nodes in a single blueprint—whether it's a multi-tier Web application with clusters of app servers and databases, or a high-availability application with instances expanding to multiple cloud locations and cloud providers.

Atos PaaS is powered by open-source projects like Apache Brooklyn and Apache jclouds. These are technologies aimed to accelerate cloud adoption by allowing businesses to benefit from cloud while remaining in control and having the power to model, deploy, and manage applications. By partnering with Cloudsoft Corp., the primary contributor to Apache Brooklyn, Atos offers customers the best cloud automation and orchestration expertise in the industry and the leading managed services experience.

For customers with IT Service Management (ITSM) implementation, such as ServiceNow, our standard API based ITSM + Atos PaaS integration offers a single pane of glass for cloud service management processes throughout the organization.

Cloud brokering would provide the Lead State the ability to deploy any blueprint to any approved cloud infrastructure platform. We offer a number of global cloud infrastructure targets with the option of a public, private, or hybrid cloud to meet all security and compliance needs.

Atos PaaS can help the Lead State with the following:

- Improve agility
  - Accelerate your time to market for new cloud-native applications
  - Improve responsiveness to business requests
  - Compose can deploy complex blueprints in minutes
- Increase flexibility
  - User can update configurations and scale horizontally or vertically
  - Take advantage of R&D and pricing cuts of multiple cloud providers
- Lower TCO
  - Pay for only what you consume
- Increased Control

- Take control of cloud sprawl and non-compliant shadow IT
- Fully utilize YAML scripting to manage the deployment of blueprints

Provisioning of Cloud-Ready Applications

Atos can help the Lead State to bring innovative new digital experiences to your customers faster than currently possible by accelerating the development and delivery of cloud-native applications.

Atos' Cloud-Ready PaaS is powered by open source Cloud Foundry, the leading cloud application platform, with additional tenancy, licensing, location, and hosting options, as well as comprehensive professional services and rock-solid enterprise-class SLAs.

Our leading enterprise PaaS, which would enable the Lead State to build, deploy, manage, update, and retire applications much faster, offers the following features:

- **Build applications faster**—Atos' Cloud-Ready PaaS will detect which frameworks and other dependencies an application uses and automatically include them in the build.
- **Deploy applications faster**—Atos' Cloud-Ready PaaS enables developers to self-service application deployments into the testing, staging, or production environments for which they have access – without having to carry out any infrastructure-related tasks.
- **Scale applications easily**—Atos' Cloud-Ready PaaS enables you to run multiple instances of your application and automatically load balance connection requests across the instances. Simply change the number of instances to match the demand on your application, and it will take care of spinning up additional instances or spinning down instances no longer required.
- **Protect your applications automatically**—If any instance of your application fails, Atos' Cloud-Ready PaaS removes that instance from the load balancing group so it no longer gets sent any connection requests, restarts the failed application instance, and then rejoins it to the load balancing group.
- **Update your applications without downtime**—Atos' Cloud-Ready PaaS enables new versions of an application to be incorporated into a load balancing group on a rolling upgrade basis, allowing all instances of the application to be upgraded from version A to version B without any application downtime. There may also be scenarios where you may want to keep both version A and version B of your application live concurrently to allow piloting/feedback of the new version before upgrading all instances.
- Scale down the number of application instances during less busy periods, or retire all instances of the application when no longer required, to **free up resources** for your other applications.

Software as a Service (SaaS)

Atos looks at business applications from the business point of view. So when it comes to providing SaaS, we look at applications that fulfill real business needs, and we scale them to the needs of our customers. We offer SaaS solutions from PLM and CRM right through to Collaboration solutions in flexible and scalable models.

6.7 (E) BEST PRACTICES

Specify your policies and procedures in ensuring visibility, compliance, data security and threat protection for cloud-delivered services; include any implementations of encryption or tokenization to control access to sensitive data.

Security is critical to the success of business operations, and Atos has designed a robust cloud security model to protect cloud systems and data at all levels of the infrastructure. The Atos cloud security model is designed so that all customers are completely isolated from one another. We can provide further isolation at the business unit level should clients wish to more granularly align their infrastructure and applications to the business units that utilize them.

Atos accomplishes this workload isolation using the private VLAN approach. This approach also enables us to support multi-tiered application architectures by defining security zones within each VLAN separating the customer's web, application, and database tiers. In addition to private VLAN isolation, we utilize hypervisor firewalls to monitor VM-to-VM (East-West) traffic inside the cloud environment as well as traffic entering and leaving the cloud environment (North-South).

In addition to using private VLANs, and physical and virtual firewalls to keep systems isolated, we use a broad range of enterprise tools to keep the environment secure, including intrusion detection systems (IDS), intrusion prevention systems (IPS), security information and event management (SIEM), and regularly scheduled vulnerability scans. These tools provide multiple layers of security to further protect the cloud workloads from unauthorized access. From an end-user access perspective, Atos can extend an existing active directory (AD) environment by provisioning AD domain controllers in the client's cloud, allowing the client to continue using their centralized identity access management system.

Managed Security Services

Atos offers proven, enterprise solutions to the growing threat of cyber-based attacks and misuse of data. Our solutions provide defense-in-depth security from the desktop to LAN/WAN and Internet levels. We manage security services in the way we manage our business process and IT services: we use a combination of mature methodologies and industry best practices in concert with our experienced and skilled professionals.

Cyber-security requirements encompass a wide range of inputs, views, threats, environments, and constraints. Businesses face external threats, insider threats, and regulatory requirements in the United States and internationally. When building sound security solutions, each factor must be considered.

We embrace the ITIL methodology as the foundation of our security services. Our policies and procedures are heavily influenced by ISO 17799 2005, and we follow ISO 20000 documentation practices. We employ a program of monitoring, responding, and assessing data in a manner that complies with current laws and regulations, while remaining flexible to changes that occur as those standards evolve. Atos mitigates risks by giving priority to critical data to ensure integrity, availability, and confidentiality.

Management Approach

Atos takes a consultative approach concerning IT security. Our approach for security management is based on the combination of stated security requirements and our best-practices methodology. We continue to deliver solutions to meet specific requirements based on this methodology. Atos' approach addresses our clients' security requirements and provides a structured management process for ongoing services.

Atos complements an industry best-practices methodology with our extensive experience. We continue to work closely with our clients to address critical security issues and offer solutions that provide the best options for managing security operations.

Logical Control Approach

Logical security controls act as a boundary between the client's network segments and the point of demarcation with Atos systems. The following examples of logical controls can be deployed for the security solution:

- Traffic Analysis
- Password Management
- Intrusion Detection Systems (IDS)
- Vulnerability Management
- Network Access Control
- User Provisioning and De-Provisioning
- Anti-Virus Solutions
- Penetration Testing
- Risk Assessment

The logical control approach for Atos security processes may include the following control phases, which are industry-accepted standards and are compliant with IT auditing standards:

- **Directive Controls** — Includes the client's and Atos management's actions, policies, and procedures. This level of control provides direction relative to system availability, auditing, integrity, and data and systems security.
- **Preventive Controls** — Atos' security practices, tools, techniques, and operational standards provide quality and reliability, as well as controls that prevent unwanted events. Training, technology review, and growth are important components of this control.
- **Detective Controls** — These controls identify security issues and events by monitoring network and systems data to ensure that directive and preventive controls have been followed.
- **Corrective Controls** — Checklists, procedures, and processes to take corrective actions comprise this phase. Incident response, remediation, and investigations are examples of our corrective controls.

Key Security Offerings

The information in the following sections provides details about the following aspects of Atos' security offerings:

- Technical Reviews and Recommendations
- Identity Management
- Network Security Service
- Intrusion Detection Services
- Penetration Testing
- Risk Assessment
- Vulnerability Management Service
- Incident Management
- Network Security Operations
- Endpoint Security

Technical Reviews and Recommendations

Atos actively reviews vendor solutions that address current security issues as well as future projected challenges. We evaluate solutions based on function, quality, fit, scalability and leveragability, procurement cost, and ongoing cost of ownership. Our clients frequently ask us to act on their behalf to ensure that security technology solutions and processes are compatible and scalable with their evolving needs. Atos provides sound, cost-effective security recommendations that take into consideration the following:

- Consultative understanding of business requirements and security objectives
- Industry best practices
- Data at risk
- Criticality of data or systems
- Existing environment and processes
- Maturity and stability of the solution and vendor

Identity Management

Atos understands the importance of identity management. Our approach includes a solution for enterprise security administration that will streamline the process for requesting, approving, and implementing changes for system access. This will incorporate our policies, processes, and procedures with an automated software utility that includes password synchronization, self-service reset, security policy enforcement, and self-service registration.

Network Security Service

Atos' network security service includes multi-layered security. Access lists and policy filters are used to prevent address spoofing, distributed denial of service (DDoS) attacks, Simple Network Management Protocol (SNMP) queries, Internet Control Message Protocol (ICMP) attacks and known malicious traffic associated with viruses, and traffic from illegal Internet

sources/Internet Protocol (IP) address space. The access lists and policy filters are modified, as needed, to help block or filter new security threats from the Internet. This layer also contains intrusion prevention systems, which further reduce the risk of attacks by automatically identifying and proactively stopping unauthorized access and malicious traffic, including worms and virus attacks.

Additionally, our Internet core perimeter firewall layer is designed to block default unwanted traffic. We take a "deny everything" approach to firewall management and open only those ports that are necessary for business operations.

Intrusion Detection Services

Our intrusion detection services include network intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS), as described in the following sections.

Network Intrusion Detection Systems

We provide in-band NIDS sensors to monitor inbound and outbound traffic through the Internet core network architecture. NIDS sensors are strategically placed within the network architecture to maximize their effectiveness. The NIDS sensor is configured to automatically alert on attempts against predetermined high-risk vulnerabilities. Our Security Engineering and Security Operations personnel update the NIDS sensors based on industry research, internal research, and industry alerts based on existing and emerging attack behaviors. Our Security Operations Center (SOC) personnel monitor NIDS sensors 24x7 for continuous monitoring of security incidents. Our SOC personnel provide Level 1 and Level 2 support on security incidents and Security Engineering personnel provide Level 3 support for heightened incidents. The parameters for service levels are mutually agreed upon by contract.

Host-Based Intrusion Detection Systems

Atos provides host-based intrusion detection systems (HIDS) for each Internet point-of-presence (iPOP). Standard service agreements include 24x7 SOC monitoring. Reports are delivered monthly to identified security and management personnel.

Penetration Testing

Our Security Engineering Group (SEG) manages a comprehensive threat management program based on essential information provided by the client. Atos' baseline security services include penetration testing for potential exploits or configuration errors that could allow an attacker to access, harm, or modify data being processed or stored on targeted systems. The SEG will recommend countermeasures for identified threats and will provide tailored threat awareness.

Atos leverages the Open Source Security Testing Methodology Manual (OSSTMM), as well as an array of assessment tools, to provide in-depth risk assessments of computer systems and networks that include data-gathering, penetration testing, IP address probing, port probing, and modem/remote access discovery and identification. An experienced Atos team will conduct an external assessment of the network to determine the overall defensive security relevance. Our goal is to evaluate the network's defensive security posture and

provide a roadmap toward securing external access. The team uses a combination of commercial and open source tools to provide a comprehensive and thorough assessment.

Atos recognizes that a wide range of Internet security requirements, threats, environments, and constraints must be addressed while still enabling the client to maintain transparent business functions. Atos' penetration testing methodology is based on proven advanced techniques for scanning and exploiting networks. The methodology consists of the functional areas shown Table 5.

Table 5. Penetration Testing Methodology

Methodology Phase	Description
Phase 1—Intelligence Phase	Consists of passive information gathering
Phase 2—Reconnaissance and Probe Phase	Consists of target definition and information-gathering tools and techniques
Phase 3—Attack and Toehold Phase	Consists of initial entry techniques and common misconfiguration exploits
Phase 4—Advance and Conquer Phase	Consists of root and administrator privilege rights and advancement techniques
Phase 5—Stealth Phase	Tools used to obscure an intruder's activities installed

Risk Assessment

Atos security engineers employ a systematic approach for conducting security risk assessments. This approach provides a detailed view of its current network security posture and enables us to provide sound, cost-effective recommendations on how to maintain and improve network security.

Atos Annual Security Risk Assessment

Atos will conduct an annual security risk assessment against the facilities and operations supported by Atos for the contract. The risk assessment is designed to assess the outsourcing environment's security posture against internal policies and procedures, contracts, and/or regulatory compliance requirements directly related to services provided by Atos. The risk assessment will assess and document administrative and technical security controls and processes delivered by Atos per the Master Services Agreement (MSA).

On completion of the assessment, the Atos Security team will provide a detailed report and gap analysis of findings, together with high-level technical recommendations for further remediation planning.

Vulnerability Management Service

Networks that will be connected to Atos' core infrastructure or those administered by Atos personnel undergo an initial vulnerability assessment (baseline) as well as ongoing vulnerability assessments. The Vulnerability Management process is a key component of our security services. Atos will configure the frequency of vulnerability assessments based on

the existing vulnerability management program, as well as critical business functions. Atos will establish this program as a monthly recurring process (as default). Additional scans may be conducted according to client needs.

Reports are provided to the authorized, appropriate parties responsible for the review and remediation of identified vulnerabilities. These parties are expected to resolve documented vulnerabilities in a reasonable and mutually agreed-on time frame. A feature-rich service enhances Atos' security capabilities. Features include the following:

- Discovers poorly configured devices
- Identifies the services running on each system assessed
- Provides tools to monitor for rogue servers and services
- Identifies Trojan horse programs
- Provides automatically updated baseline reports with every assessment
- Publishes new vulnerabilities daily
- Compares new vulnerabilities with the client's baseline profile
- Supports user-defined "Logical Division" report grouping and rollup—for example, by critical business function, geographic location, network, or machine platform
- Supports integrated accountability mapping for reporting and alerting
- Provides vulnerability filtering based on user-defined priorities

Each business unit performs the following tasks:

- Internet vulnerability scanning, using the Atos corporate standard for vulnerability scanning, as designated by the Office of the Chief Information Security Officer, to ensure that consistent and centralized monitoring of system vulnerabilities and weaknesses are identified
- Vulnerability scanning to be run on a monthly basis, scanning all Internet-facing systems and network devices to ensure that these systems are properly patched and configured
- Periodic vulnerability scanning on the LAN using either the Atos standard or similar tool, to ensure that systems and network devices are properly patched and configured

Each location will maintain a documented process identifying how all identified vulnerabilities will remediate within an acceptable minimum time frame based on criticality of exposure, impending risk to system resources and data, and contractual requirements, but not to exceed the following:

- All critical or high-risk security must remediate as soon as possible, but not to exceed one month from when either a patch is released from the vendor or the scan identifies configuration vulnerability.
- All medium-risk security vulnerabilities remediate in a timely manner, but not to exceed three months from when either a patch is released from the vendor or the scan identifies a configuration-based vulnerability.
- All low-risk security vulnerabilities or warnings are addressable providing that not deploying the patch or the configuration will not place the system at unnecessary risk.

Incident Management

Security incidents are addressed promptly and are resolved diligently based on the incident's severity and immediate threat to the network, systems, or data. Atos will create a custom solution to satisfy security needs and exceed service level expectations. The incident management services include the following:

- Incident response process (computer emergency and virus incidents response teams)
- Customer notification, escalation, and update
- Engage, hand-off, and verification with remediation team
- Root cause analysis (RCA) and incident investigations
- Policy review and recommendations

Network Security Operations

The Atos Enterprise Command Center (ECC) includes the Network Operations Center (NOC) and the SOC with personnel staffed 24x7 to monitor IDS sensors and address general security incidents (Level 1 and Level 2 support). Our Network Engineering and Security Engineering teams provide Level 3 support for non-standard incidents, as escalated by NOC and SOC personnel through incident response process. Security monitoring services include the following:

- 24x7 monitoring of IDS and incident response
- Alert update/notification on latest vulnerabilities affecting the environment
- Log review and analysis
- Reports provided as contractually agreed
- Advanced network security services

Endpoint Security

Atos uses industry best practices in the area of endpoint security services. We have the experience to support and manage several endpoint security applications, and the flexibility to do so. Our strategy for endpoint security includes the following:

- Weekly executive/detail reports
- Systems remediation
- Tickets opened/assigned, as necessary
- Products patched/updated, as necessary
- Available to assist with outbreaks; time billed separately
- Customer support for IPS/firewall/application blocking exceptions and log investigation
- System remediation with custom tools
- Direct management of virus outbreak resolution on a 24x7 basis

Security Management Controls Framework

Atos leverages standards-based regulatory policy controls, recommended best practices, and compliance with client-stated requirements for control of sensitive and private information. All policies and procedures are designed to comply with the ISO 27000 series, ITILv3, SAS 70 Type II, and SASE 16 compliance standards. We've developed a series of Atos exclusive security policies that supplement the guidance provided within ISO 27001 best practices. Atos reviews standards and controls annually, and we update these controls as regulatory and client requirements change. We also perform audits and assessments by third parties on an annual basis.

Anti-Virus/Anti-Malware

Our strategy for baseline endpoint security includes anti-virus, anti-spyware, anti-malware, and personal firewall protection. We'll provide weekly executive and detail reports, as well as systems remediation. Additionally, we patch and update anti-virus signatures as they become available, and manage virus outbreaks to resolution 24x7x365. We also recommend redundant, overlapping systems to ensure desktop systems are protected from virus infections.

Security Information and Event Management (SIEM)

We provide the Hawk SIEM platform to provide centralized log management services to simplify compliance programs and optimize the client's security incident management. The Hawk solution facilitates the automated collection, analysis, alerting, auditing, reporting, and secure storage of all logs. We believe that clients can simplify compliance by using regulation-specific, out-of-the-box reports, alerts, and correlation rules. Reports can be scheduled or run on an ad-hoc basis. Alerts are managed by the Atos SOC and integrated into the overall incident response capability.

Security Compliance Processes

The following information provides details on Atos' security compliance processes.

Information Security Policies

Atos' security policies are based on ISO 17799 2005 guidelines and policy development processes. Atos adopted the ISO 17799 2005 policy numbering scheme to facilitate ease of identification for employees and improve efficiency of audits. We've also developed a series of Atos Exclusive Security Policies that supplement the guidance provided within ISO 17799 2005 best practices.

Key Security Processes

Atos will implement key security processes to meet your specific needs, and we'll ensure that continued maintenance of these processes conform to your existing processes and standards. These processes are designed to be flexible and to strengthen the Lead State's

network and application security environment. The following information briefly describes our key security processes:

- **Incident Response** — Monitor the client's network, and track, research, and respond to security incidents; analyze incidents and look for trends and patterns; and produce management reports as necessary
- **Hardware/Software Support** — Maintain security hardware and software, including ensuring that appropriate backups are made and securely stored
- **Vulnerability Assessments** — Conduct ongoing automated network vulnerability assessments as a monthly process to identify vulnerabilities, analyze the results against the previous month, and distribute the results to appropriate site personnel for timely and continued remediation; these periodic assessments are necessary to ensure that network-attached devices continue to remain hardened against known and emerging vulnerabilities
- **Audits and Site Visits** — Perform annual security audits and site security compliance visits to ensure that security policies and best practices are followed
- **Network Security Architecture Reviews** — Assist with security reviews of network configurations and new equipment purchases as necessary across the client's enterprise
- **Penetration Tests** — Conduct penetration tests annually; more frequent and/or follow-up testing available on request
- **Status Meeting Representation** — Attend security-related meetings with client counterparts as requested and assist with the coordination of security issues
- **New Site Evaluations** — Conduct security evaluations for any new sites that are added to the partnership
- **Expand Knowledgebase** — Continue to monitor the security industry and attend training to remain current on the latest security threats, countermeasures, and technologies

Network Security Operations

Atos will provide primary network security monitoring operations from one of our ECCs. The ECC performs numerous network operations and security operations services, including the following:

- **Logging and Auditing** — The ECC monitors critical systems with auditing/logging capability for anomalies, system errors, and faults. The ECC responds to alerts and abnormal system activity with fault isolation and problem resolution. Sometimes, system anomalies indicate an attack or misuse of the required system. ECC personnel will escalate expected security issues to the Atos Security team for further analysis and, if required, incident response procedures.
- **Incident Management** — Our Incident Response and Crisis Management team is adaptable to given requirements. We determine the client's requirements and create a customized process for our personnel to follow based on requirement specifications. At a minimum, our baseline process includes the following activities:
  - Our ECC will take initial ownership of the incident when an incident originates from our automated tools.
  - Our ECC will coordinate the break/fix effort, including incident escalation procedures.

- Security incidents will be referred to our Security Operations and Security Engineering teams for response.
- The management and response levels are governed by the profile established.
- The Atos Security Engineering group will provide Level 3 support to the incident. This level is initiated when events require a senior network security engineer's direct involvement in incident resolution. During that time, ECC personnel and Atos' Security Engineering will work together to resolve the issue.
- Client personnel will be notified if the incident reaches an escalation level as defined in the given profile, and will be kept informed throughout the response process.
- The client will receive incident and status reports as required.
- Atos will deploy one emergency response team per year under the contract. This team will be airborne within 24 hours of notification and will remain onsite for up to three days. Additional response teams or time onsite is available on a per-incident basis. Pricing is available on request.
- Atos will keep the client advised of the incident status through resolution. This is accomplished by telephone contact, pager updates, and/or email, based on given requirements.
- Our state-of-the-art network management system (NMS) identifies the most critical problems, correlating downstream events to the root cause so that the Network Operations group is working to solve the problem.
- Atos ECC personnel monitor network devices and resolve standard network issues. Security-related issues are resolved based on the incident's severity, the given profile, and the immediate threat to the network or data. Atos will strive to create a custom solution that satisfies defined security needs and exceeds required service levels.

Organization Profile

ORGANIZATION AND STAFFING

7.1 (ME) CONTRACT MANAGER

The Offeror must provide a Contract Manager as the single point of contact for management of the NASPO ValuePoint Master Agreement, administered by the State of Utah. The Contract Manager must have experience managing contracts for cloud solutions.

7.1.1 Provide the name, phone number, email address, and work hours of the person who will act as Contract Manager if you are awarded a Master Agreement.

Name: Karan Chetal, Director—Client Services

Phone number: 914-733-5519

Email address: karan.chetal@atos.net

Work hours: 9am – 6pm Central Time

7.1.2 Describe in detail the Contract Manager's experience managing contracts of similar size and scope to the one that will be awarded from this RFP. Provide a detailed resume for the Contract Manager.

Atos has high standards for establishing formal Governance frameworks with our clients and a structured umbrella Account Management Office (AMO) is staffed with seasoned staff acting is various functional roles, all of which operate under the single point of contact (SPOC) who is the Atos Account Executive or Contract Manager. The Atos Account Executive acts as the SPOC and utilizes several supporting staff members to execute daily operations and maintain strong communications with our target client sponsors. A Service Delivery Manager, Financial Analyst and Reporting Analyst are traditionally housed within the Atos AMO fabric.

Karan Chetal Resume

Highly qualified service delivery manager with more than 20 years of IT experience. Extremely business-focused to meet contractual deliverables for clients with large and distributed environments. Strong ability to communicate in both technical and business environments to deliver continuous improvement of client services by fostering cooperation between systems support staff and client executive management. Excels in defining service level metrics, leading high-performing technical support for innovation and technology improvement for clients, and preparing status reports. Strong interpersonal and communication skills, and effective skill set in relationship management, strategic planning, operations management and quality improvement. Expertise includes the following:

- Strategic and tactical plan development and implementation
- Client relationship building
- Contract management
- Policy and procedure development (ITIL compliance)
- Global delivery model
- Quality improvement
- Process improvement
- New business development
- Finance/budget administration
- Proposal preparation

Account Executive at Atos, reporting to Chief Executive. Leading IT strategy and initiatives critical to achieving corporate goals. Working across verticals and the public sector to grow the footprint of Professional and Consulting services.

Senior Executive at UST Global, reporting to the President. Leading IT strategy and other initiatives critical to achieving corporate goals. Practice includes Media Entertainment, Healthcare, Manufacturing, and Energy/Utilities verticals.

Account Executive at CapGemini. Planned/executed business and operations strategy as a member of the executive team reporting to the CIO. Re-engineered IT organization to strengthen the quality of service, ensure timely delivery, and develop staff capabilities while improving reliability and reducing costs. Controlled annual $100 million budget per Client.

Senior Business Operations Executive at HCL reporting to Senior Vice President. Led innovation development and internal operations. Managed strategic account with client engagement services and solution implementations.

7.1.3 Describe in detail the roles and responsibilities of the Contract Manager as they apply to the NASPO ValuePoint Master Agreement that will be awarded from this RFP.

Atos anticipates the NASPO will supply individual task orders and request specific solutions that will be self-contained within a respective SOW or addendum for fulfillment by Atos. Unless specifically stated with the SOW, the terms and conditions within the MSA shall apply to services provided. Adherence to any stated restrictions or terms specially crafted within a respective SOW will be managed by the Atos Account Management Office working in conjunction with the designated NASPO entity sponsor or assigned Liaison.

The actual Atos Cloud solutions and services related engagements will be delivered to various NASPO entities using a Statement of Work (SOW) or addendum to the MSA which clearly stipulate the price, scope of effort, deliverables, timelines and associated acceptance criteria.

As part of the formal RFP process initiated by NASPO, Atos will conduct a thorough legal review of the Master Services Agreement. Upon joint contractual agreement of the terms and conditions stated within the MSA by both parties, this shall be the overall governing contract for any services delivered.

The Atos Account Management Office (AMO) team would provide on-going interaction with a participating NASPO entity on monthly, quarterly and annual review cycles. The matrix below illustrates typical interaction and outputs for these targeted meetings.

Governance Reports	
Report Name	**Description**
Executive / Management Reports	
Quarterly Business Review	Quarterly summary of Service performance including: performance against Service Levels; highlights of Service delivery; status of major Service issues; major Project implementation status. Quarterly summary of strategic relationship performance including: NASPO business updates; Supplier business updates; new initiatives; and challenges/obstacles/opportunities.
Executive Summary Scorecard	Summary of: Service performance against Service Levels; highlights of Service delivery; status of major Service issues; and Project implementation status.
Annual Scorecard Performance Summary	A dashboard summary of key performance metrics and their attainment showing performance trends, Service Level defaults, credits and improvement plans by Service Delivery Tower.
Issue Tracking Reporting	
Monthly Issue Management Report	A report providing monthly counts of logged, resolved and open issues. This report shall also contain summaries of root cause analysis results from the prior month and root cause analysis ongoing activities for issues affecting the Services.
Monthly Trend Issue Management Report	A report providing monthly trends of logged, resolved, and open issues.
Satisfaction Survey Reporting	
Executive Customer Satisfaction Survey Results	The results of an annual customer satisfaction survey for applicable BD managers and executives on their satisfaction with Supplier's performance in delivery of the Services.
Point-of-Service Customer	The results of the point-of-service customer satisfaction surveys

Governance Reports	
Report Name	**Description**
Satisfaction Survey Results	conducted over the period of a month.
Annual End User Customer Services Satisfaction Survey Results	The results of the annual End-User customer services satisfaction surveys conducted.

Technical Response

This section should constitute the Technical response of the proposal and must contain at least the following information:

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

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

Offeror's should focus their proposals on the technical qualifications and capabilities described in the RFP. Offerors should not include sales brochures as part of their response.

Atos will provide a pre-integrated, pre-tested, pre-validated, fully managed, highly available, and automated cloud infrastructure. This proven infrastructure offers trusted performance with scaling and trusted availability under high workloads, and trusted cloud security for business-critical data. Atos Cloud services provide a trusted first step into the cloud, where you can cloud-enable all your enterprise applications, with both a virtual and physical cloud environment.

Atos also will provide required Internet access and can provide back-end network access for the Lead State or the Participating Entities. Some Participating Entities may require provision of their own network access, which Atos can accommodate.

Atos can provide data centers as required and is committed to being a leader in environmentally responsible data center services. This strategy is at the heart of the Atos data center roadmap, shown in Figure 1. Atos has been recognized since 2011 as a leader in the IT sector for sustainability.

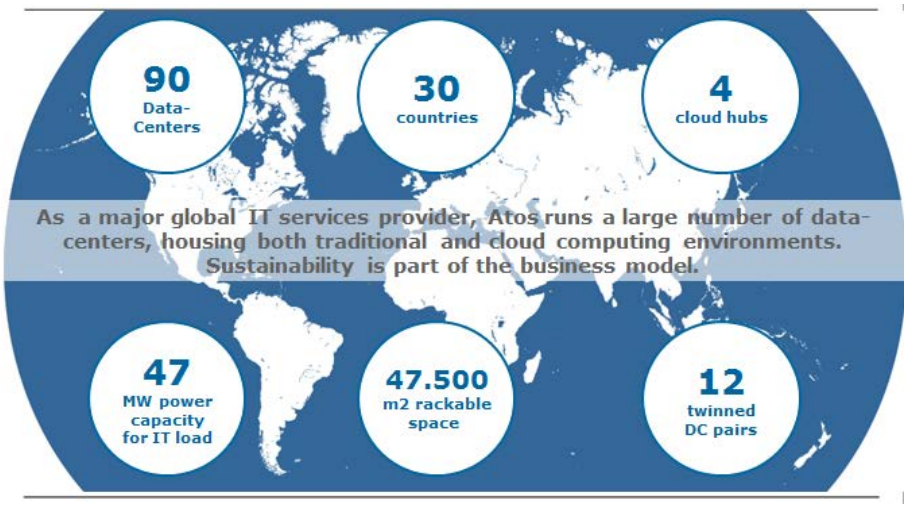


Figure 1. Globally, Atos' 90 data centers are located in 30 countries.

Atos offers dynamic scalability, providing the Lead State with highly flexible consumption of compute and storage resources for seasonal business demands and volatile business, as well as production transfers, year-end closing, and more. Dynamic scalability also enables rapid elasticity, allowing on-demand resizing of resources, and scale-up or scale-down for peak workloads. The Atos solution also has the unique capability to enable applications to automatically scale up and down without human interaction based on a predefined policy and workloads.

The Atos Cloud provides intuitive dashboards, views, and reports which help align IT spending with business priorities by getting full transparency of infrastructure and application cost and service quality. Usage metering provides the requisite transparency for both the provider and consumer of the utilized service for use in dashboards, reports, and "bill of IT."

Atos has a full complement of cloud-based solutions and services. For the purpose of this RFI response, Atos has elected to align with your stated categories for alignment. Figure 2 represents solutions available for adoption by the Lead State entities. Atos' cloud services and offerings include the following:

- Automated discovery of compute and application landscapes
- Cloud consultancy and readiness assessments
- Cloud architecture design and deployment services
- Infrastucture2Cloud assessment, planning, design, and migration services
- Hybrid cloud adoption and transformational services
- SaaS integration design and deployment services
- Public Cloud adoption strategy assessment, planning, and transition services
- Cloud application assessment and transition services
- Cloud application workload migration and implementation services

Atos Cloud Solutions

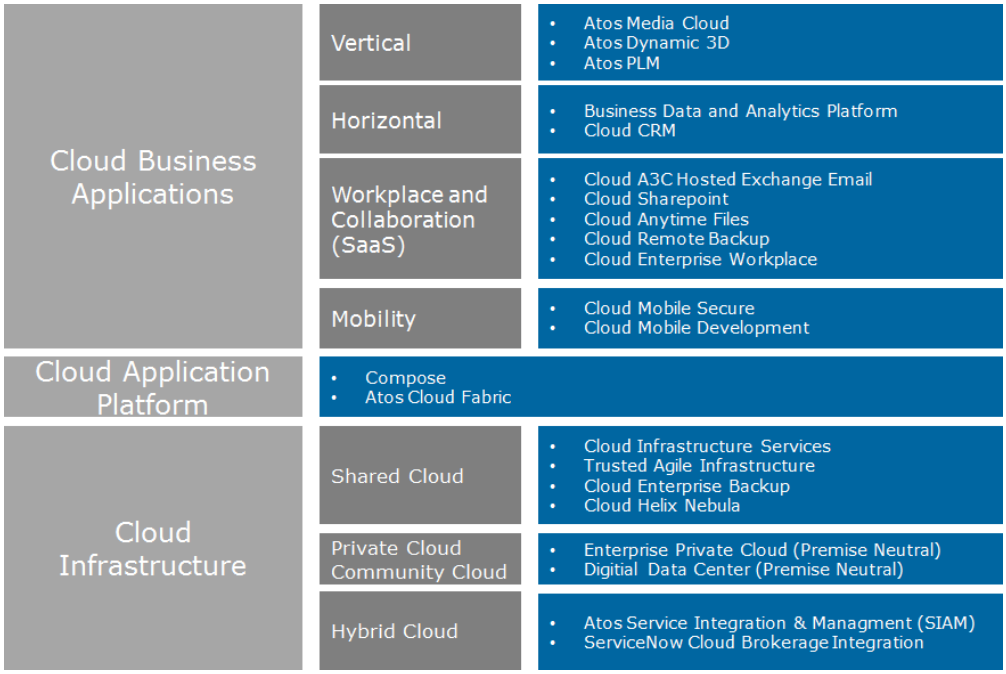


Figure 2. Atos Cloud Solution Matrix

TECHNICAL REQUIREMENTS

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

If an Offeror's proposal contains more than one Solution (i.e., SaaS and PaaS) then the Offeror must provide a response for each Solution. However, Offerors do not need to submit a proposal for each Solution.

8.1 (M)(E) TECHNICAL REQUIREMENTS

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.

Atos will provide the following to Eligible Users:

- Cloud Service Models
  - Infrastructure as a Service (IaaS)
  - Platform as a Service (PaaS)
  - Software as a Service (SaaS)
- Deployment Models
  - Private Cloud

- Community Cloud
- Public Cloud
- Hybrid Cloud

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:

Atos understands the requirement for a standardized approach to the cloud environment; therefore, Atos' portfolio of cloud-based offerings being proposed in this document all comply with NIST Special Publication 800-145 definition for Cloud Computing.

Please refer to Sections 8.1.2.1 thru 8.1.2.5 for further clarification.

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.

Atos complies with the Lead State's NIST Characteristic - On-Demand Self-Service requirements and provides a cloud solution that is built on a foundation for self-service, a single platform for all service requests, automation of server provisioning, and the associated approval process, which ultimately simplifies traditionally complex business processes. A user can provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

Atos will provide a cloud self-service portal, which is the customer's single point of entrance to the solution. It provides the Lead State or the Participating Entity with the ability to interact with the environment in the following ways:

- Create user accounts for all customer users who need to interact with Cloud Services, associated with the customer's own authentication services
- Determine tenant roles for administration, business, and approval tasks within the portal
- Split the customer's environment into multiple resource pools in the form of separate tenants and business groups
- Define new blueprints (within the relevant organization/tenant)
- Trigger all Cloud Services standard service requests, with awareness of customer tenant resource pool, data center location, network security zone, and capacity type
- Provide real-time overviews of the production environment

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.

To ensure that the NIST Essential Characteristic – Broad network access is satisfied; Atos provides multiple network connectivity options to its cloud infrastructures:

- Dedicated connectivity to client network(s) – establish network connectivity to the client network based on an agreed network design
- Supplier connection to supplier support network – provide secure VPN-based connectivity over the Internet
- Dedicated Internet connectivity – provide and connect a client-dedicated DMZ security zone to the Internet

Atos works collaboratively with clients to design and approve network connectivity plans to ensure any and all security compliancy is met.

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.

To ensure that the NIST Essential Characteristic – Resource Pooling is satisfied, Atos abstracts the compute (CPU and memory), storage, and networking components into resource pools using Software Defined Data Center (SDDC) technologies, such as VMware's vSphere, vSAN, and Distributed Switching.

Dependent on the cloud deployment model being utilized, and the security compliancy required, Atos can provision resources from either a dedicated or shared set of pooled resources, from either within an Atos data center or a public cloud provider (e.g., AWS, vCloud Air, Numergy, etc.).

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.

To ensure that the NIST Essential Characteristic – Rapid Elasticity is satisfied, Atos provides the capability and capacity within its cloud environments to rapidly scale up and down within pre-agreed billing cycles and prescribed limits, to ensure that workloads can be provisioned and decommissioned, in a timely and agile manner, to meet the client's business needs.

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.

To ensure that the NIST Essential Characteristic – Measured Service is satisfied, Atos uses technologies, such as VMware's vChargeback, for the billing of consumed resources within its cloud environments. Additionally, a set of industry-standard monitoring and reporting tools provide support information to ensure that Atos' cloud environments are available to

meet clients' SLA requirements and to generate a set of either standard (Availability, Utilization, etc.) or client-specific reports.

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.

Atos' portfolio of cloud offerings to be proposed as part of this RFP submission will be as follows:

- Infrastructure as a Service (IaaS)
  - Dedicated Private Cloud
  - Shared Private Cloud – Single Tenant
  - Shared Private Cloud – Multi-Tenant
  - Hybrid Cloud Brokering / Orchestration
- Platform as a Service (PaaS)
  - Virtualization / Provisioning of Legacy Applications / Workloads
  - Provisioning of Cloud-Ready Applications / Workloads
- Software as a Service (SaaS)
  - Collaboration SaaS offering – email, SharePoint, etc.
  - Business Productivity SaaS offerings – File Backup and Archiving
  - Customer Relationship Management (CRM) SaaS offering
  - Product Lifecycle Management (PLM) SaaS offering
  - Security SaaS offerings

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

Atos is fully willing to comply with the requirement of Attachments C & D.

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.

Atos' cloud-based offerings (IaaS, PaaS, and SaaS) fully adhere to all of the categorizations and requirements outlined in Attachment D.

8.2 (E) SUBCONTRACTORS

Offerors must explain whether they intend to provide all cloud solutions directly or through the use of subcontractors. Higher points may be earned by providing all services directly or by providing details of highly qualified subcontractors;

lower scores may be earned for failure to provide detailed plans for providing services or failure to provide detail regarding specific subcontractors. Any Subcontractor that an Offeror chooses to use in fulfilling the requirements of the RFP must also meet all Administrative, Business and Technical Requirements of the RFP, as applicable to the Solutions provided. Subcontractors do not need to comply with Section 6.3.

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. do not need to comply with Section 6.3.

Yes, Atos intends to provide all Cloud Services directly except for any services that the State of Utah wishes to procure from other providers such as Amazon (AWS), Microsoft (Azure) or other vendors.

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.

As part of the Master Services Agreement (MSA), and outlined within a specific Addendum or Exhibit inside the MSA, Atos will identify any associated subcontractors expected to participate in our overall solution framework, the service provided, and the given percentage of their involvement within a respective solution or service delivery.

Atos leverages proven industry-recognized and mature subcontractors in support of a given solution set. Atos establishes formal contracts directly with any identified subcontractor and outlines stringent Service Level Agreements (SLA) in order to control performance. Any subcontractor leveraged is continually monitored and managed against stated SLAs, and their respective performance is closely scrutinized by Atos to the highest standards.

Historically, Atos will capture and triage performance issues related to a provided service using an agreed upon service desk process and Level 1 ticket capture and routing sequence. If the event of non-performance or degraded service by a subcontractor, Atos will take ownership to identify the root cause and either rectify the issue or replace with another qualified provider, thus shielding the Lead State from direct involvement.

Additionally, Atos assumes overall responsibility for subcontractor performance execution for our solution sets, including reporting measures that are jointly agreed upon with the Lead State or Participating Entity. The assigned Atos resources operating within the Account Management Office (AMO) make extensive use of Action, Issue, and Risk (AIR) logs associated with subcontractors on a continual basis to proactively manage performance to provide execution transparency into our clients.

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.

Atos partners with a variety of industry-leading suppliers and experts in multi-vendor environments to develop and deliver a broad scope of solutions for our clients. We put our vendors and partners through a rigorous evaluation process to ensure quality; they're chosen based on the best fit between their capabilities and the solution's requirements.

Additionally, in our contracts with the State of Texas; Orange County, California; and the City of San Diego, we have implemented two multi-source delivery models and one that has implemented a third-party integrator.

We adopt a collaborative team approach based upon our proven governance framework to promote ongoing engagement between all parties. This approach helps ensure clear and timely communication and a productive working relationship, all driven by client-centric results and accountability.

Our governance model applies structured communication processes and escalation procedures to enable us to seamlessly manage the interfaces between all involved parties. We enable integration across the IT operations level for delivery effectiveness and operational efficiency, and the business operations level to provide a "one IT" view to the organization. This multi-level integration eliminates silos of management teams while maximizing synergies across functions.

Our multi-level, collaborative approach and governance model help mitigate many of the common challenges inherent in delivering a shared portfolio of IT services while maximizing cross-functional synergies. We typically mitigate the following challenges through our governance approach:

- Lack of SLA visibility—In the absence of an integrated service management office, the client may experience a situation where all the vendors are green on their SLAs, but the net outcome of IT to the business is unsatisfactory. This arises due to lack of existence of and governance over the end-to-end SLAs.
- Differing organizational cultures—We work with all parties involved to find a common platform, understand the perspectives of other organizations and people, and ensure that the overall client objectives are met effectively.
- Distinct processes and procedures—The internal processes of various vendors need to be aligned with best practices across the ecosystem. As part of our governance activities, we ensure that this methodology is agreed upon by all stakeholders involved in the engagement.
- Incompatible systems and applications—The systems, infrastructure, applications, and hardware used by various vendors must be compatible and agreed upon by all stakeholders involved in the engagement.
- Protection of intellectual property—Sharing and managing intellectual property is another major challenge in a multi-vendor environment, and is managed by ensuring that all parties respect and adhere to NDAs, confidentiality, and IP ownership.

Our accountability-driven, performance-based approach enables operational excellence and customer intimacy, leading to successful long-term client relationships.

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;

The Computer Security Incident Response Team (CSIRT) team analyzes potential incidents and determines their severity, priority, and what activities to undertake to mitigate the threat. The security incident response is shared and delivered as a service based on shared resources and the follow-the-sun principle. The following tasks comprise a security incident response:

- Solve the incident
- Limit damage
- Identify initiator
- Develop a recommendation
- Communicate each time it's needed, and escalate thanks to the customer-provided escalation matrix
- Create the final report

Based on a full service delivered by Atos, Figure 3 shows the Security Incident Response process and possible scenarios with customer-owned service parts.

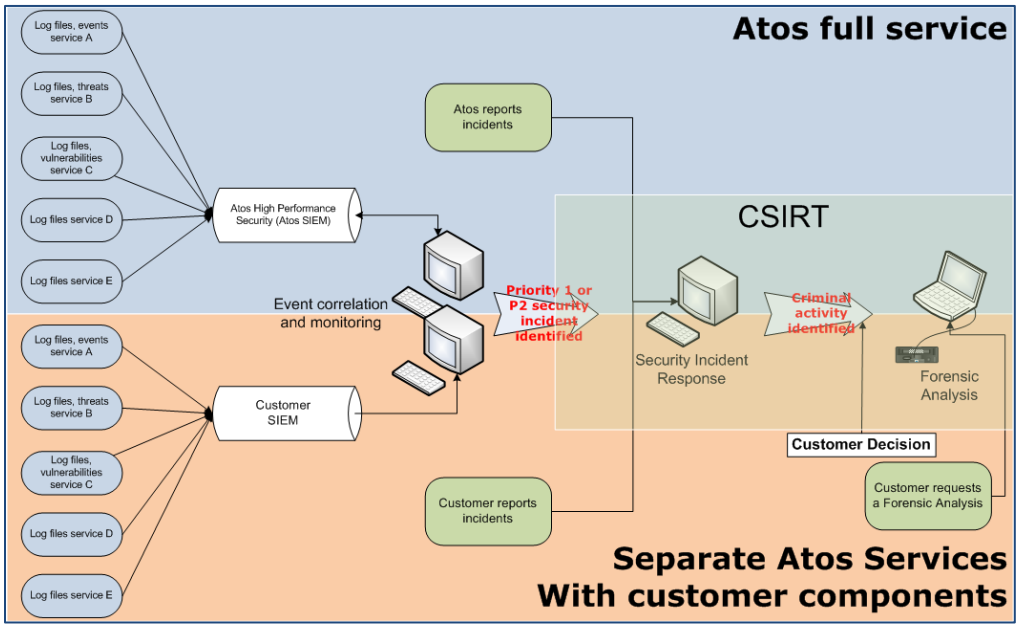


Figure 3. Security Incident Response Processes

Security Incident Response Service - Dedicated

For the dedicated Security Incident Response service, Atos delivers the same shared functionalities as listed in the preceding section. Additionally, with the dedicated service, Atos delivers dedicated analysts to investigate your security incidents.

Additional Security Incident Response services, such as EnCase Analytics, Cyber Security, and eDiscovery, also are available.

Forensic Analysis – Remote

The CSIRT is able to perform forensic investigation that includes gathering and examination of data in order to recover and investigate material found in digital devices. Within this service, only open-source analysis tools are included.

The customer identifies the suspected devices and hands over all necessary documentation, such as network topology and infrastructure details relevant to the incident, to Atos.

The remote forensic analysis tasks are as follows:

- Acquire data from disk or RAM; e.g., documents, images, email, webmail, Internet artifacts, Web history and cache, HTML page reconstruction, chat sessions, compressed files, backup files, encrypted files, RAIDs, workstations, servers, and smartphones and tablets
- Give complete endpoint visibility
- Store all captured evidence in court-accepted evidence file formats
- Recover files and partitions, detect deleted files and password protected files, perform file signature analysis, and hash analysis, even within compounded files or unallocated disk space
- Preview of results by examiners while data is being acquired
- Allow users to create custom scripts to help them automate time-consuming investigative tasks, such as searching and analyzing specific document types or other labor-intensive processes and procedures
- Generate reports

Forensic Analysis – Remote with Encase

Within this service component, Atos provides remote analysis with the “dead-box” stand-alone forensic tool from Encase; the software license is included in the service. With this type of analysis, the customer is responsible for installing the product, or must provide instructions for Atos if Atos is the full managed service provider. The installation of the Encase component should be done at the beginning of the project because if the system is infected, installation isn’t possible. The interaction between the customer and forensic analyst is very important since the analyst needs access to the suspect customer device to collect the evidence.

Forensic Analysis - Onsite

When it is not possible to use remote forensics, Atos sends an expert onsite to investigate the forensic case. We offer this service on-demand or per monthly fee if the customer wants a predefined number of onsite forensics per month. The SLA is the onsite arrival of the expert in two business days for P1 cases, after Atos receives the forensics request. The expert will save the evidence, and analyze and investigate the saved data at a later time.

Benefits

Atos' Security Incident Response service provides the following benefits:

- Atos supports customer business with well-trained experts that have up-to-date knowledge from collaboration with our strategic partners and are available 24x7 following the sun.
- Atos is your single point of contact and has relationships with national Computer Emergency Readiness Teams (CERTs); we will make national and international security guidelines and regulations transparent to you.
- A dedicated Atos "customer security officer" can be nominated to be your main point of contact to Atos Global CSIRT.
- Our three CSIRT competence centers interact with local security officers to understand local rules and regulations, and customer-specific business information.
- For EMEA and LATAM, we have existing relationships to local CERTs in France, Germany, Netherlands, Belgium, Luxemburg, Russia, and Brazil.
- The Atos CSIRT is closely connected to all service delivery units to rapidly identify potential risks and limit the impact of security breaches.
- Our customer can decide how to best react based on the information we deliver from our Threat Management Service about vulnerabilities, threats, and advisories that have influence on the infrastructure.

An incident response plan will be documented and available for the Lead State; Atos will comply with notification SLAs. The Lead State's IT security personnel will be given direct access to interact with Atos engineers and management during the full life cycle of each security incident, and after-action reports will be distributed. To ensure successful management and delivery of services, Atos will establish an AMO for service delivery to oversee and manage the execution of support services and to direct continuous improvement activities related to these services. The AMO responsibilities include administering and streamlining operational and change management processes, as well as comprehensive reporting and communication.

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.

Atos has more than 20 years of experience in protecting Internet mail gateways, as follows:

- 100+ Internet mail gateways worldwide in operation
- 700,000+ mailboxes based on Exchange and 12,000+ mailboxes based on Notes

- 12,000+ Windows servers, several terabytes of storage devices, and 10,000+ mobile devices

Atos' Malware Scanning Services focuses on providing a secure and reliable email service. Extensive scanning of malware—in combination with a number of spam filters at the gateway(s)—protects systems and the business itself.

The service is based on a modular structure. Clients can buy a basic service and then opt for additional security functions based on the business's security requirements. The Internet communication gateway—i.e., the mail relay / mail gateway—defines the basic module. Additionally, the Lead State has a choice of the following optional services:

- Spam protection
- Virus protection messaging content (includes Web reputation module)
- Alias management
- Encryption mail-traffic
- User-based quarantine
- Optional service report

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

In addition to Production application environments, Atos' Cloud environments can host Test/Development/UAT/Staging environments, as required.

Atos' Agile infrastructure can provide a pool of compute, storage, and network resources to the virtual data center layer. This give control to client users to provision and manage their own server installations enabling them to reduce time to market and increase agility when provisioning or decommissioning non-production workloads.

Application "blueprinting" through Atos' PaaS offerings enable clients to prepackage workload components and rapidly deploy them across multiple clouds at the click of a mouse.

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

Atos full acknowledges this requirement and will comply as requested with / to this policy as outlined.

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

Atos fully acknowledges this requirement and is fully cognizant that the multiple browsers are leveraged by end users within the industry today; we will comply as requested with / to this directional guidance as outlined.

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.

Atos understands the importance of dealing with personally identifiable information (PII), and our comprehensive solutions are fully compliant with PII, HIPAA, PCI, and other related federal and industry requirements. Prior to the execution of an SLA, Atos will meet with the Purchasing Entity to determine whether any sensitive or personal information will be stored or used by Atos. Any such information stored or used by Atos is and will be subject to any law, rule, or regulation providing for specific compliance obligations.

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.

Our services are implemented using a multi-phased approach including development of strategy, roadmap, project plan, deployment approach, and operational readiness. Our Project Services Subject-Matter Experts and Project Managers will follow our service delivery methodology as we work with customers to implement the various technologies needed. In situations where customers look to implement multiple technology solutions, we will combine and streamline efforts to ensure multiple technology disciplines are assigned to the appropriate Subject-Matter Experts.

Figure 4 - Service Delivery Methodology

Core services include:

- Advisory strategy/roadmap, architecture, integration, Proof-of-Concept (PoC) and production deployment
- Design, integration, and implementation of Software-Defined Network and Storage solutions to extend virtualization across the infrastructure
- Design, integration, and implementation of Automation & Orchestration tools and best practices to create an operational framework
- Integration recommendations for operational readiness, processes, and workflow requirements to support requirements.

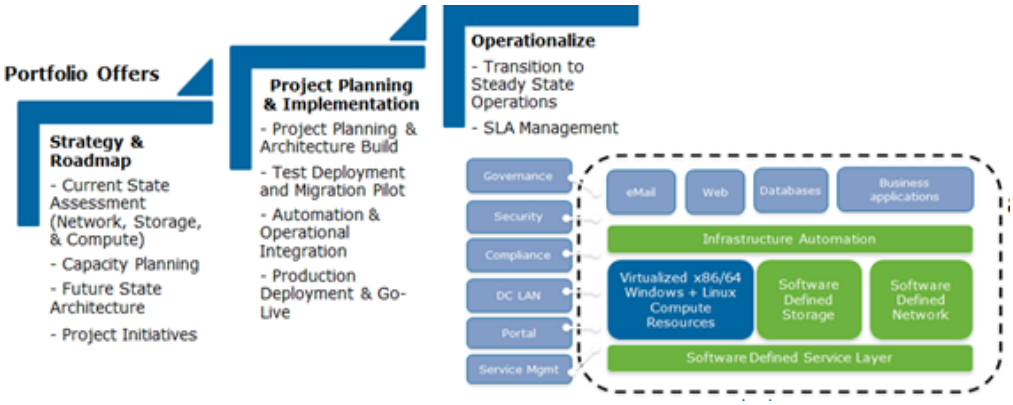


Figure 5 - Atos SDDC Project Services

Readiness Services

The Atos approach starts with a Framework Readiness Service to understand what is required to build the environment. A Current Mode of Operation and Future Mode of Operation design are developed to create your roadmap.

Basic Services	Optional Services(s)
Mandatory Modules provided by Atos	**Optional Modules provided by Atos**
▸ *Software-Defined Framework Readiness Services* ▸ *Setup,* Assessment, Strategy, & Roadmap ▸ Technology Review & Project Setup / Kick-Off ▸ Assessment of current state and readiness for SDDC ▪ Business Alignment ▪ Data Collection ▪ Hardware Readiness ▪ Application Readiness ▪ Infrastructure Readiness ▪ Operational Management ▪ Requirements Specification ▸ Current Mode of Operation / Future Mode of Operation ▸ High level design recommendations	▸ Physical Data Center Readiness Service ▸ Assessment & Gap Analysis of Physical Readiness ▸ Current Mode of Data Center Architecture Review ▸ Current Hardware & Software Inventory ▸ Innovation and strategy workshops ▸ Automated data collection ▸ Roadmap of technology innovation

Figure 6 – SDDC Framework Readiness Services

Infrastructure Services

Our Services provide our customers with a comprehensive approach to assessing, architecting, building, deploying, and integrating an architecture to fit your desired business and IT priorities. These services are designed to provide you with the base implementation that fits your needs. Since every environment is different, our full set of capabilities is flexible to fit your desired outcomes.

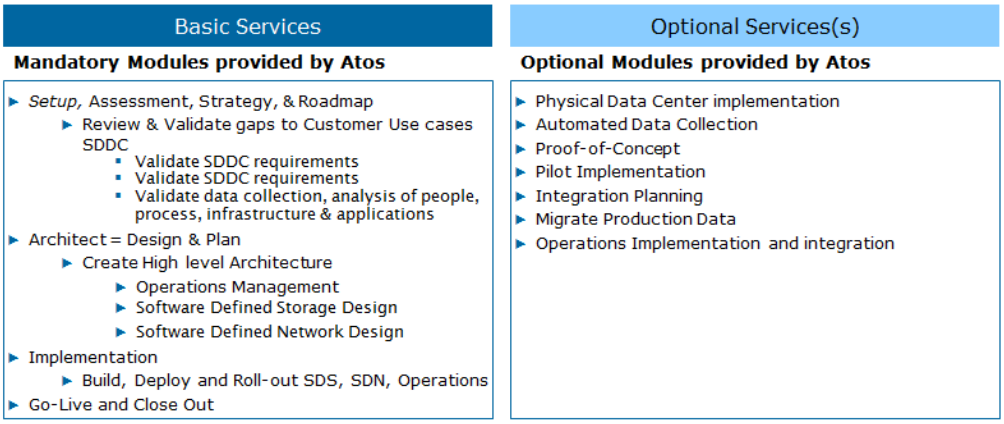


Figure 7 – Software-Defined Infrastructure Services

Automation & Orchestration Services

Once we have a deployed an Infrastructure, we provide the necessary services to integrate the core components. With our Automation and Orchestration services, your processes are streamlined for efficiency, automated for simplified operational management.

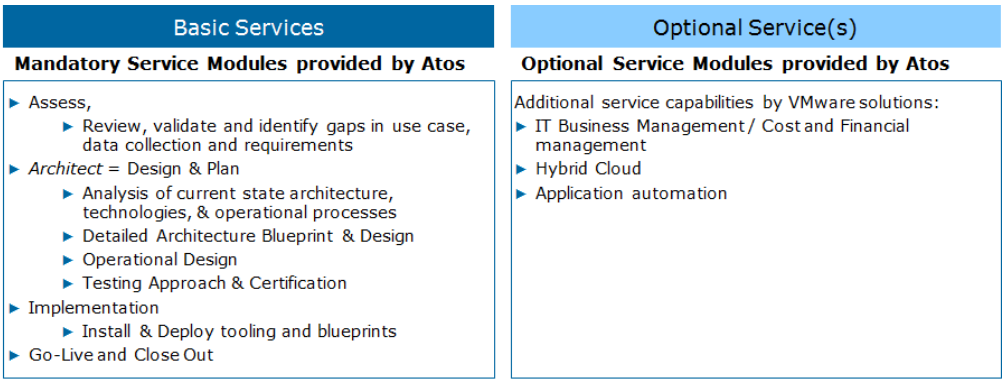


Figure 8 – Automation & Orchestration Services

Optional Services: Application Automation Services

Application Services provides all the activities and processes required to deliver a consumable ready, multi-tier application. These services will:

- Streamline the design process by assembling applications from pre-built components using a visual canvas with a drag and drop interface.
- Rapidly deploy infrastructure and application services with standardized, consistent configurations across hybrid clouds.
- Accelerate workload deployment by leveraging a library of out-of-the-box content and investments in existing configuration management tools

This service is optional as it provides the most advanced features in the maturity model. Implementation will be dependent on customers' readiness to deliver and consume applications in this manner. To achieve this level requires a thorough planning effort complete with application workflows and dependency mapping. Often this effort can involve multiple application owners, business process mapping, and significant time requirements.

8.4 (E) CUSTOMER SERVICE

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

- **Quality assurance measures;**

LEAN Six Sigma was deployed at Atos in April 2003. LEAN Six Sigma for Services (LSSfS) differs from Six Sigma in that it integrates LEAN tools or Speed tools into the proven Six Sigma methodology, specifically targeting waste in processes. This initiative is the enabler to implement process improvements identified from any of the tools and methodologies we use in our quality program. Our clients have realized many direct benefits; some examples include the following:

- A 5 percent increase in all call resolution (ACR) through a project to improve service desk resolution rate in which an internal agent-created software tool was deployed throughout the service desk.
- A reduction in wait time of two hours per administrative ticket was achieved through a project to reduce the time and the client rework of re-entering information into their call ticket system. Wait time resulted in less than 30 seconds, and some client rework was eliminated.
- Development of a quality survey instrument for a client to use internally was created through a project led by an Atos Six Sigma Master Black Belt. In pilot, it proved a more than 30 percent increase in response rate from previous surveys.

LSSfS is proven for making lasting process improvements that result in an efficient delivery of services to our clients' users. LSSfS is dependent on our efforts to meet our clients' critical-to-quality requirements. We understand that these are not only defined as contract or service level requirements, but also held within the expectations of our clients' end-user community. LSSfS is not only used in Atos as a process improvement methodology, but it's also the way we do business. Since the implementation of LSSfS, we've been undergoing a culture change that enables us to be a more client-focused, fact-based, data-driven organization.

At Atos, LSSfS is the learning and development process that provides employees at all levels with the tools and techniques to undertake a major improvement effort to enhance our abilities to meet client needs, improve processes, and drive our market share.

Commitment to LSSfS

Atos worldwide has been an early adopter and promoter of Six Sigma. The Atos approach of leveraging LEAN plus Six Sigma has been disseminated throughout Atos globally. To date,

we have applied this key practice as a tool to improve our own internal business and our client environments.

Atos allocates a significant amount of investment each year into expanding our LEAN Six Sigma practice. Currently, Atos in the United States has two Master Black Belts, nine Black Belts, and 42 Green Belts.

Key Benefits

Adoption of Six Sigma has led to the following key culture change benefits:

- Significant increases in client satisfaction
- Improved cost positions to maintain and assure competitive edge
- Involving people in the process to define solutions (solutions stick)
- Better use of data to drive decision making and improvements
- Data providing the real issue; no longer wasting time on things that do not matter
- Structured methodology drives better/quicker business decisions
- Management oversight via the tollgate process ensures accomplished goals
- Allows employees at all levels to contribute to continuous improvement projects, which increases empowerment

Highlights of Six Sigma Initiatives

The implementation of LEAN Six Sigma has enabled us to realize internal benefits in the following areas:

- Increasing capacity by eliminating non-value-added work out of network services administrators' daily activities
- Eliminating duplicate work by refining the network services alert process to ensure that network failures only send one alert instead of multiple
- Reduced cycle time of summary invoicing process; project resulted in an 18-hour process reduced to less than five minutes
- Reduced average time in queue for Network Services administrative tickets from 7.2 hours to 2.5 hours
- Eliminated 50 percent of client false network alerts, improving the defects per million opportunities (DPMO) from 718,000 to 44,600 (72 percent to 4 percent)

All benefits achieved through the projects listed will allow for more efficiency internally resulting in a lower cost of service and less variability in our processes for our clients.

Value of LEAN Six Sigma for Services

Besides the value gained from the specific project examples listed, being supported by a Six Sigma company enables Atos clients to feel confident that we are proactive with improving our services and processes. Our clients receive the following other direct benefits:

- Gain invaluable insight from Atos as to how they view and use our products and services. This benefit gives Atos the ability to prioritize and focus our improvement

efforts where they will be most effective and have the biggest positive impact on our clients.

- Process improvement allows for lowering operating costs; we will be able to offer the best solution at the lowest possible cost.

Our expertise and real-world experience enables us to be a trusted advisor to our clients, helping them improve and streamline existing integrated processes. The result is fewer process defects, which can lead to a reduction in operating costs and improved response to growth.

- **Escalation plan for addressing problems and/or complaints; and**

Escalation is a critical part of service delivery in appropriately addressing extraordinary events happening, and the associated governance procedures to be adhered to. Of particular urgency is governance in escalations relating to SEV 1 incidents. We establish a SEV 1 Incident Team that will execute SEV 1 resolutions and according escalations in alignment with the provisions made for the Situation Management Team. The roles definition and RASCI of the SEV 1 Incident Team will be detailed as part of the Operations Manual as one of the transition deliverables.

Atos understands that there could be SEV 1 incidents within and outside of working hours. The major incidents are defined by the priority/severity of the incident being handled. In such scenario, the service delivery manager is automatically notified of all SEV 1 incidents. The incident manager will act as or nominate a SEV 1 incident manager, coordinate resolution activity between all relevant groups, and communicate progress updates to the Lead State and Atos stakeholders. If a SEV 1 incident occurs, Atos will perform the following:

- Take responsibility for the management and resolution of the incident, in accordance with the agreed service levels
- Designate a member of the service management team as the SEV 1 incident manager
- Focus on the provision of an appropriate work-around, in recognition of the importance of avoiding or reducing the duration of any interruption to users
- Ensure that the agreed escalation/communication procedure is followed
- Keep the affected users and stakeholders informed of the status of the incident and on the availability of work-arounds until the root cause is addressed
- During the incident, record a time line of events in the service management toolset, which will then be used as the basis of the major incident report
- Confirm with the Lead State's nominated contact(s) that the incident is closed
- Document and issue the major incident report for review by the Lead State
- Propose any required service improvement actions, for agreement with the Lead State; these will be tracked within the "service reviews"

Atos communication and escalation procedures alert senior staff in both (all) involved organizations when a SEV 1 incident is recorded, usually via multiple simultaneous channels (SMS, email etc.). Channels will be agreed with the Lead State at the appropriate time during transition. In responding to a SEV 1 incident, resolution times will be foreshortened and appropriate activities initiated (e.g., business continuity). The frequency of client

contact will be increased in line with the communications plan and escalation procedures as specifically agreed with the Lead State.

Atos' client management structure puts the Lead State at the center of our business philosophy. All new initiatives are qualified by evaluating the benefits to the Lead State. The AMO executive, working directly with the Lead State, becomes the conduit through which you take advantage of Atos' technical resources. Specifically, the AMO executive provides the following services:

- Individual attention—To better serve your needs and help map future plans, the AMO executive spends time meeting and interacting with your personnel and other key individuals in your company. The AMO executive becomes familiar with your environment, and gains an understanding of the systems and their importance to you. AMO executives also conduct onsite orientations to educate employees on the effective use of Atos' services. Additionally, they educate Atos employees about your environment, personnel, and IT objectives.
- Focal point for ongoing concerns—Although the Atos Service Desk resolves daily system, network, and operational problems, the AMO executive is the focal point for ongoing questions, concerns, and issues. If the AMO executive is unable to respond with an answer, he or she knows who to contact to resolve an issue.
- The Lead State advocate—The AMO executive represents your interests within Atos. This person facilitates support activities, participates in projects, and coordinates the communication process between Atos and your appropriate contacts.
- Improved problem resolution—If problems occur, a shared responsibility exists between the operational/technical groups and the AMO executive to ensure a quick, effective response. This responsibility includes resolving the problem, as well as communicating to you the details of the situation, possible work-arounds, and when it will be resolved. The AMO executive also is responsible for working with other Atos departments to identify symptoms before they become problems and take corrective action to ensure the issue does not recur.
- Service Delivery Reference Manual (SDRM)—The AMO executive works with key employees within both organizations to develop an SDRM that reflects service agreements and operations policies. This manual will be the basis for helping the Lead State and Atos develop strategic IT objectives as well as define daily operations.
- Performance review—Atos maintains contractual performance statistics that the AMO executive reviews monthly with your management. This information is presented graphically with a rolling 12-month history to help identify trends. Atos works proactively to identify areas for improvement and, where a problem exists, establish the root cause and present procedures for prevention.
- Enhanced emergency responsiveness—If a critical problem occurs, the AMO executive has the responsibility and authority to escalate the situation from technicians to supervisors to managers, and ultimately, to executive management. This approach ensures that necessary resources are available to solve a problem.
- Strategic planning assistance—As you develop your future IT strategies, the AMO executive, at your discretion, can participate with or can coordinate Atos technical, operational, and management resources to help with the process. A planning document is developed that formally communicates this strategy; the AMO executive then tracks activities and provides regular progress updates.

In addition to these activities, the AMO executive is responsible for keeping the lines of communication open between the Lead State and Atos. The AMO executive communicates changes that may affect both organizations and makes sure that interested parties are informed.

- **Service Level Agreement (SLA).**

The proper implementation of service metrics enables both the Lead State and our clients to accomplish the following:

- Measure the impact of IT services on the business
- Enable IT to align its goals and objectives to the business
- Provide the client with a lever to affect pricing

An SLA can be tied to the on-time delivery of the agreed-upon reports; we recommend a contract schedule that lists agreed-upon reports and their frequency.

The basis of our approach is to understand your business objectives and work with you to tailor the service metrics that will provide optimal performance compliance in meeting your indicated business and supporting your end users' perspective of quality service delivery within these business objective parameters. Atos proposes working with the Lead State to analyze existing data, and critical and key services that are documented; and historical performance data, or where no performance data exists, using a baseline measurement period. During transition, we'll also define how both the Lead State and Atos will work to achieve the service level objectives, including the current processes that map to the objective and who has responsibilities to complete the processes. Well-designed service metrics provide direction for building a sound technical architecture and guide our personnel in the efficient delivery of promised services.

The client will have the opportunity to apply weighting to each service level measure. Before final service levels can be developed, however, a baseline target for each service must be established. This is important because a service tends to be a composite of services from many functional areas, all contributing to a common objective. Therefore, it's important that each component in the delivery of a service be measured on an individual basis to create the best probability for success at the highest level.

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.

The Atos AMO executive is responsible for each entity that executes a Participating Addendum. Contact information will be kept current and lines of communication will be kept open between the Lead State and Atos. The AMO executive communicates changes that may affect both organizations and makes sure that interested parties are informed.

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.

Atos confirms customer service representative(s) will be available by phone or email at a minimum, from 7 a.m. to 6 p.m. Monday through Sunday for the applicable time zones.

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

Atos confirms customer service representatives will respond to inquiries within one business day.

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

Atos confirms we will provide design services for the applicable categories.

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

Atos confirms we will provide installation services for the applicable categories.

8.5 (E) SECURITY OF INFORMATION

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

As shown in Figure 4, Atos provides a comprehensive and end-to-end approach to design, build, and operate managed security services for our clients. Governance, risk management, audit integration, and compliance are fundamental to the management of security. It ensures the right policies, training, process, and tools are in place and provides visibility to the environment for proper communication and decision making.

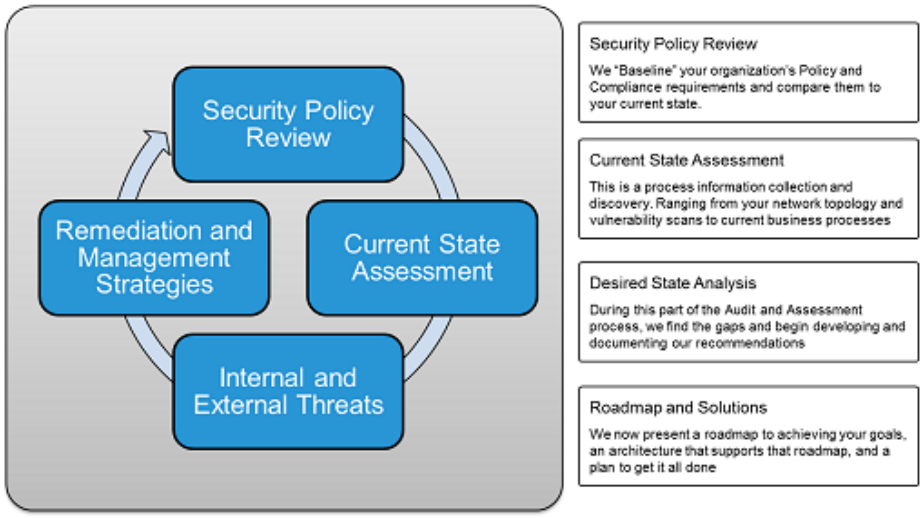


Figure 9. Atos' End-to-End Security Approach

For the Lead State, Atos can implement our comprehensive managed security services, as depicted in Figure 5, to align with your objectives to enhance confidentiality, integrity, and availability of your IT resources and data. Atos can increase the IT infrastructure's security posture through services such as security incident management, vulnerability management, risk management, and intrusion detection capabilities.

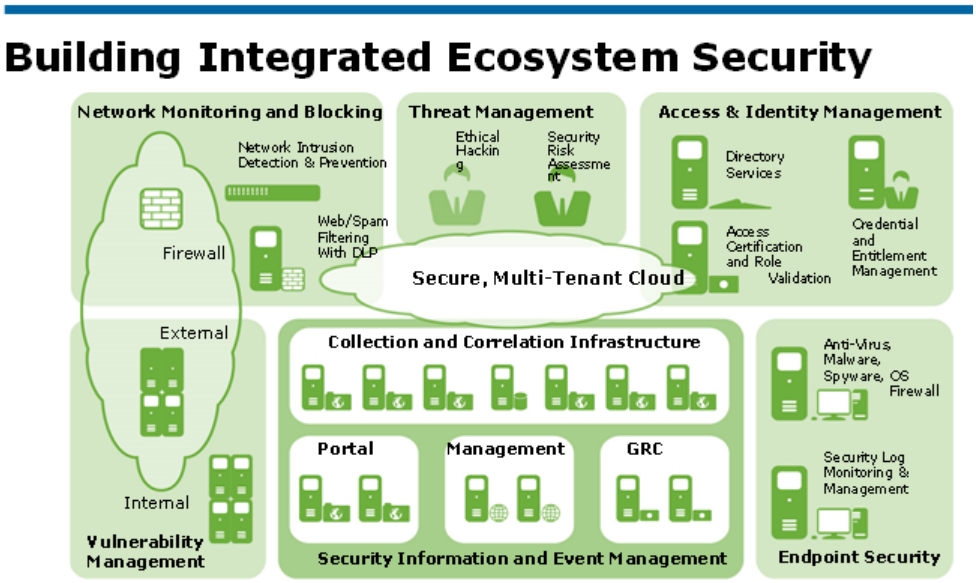


Figure 10. Atos' Comprehensive Managed Security Services

Specific to network security, Atos defines three types of zones to meet demands for security and network access. Combinations of these three zones can be implemented to create multiple-zone solutions. Multiple zones are ultimately securely interconnected using firewalls, as illustrated in Figure 6.

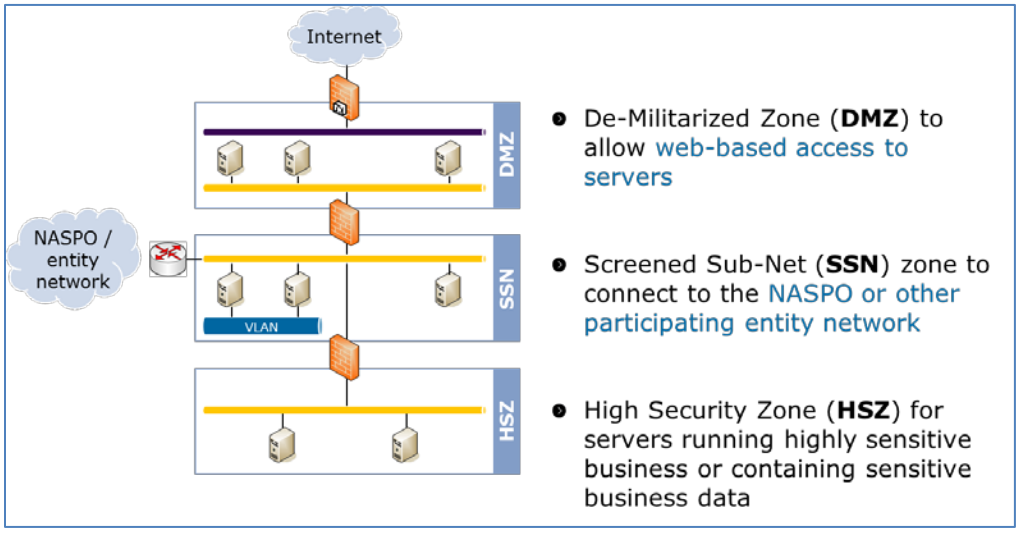


Figure 11. Atos' Security Zones

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

Atos places great importance on the principle that business should be conducted both profitably and responsibly. Atos complies with applicable laws in all countries—this is mandatory. But this is not enough. Atos wants to conduct its business with good ethical principles and practices internally and with third parties.

Atos applies the highest standards of professional integrity internally and with third parties, based on merits and qualifications, without consideration for race, nationality, sex, age, handicap, or any other distinctive trait. For additional details, please see Atos' response to the following question.

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.

Atos firmly believes in the following principles as the basis of dealings with and between its people, and with clients, suppliers, partners, and other third parties throughout the world:

- Atos rejects any form of corruption or bribery.
- Atos is a fair competitor.
- Atos does not tolerate conflict of interest.
- Atos protects its assets.
- Atos protects confidential information.

Our Code of Ethics applies to Atos employees, and its principles must be shared by third parties assisting Atos in developing our business—partners or suppliers. Therefore, Atos

expects all of them to comply with both the letter and the spirit of the Code of Ethics, in addition to the laws and regulations of the countries where they operate.

Atos shall not tolerate any form of bribery or corruption; i.e., providing something of value to influence someone in our favor or accept something for acting against Atos interest, nor participate in any form of money laundering.

As a participant to the United Nations Global Compact, Atos adheres to United Nations principles related to human rights, labor, environment, and anti-corruption. The 10th principle states: "Businesses should work against corruption in all its forms, including extortion and bribery."

Atos thus commits to the following:

- Avoid bribery, extortion, and other forms of corruption
- Develop policies and effective programs to avoid corruption within Atos organization and business operations

This clearly means that Atos firmly rejects the following:

- The fact to offer, give, request, receive or accept, directly or indirectly (active or passive corruption) an inducement or reward (money, gift, hospitality, entertainment, trip, service, etc.) to or from a potential customer or supplier, in the public or private sector in order to influence his behavior in our favor
- Get business (or to do or forbear to do) any act or show, or forbear favor or disfavor to someone

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.

Many of our customers have critical needs around privacy and security in the finance and banking, Government, and energy sectors. Atos provides services to a number of governmental agencies at the state, county, and large municipality level. Atos' services are ITIL-based with a strong focus on customer needs.

Our customers commonly prefer private cloud solutions with service models ranging from PaaS to more complex solutions with varying levels of customer involvement. We embrace NIST standards on cloud computing, and just as important, we focus on the customer's requirements whether they fit squarely within a standard or require hybridized solutions.

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.

Atos has been a worldwide early adopter and long-time promoter of best practices, including International Organization for Standardization (ISO) and other proven guidelines for quality IT service management. Our solutions are fully compliant with PII, HIPAA, PCI, and other related federal and industry requirements, including those listed in Table 1.

Table 1. Atos Certifications

Certifications	Short description (scope, standards institute)
ISO 9001:2008	Atos has been awarded an ISO 9001:2008 certificate for IT-Services and Business Process Outsourcing worldwide.
ISO / IEC 20000-1 : 2005	Atos has implemented and maintains an IT Service Management System.
ISO / IEC 27001 : 2005	Atos has implemented and maintains an Information Security Management System.
ISO 14001	Atos has been awarded an ISO 14001 certificate throughout the entire company. Atos has created a global team, which is responsible for reporting Atos' sustainability achievements in line with the Global Reporting Initiative (GRI), the world's de facto standard in sustainability reporting, created in 1997 in partnership with United Nations, and today used by all best-in-class companies.
ASMM (ITIL)	We employ specific methodologies, skills, and techniques such as our own Atos Service Management Model (ASMM), which is 100% ITIL compliant. ASMM is also fully compliant with the international quality standards ISO 9001, ISO 27001, ISO 20000, and IT-CF 4.0.
Prince2	We believe in equipping our program and project managers to succeed. We have done this by adopting IPMA, MSP, and Prince2 as our preferred project management methodology, and the majority of our project managers are IPMA, MSP, and/or Prince2 certified. (All our project managers are Prince2 certified.) Development projects are carried out according with Prince2, which is the standard method for project and program management. Prince2 also ensures proper involvement of all stakeholders, required to provide on-time delivery..
SAS70/SOX Type 1 and 2	Atos has implemented a control framework to compile SAS70 auditing statements for meeting regulations as laid down in the Sarbanes-Oxley (SOX) Act of 2002, for its own organization as well as to support its customers. The SAS70 auditing standard is used by service auditors to assess the internal controls of a service organization. The final version of a SAS70 auditing statement is submitted to customers if contractually agreed, enabling customers to assess the validity of Atos' internal controls.
CMMI & IT Service CMM Level 3	Atos has a very active program for certification of its business to the Capability Maturity Model Integration (CMMI) Level 3. Atos has development centers in France, Netherlands, and Spain, and offshore development centers in India, China, and Brazil, all appraised at CMMI Level 3.
CMMI Level 5	Since its inception, Atos India operations have had a very strong focus on formal and industry standards for processes and quality management. Atos India operations was awarded

Certifications	Short description (scope, standards institute)
	CMMI Level 5 in 2014. Atos India decided to further increase the level of industrialization by bringing in new elements such as multi-lingual, multi-technology, multi-service, and multi-located delivery models.

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.

Data Protection

Atos looks at every customer's specific needs and applies security solutions based around best practices in data protection to address the unique demands of the customer and industry to assure the highest levels of security necessary to protect the customer's data. Data protection is a multifaceted challenge addressed through secure services, operating processes, and controls, and limiting data access.

Secure services include secure hosting, secure hardened systems, secure perimeters, secure proxies, data encryption, data loss prevention, malware protection, effective detection and monitoring, and best-practice-based processes to assure services remain effective.

Secure operating processes and controls address adherence to the Lead State and Atos policies through account/credential management, the Lead State, and Atos access, change management, and service delivery.

Data access is limited to role-based solutions that are reviewed regularly for separation of duties and right of least access. Atos' internal architecture for the service network and the Lead State's network for access to your equipment and data is limited with control and monitoring points. This ensures that any access to the Lead State's equipment is tracked and limited to authorized staff assigned to perform specific duties.

A change management workflow is built into Atos ticketing and change systems. Changes must follow workflow that includes a number of approval gates prior to implementation. All change requests are monitored, and control gate level approvals are monitored internally, in addition to any change management processes enforced by the customer. Atos has a "no tolerance" policy for failure to comply with the clearly defined processes and controls for changes.

Further controls are in place to ensure the highest levels of service through every aspect of delivery including call handling, customer documentation, operation of services, data handling, and regular meetings/communication with customers.

Facility Protection

Secure facilities are a high priority at Atos. Physical security at our data centers utilize state-of-the-art access control, alarm monitoring, and digital video recording. Digital video

cameras are placed throughout the facility and at key points on the exterior. These components are integrated to provide time-stamped recorded video for all events. Atos also employs trained professional security officers onsite 24x7. These officers are responsible for the continuous monitoring of the facility's system components and for reporting of incidents to security and data center management.

The access control system is established with various zones and access levels. HID iClass badges and readers are installed on all doors and used to control access into the different zones. External entrances are equipped with key pad readers requiring an associated PIN. Biometric readers are used on the entrances to the data center raised floor. Elevated access into the different zones must be documented and approved by the area owner, and access permissions are audited regularly.

At the U.S. data center proposed as the primary data center for the Lead State, there is only one entrance onto the property through an entry gate requiring badge access or security guard intervention. Other facilities have features such as K-12 delta vehicle barriers and K-12 rated fencing at vehicle entrances.

Finally, Atos documents and audits all of the policies, procedures, and work level instructions of physical site security.

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).

Atos Managed Service Controls

Atos implements and enforces controls across the breadth of its services to assure the highest levels of policy compliance to the Lead State and Atos policies. Process reviews occur quarterly; random checks and remediation steps are used to enforce policy and control compliance. Controls are embedded throughout all internal and customer facing services within Atos. The following are the most common customer-facing areas where controls are visible:

- **Customer Environment Access**—Access to the Lead State's equipment and information is tightly controlled. Access is monitored through access limitations enforced at jump servers. Only users who are assigned to accounts have credential access to the Lead State's jump servers, where controls are enforced through logging. Access can be correlated between tickets and change requests. Access beyond jump servers is limited to use of customer-assigned credentials.
- **Account Management**—From onboarding a new user credential through termination, Atos requires two levels of approval, internally and customer, to enforce policies including separation of duties, least privilege, and non-shared accounts. Accounts are reviewed regularly to ensure policies are enforced and primary on-boarding and off-boarding processes and controls are enforced.

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.

Atos' third-party attestations, reports, security credentials (e.g., FedRamp), and certifications relating to data security, integrity, and other controls include ISO 9001, ISO 20000, ISO 27001, and SSAE-15 SOC 2; other attestations, credentials, and certifications can be secured and provided at the request of the Lead State.

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.

Logging is performed on a customer-by-customer basis per requirements. Our baseline recommendations include logging for successful and unsuccessful access attempts, full logging from all security services, and a large number of other logs and datapoints, integrated into our SOC and CSIRT services.

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

Each customer's set of equipment is grouped as a Customer Dedicated Environment (CDE) into one or more network zones dedicated to that customer. There are three types of zones available, which can be combined to create multiple-zone solutions. Multiple zones are always securely interconnected using firewalls. The zone types are as follows:

- A De-Militarized Zone (DMZ) connects to the Internet and allows web-based access to these servers.
- A Screened Sub-Net (SSN) zone has the capability to connect to the customer corporate network.
- The servers in a High Security Zone (HSZ) can only be accessed from entities in the SSN if explicitly allowed by means of a firewall configuration. An HSZ is intended for servers running highly sensitive business or containing sensitive business data.

A customer can have multiple occurrences of any type of zone; e.g., to allow for separation of production, test, and development environments, or to support multiple needs of different units within a business or organization.

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.

First, the scope of the incident is taken into consideration by determining risk, affected users, assets, and locations. A security incident will be assigned as "Priority Level 1" if the incident is characterized by the following:

- The incident is one that has a high impact on the confidentiality, integrity, or availability of information and will increase in scope and impact if the incident is not mitigated.
- The incident, because of the immediacy of its effect on critical business functions or information, requires a resolution (for example: a change) on an immediate-response basis.

A security incident will be assigned as “Priority Level 2” if the incident is characterized by the following:

- The incident can materially affect the customer, causing a substantial impact.
- The effect of the incident is such that it does not require immediate resolution, but it does require a resolution (for example: a change) is executed on a date and time in the near future specified by the customer.

A security incident will be assigned as “Priority Level 3” if the incident is characterized by the following:

- The incident does not materially affect the customer and does not cause a substantial impact on confidentiality, integrity, or availability. The incident does have the potential to do so if not resolved expeditiously.
- The effect of the incident is such that it does not require an immediate resolution, but it does require that a resolution (for example: a change) executed on a date and time mutually acceptable to both parties.

A security incident will be assigned as “Priority Level 4” if the incident is characterized by the following:

- The incident does not have an adverse impact on confidentiality, integrity, or availability because of either the nature of the fault or the small extent of the fault and the fact that the incident will not increase in impact over time.
- The effect of the incident is such that it does not require immediate resolution. A resolution (for example: a change) may be required that can be planned for a date and time that is mutually acceptable to both parties.

For each Priority 1 and 2 security incident, the Incident Response team will lead a defined action plan and do all necessary escalations in Atos, or using a customer escalation matrix. Customer contact persons will be involved in this escalation.

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.

Customer environments are isolated from one another through the use of VLAN technology. Firewall technology is additionally used to isolate security zones within the customer environment. Customers may share enclosures. Server blades are not shared in CIS Single-Tenant services. Server blades are shared in CIS Multi-Tenant services. The system management environment is also separated by firewalls.

Each customer environment has its own separate security zone(s). This environment is accessible through a secure connection over the Internet or a dedicated WAN connection. Both virtual and physical compute options are available from an Atos Cloud Services

catalogue of supported OS's, designed and built for rapid automated infrastructure provisioning.

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)

The referenced architecture for most of the cloud services provided by Atos is detailed in the following graphics.

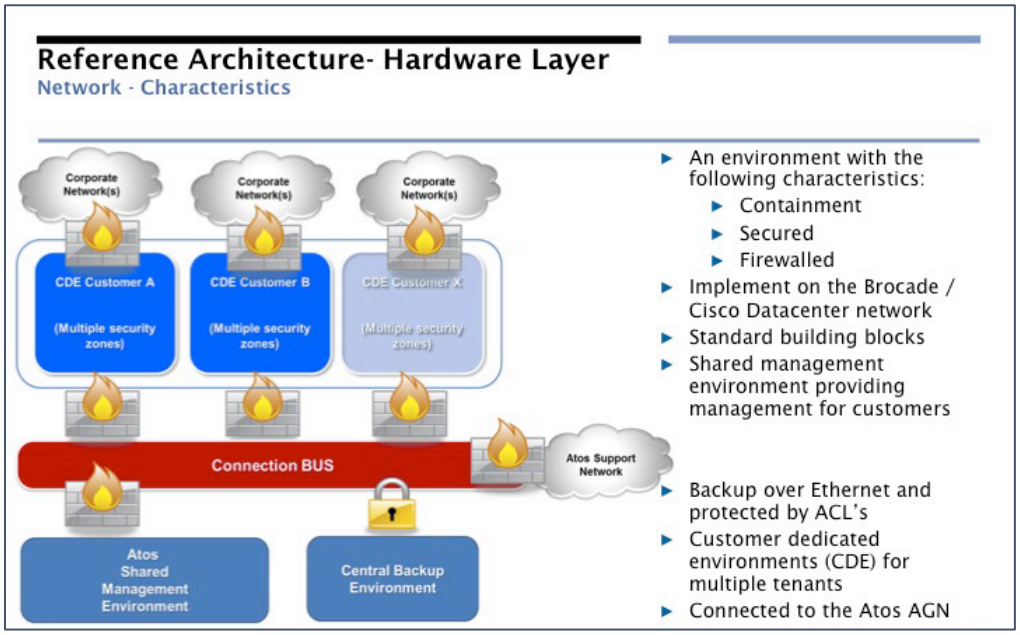


Figure 12. Reference Architecture – Characteristics

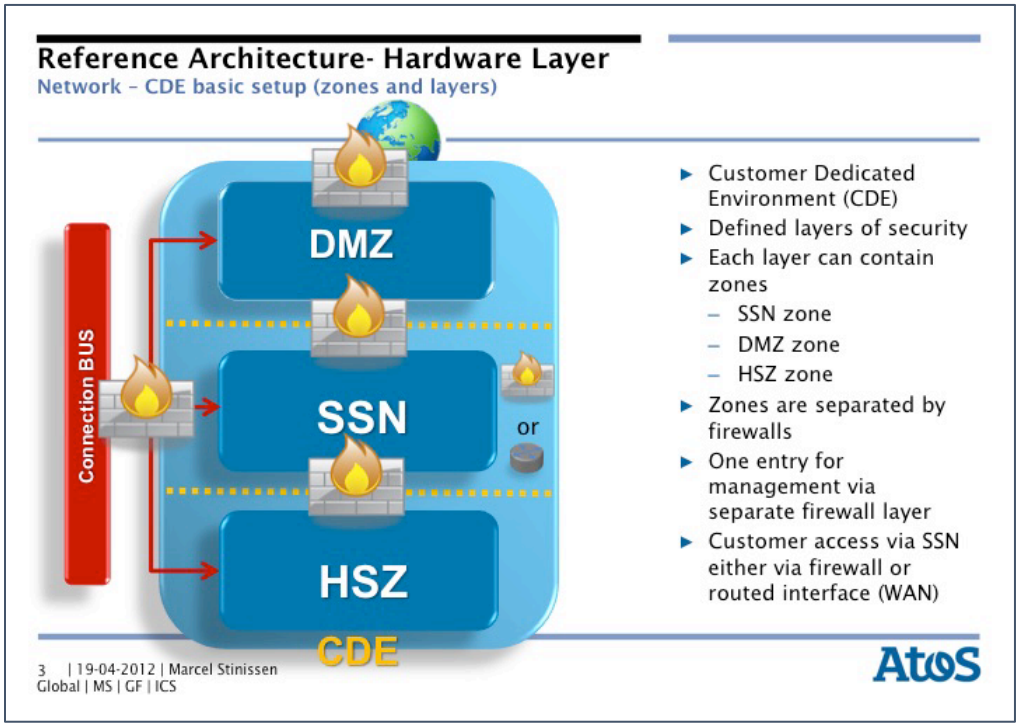


Figure 13. CDE Basic Setup

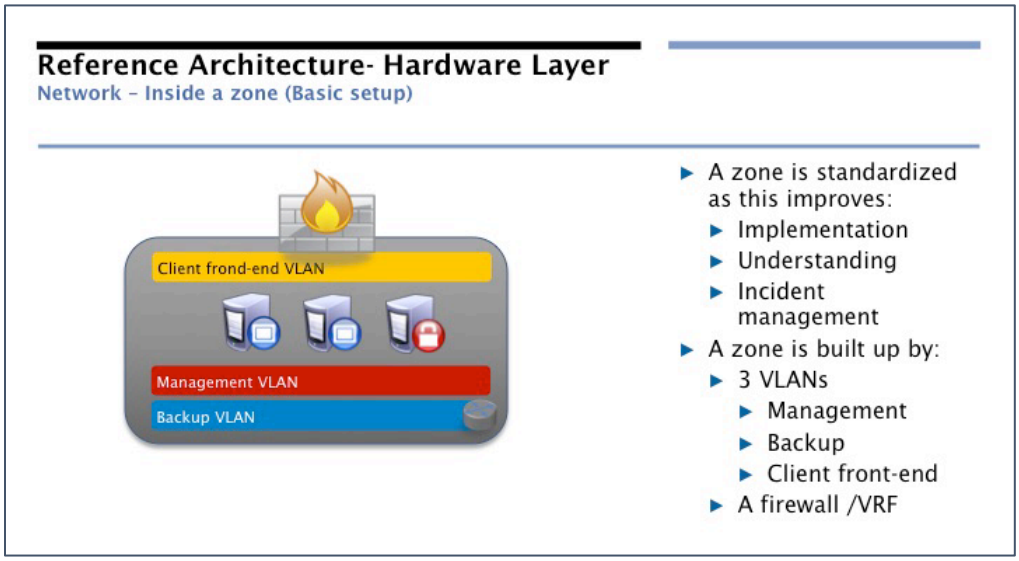


Figure 14. Inside a zone (basic setup)

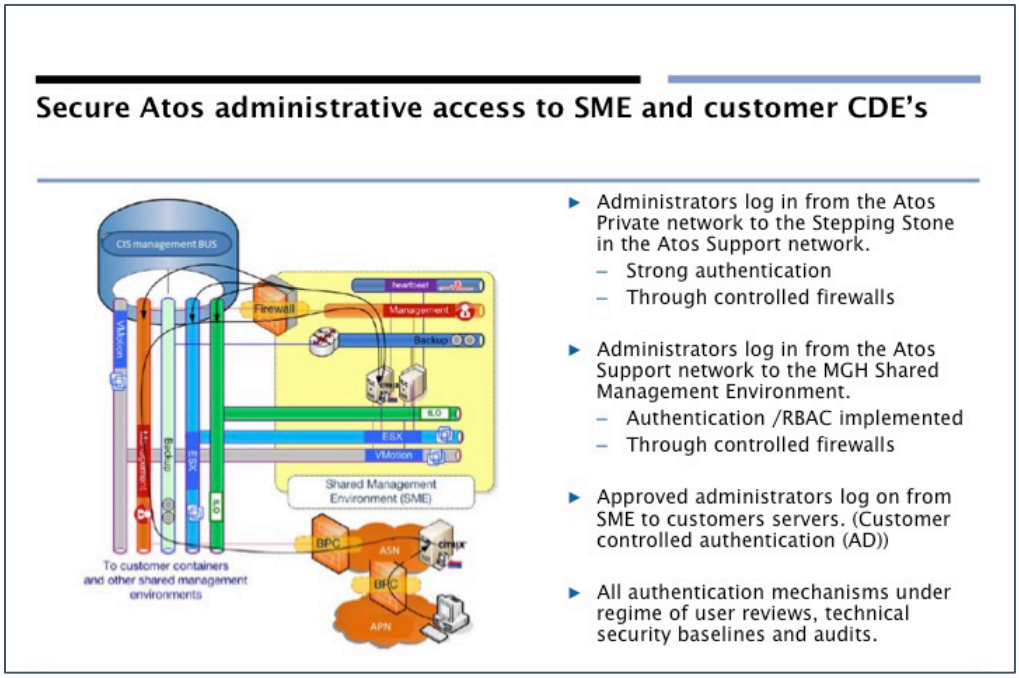


Figure 15. Secure Administration

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.

As part of our rigorous recruiting and hiring process Atos' HR personnel screen potential applicants to identify any issues that contradict our policies and standards for employment, such as a criminal record or illegal drug use. Candidates who do not meet Atos' policies and standards are not considered for further evaluation in the recruiting process. All candidates selected to be hired by Atos must submit to a formal background check and drug screening prior to finalization of the employment offer, and if a candidate does not pass the background check and drug screening, the offer of employment is rescinded.

Below is the general policy for the United States. Globally, the policy is similar allowing for particular legalities in each respective country.

Employment with Atos in the United States is contingent upon satisfactory background screening which includes residence, employment and school attendance (RESA), all convictions for 7 years, and Social Security number(s)verification. Atos works with Verifications Inc., to perform criminal background screening. All findings are then reviewed by Risk Management and HR. Verifications Inc. will also check any area of residence, employment, and school attendance revealed during the background check.

The following background checks are performed for standard staff and managers:

- Academic: Highest completed
- Employment: All employment for past 7 years (maximum 3 employments)
- Criminal:

- County Criminal Provided and Developed RESA for 7 years
- NCRL National Criminal Record Locator
- Federal Criminal District

Global Watch Alert: A check of numerous government watch lists that include individuals, organizations, and companies that have been placed on watch status by the United States Government, European Union, United Nations Security Council, World Bank or foreign governments.

In addition to the background check, a drug screening is conducted, which includes a urinalysis based HHS 10-panel test. Analysis is done at a SAMHSA certified laboratory, and a medical review is completed. The 10-panel test includes testing for marijuana, cocaine, amphetamine/ methamphetamine, opiates, phencyclidine (PCP), barbiturates, benzodiazepines, propoxyphene and methadone.

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.

To safeguard sensitive data at rest and data in motion throughout Atos's physical and logical plants, we employ systems to ensure Encryption, Key Management, Access Controls, and Data Event Information. Atos is also ISO 27001 compliant and certified.

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.

The designated State of Utah security officer will be notified immediately in the event of any data breach. A clear chain of command will be documented and updates will be provided when changes are made. Security incidents follow Atos' incident management processes. The details of customer notification (how and when) are determined and agreed to by both parties during the transition phase.

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 de-provisioning 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.

All contract end activities would be governed by the AMO and delivered by the same managed service and operational teams to ensure a consistent approach and feel during this period of time. This would include all planned and unplanned activities and data migration operations within Atos' sphere of influence.

Atos would work collaboratively with the Purchasing Entity to present (in a suitable format) and migrate its data from Atos' Cloud environments, utilizing approved replication and synchronization technologies. Data hosted within Atos systems during the migration process would continue to comply with any and all security requirements. Data that has left or is in-flight from Atos system control would no longer be the responsibility of Atos.

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.

To ensure an orderly return of data from Atos to the Purchasing Entity, Atos would work collaboratively with the Purchasing Entity to design and approve a set of migration strategies, solutions, and tasks that would facilitate the desired results; zero data loss in a secure and timely manner.

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.

Extended downtime, although extremely rare due to inherent resiliency and redundancy measures built into Atos' Cloud environments, would be handled through Atos' ITIL-based escalation processes.

Escalation of issues follows a chain of command from operational management up through the executive level. To ensure critical issues are raised soon enough to prevent undesirable impacts to the operating environment, the Lead State and Atos will work during transition to identify the triggers and business rules for effective escalation. This activity includes proper identification of escalation time frames, paths, procedures, and contacts. In supporting the Lead State, this process provides for proper alignment of resources to incidents based on severity and need to correctly drive key organizational performance objectives based on those priorities.

The following sample escalation alerts will be triggered based on service levels:

- Open calls within 30 minutes of service level expiration. These alerts are distributed to call allocators, enabling them to take immediate remedial action.
- Open calls at service level expiration distributed to the call allocators' team leader
- Alerts beyond service level expiration— two hours and four hours—distributed to the service account manager through to the national operations manager, depending on service level time exceeded

When an issue is not resolved within service level expectations, we initiate proactive steps to achieve resolution through established escalation channels.

b. Suffers an unrecoverable loss of data.

Atos works diligently with each client to ensure data is fully protected against corruption or loss and depending on preferences, can deliver recovery point objective (RPO) times of "near zero" through continuous operations.

Atos uses technologies such as data backup, cloning, replication and synchronization, database log shipping, etc., to achieve desired RPO times.

c. Offeror experiences a system failure.

System failures within the Atos Cloud environments are at, or near zero, due to the resiliency designed and built into these systems.

The level of resiliency within a given Atos Cloud solution is driven by clear SLAs and agreed upon requirements specifications for business continuity, disaster recovery, and recovery time objective (RTO)/RPO metrics. Resiliency elements may differ for the compute and application environments residing on development and test cloud architecture versus those housed within a mission-critical operational production architecture. Cost factors rise when associated resiliency complexity increases. The higher the level of resiliency required to meet a specific client need, the more redundancy or complexity of protection schema needs to be introduced.

Most Atos Cloud solutions offered today offer a high degree of resiliency already embedded within the solution, and if more aggressive RTO/RPO metrics are needed, Atos can accommodate those demands as required. Atos makes extensive use of highly automated software suites and processes to streamline execution and eliminate human intervention to increase our level of resiliency within the cloud. Data duplication, automatic failover, and twin data center configurations are at the core of the Atos Cloud resiliency strategy.

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

Through Atos ITIL-based incident management process, recovery and restore operations would begin (depending on the severity of the incident) within four hours of an event; however, completion times of less than four hours would depend on the volumes of data to be recovered.

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

The designated Atos Cloud services partners have pre-defined RTO/RPO metrics outlined depending on classification of the actual services contracted. The resiliency of the solution and DR capabilities delivered are pre-negotiated based upon each client's individual needs and price thresholds.

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

a. Method of data backups

Atos uses best-of-breed, industry-standard, disk-based backup technologies as the backbone for our data backup and recovery infrastructure.

Atos works closely with clients to identify suitable backup schedules and data retention periods to meet their business RTO/RPO needs.

b. Method of server image backups

Atos uses both the Full (backup) Once-Incremental Forever methodology that is fully supported by the backup environment, and de-duplication and compression technologies; combined they ensure that data is only backed up once, reducing consumed resources, and hence, costs on the backup environment.

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

Backup data hosted within the primary data center is replicated to a matching disk-based host at a secondary data center. A tape-out facility can be provided at the secondary location for long-term retention or compliancy reasons.

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

Although Atos currently has data centers across the United States, through its partnership with a number of data center facility providers, it has the ability to host client data to meet specific business requirements.

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.

Atos looks at every customer's specific needs and applies security solutions based around best practices in data protection to address the unique demands of the customer and industry to assure the highest levels of security necessary to protect the customer's data. Data protection is a multifaceted challenge addressed through secure services, operating processes, and controls, and limiting data access.

Secure services include secure hosting, secure hardened systems, secure perimeters, secure proxies, data encryption (in transit and at rest), data loss prevention, malware

protection, effective detection and monitoring, and best-practice-based processes to ensure services remain effective.

Secure operating processes and controls address adherence to the Lead State and Atos policies through account/credential management, the Lead State and Atos access, change management, and service delivery.

Data access is limited to role-based solutions that are reviewed regularly for separation of duties and right of least access. Atos' internal architecture for the service network and the Lead State's network for access to the Lead State's equipment and data is limited with control and monitoring points. This ensures that any access to the Lead State's equipment is tracked and limited to authorized staff assigned to perform specific duties.

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.

Yes, Atos would comply as applicable.

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.

Data access is limited to role-based solutions that are reviewed regularly for separation of duties and right of least access. Atos' internal architecture for the service network and the Lead State's network for access to the Lead State's equipment and data is limited with control and monitoring points. This ensures that any access to the Lead State's equipment is tracked and limited to authorized staff assigned to perform specific duties.

Secure operating processes and controls address adherence to the Lead State and Atos policies through account/credential management, the Lead State and Atos access, change management, and service delivery.

Atos looks at every customer's specific needs and applies security solutions based around best practices in data protection to address the unique demands of the customer and industry to assure the highest levels of security necessary to protect the customer's data.

Data protection is a multifaceted challenge addressed through secure services, operating processes and controls, and limiting data access. Secure services include secure hosting, secure hardened systems, secure perimeters, secure proxies, data encryption, data loss prevention, malware protection, effective detection and monitoring, and best-practice-based processes to ensure services remain effective.

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.

Atos prides itself on demonstrating a high degree of flexibility into our clients for our cloud offerings and services, especially in the area of SLA negotiations.

Although Atos offers a set of standard SLAs with our cloud services, clients may negotiate more stringent SLAs, but be in the full knowledge that certain risks may have to be mitigated, or pricing penalties may be incurred, before any SLAs can be operationalized and enforced.

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.

The following table illustrates the SLAs that accompany the IaaS – Shared Private Cloud services:

Table 2. IaaS – Shared Private Cloud SLAs

Element	Measure	Service Level
CIS Storage Bronze Class	Service available 7 days, 24 hours, measured to host adapters in servers where storage is connected to.	99.5%
CIS Storage Silver Class with and without Remote copy option for disaster recovery	Service available 7 days, 24 hours, measured to host adapters in servers where storage is connected to.	99.8%
CIS Single-Tenant Private Cloud physical	Service available 7 days, 24 hours, measured to the operating system prompt.	99.8%
CIS Single-Tenant Private Cloud physical with Infrastructure Continuity option CIS Single-Tenant Private Cloud virtual (based on spare virtualization host and single site cluster) CIS Multi-Tenant Private Cloud (based on shared spare virtualization host and single site cluster)	Service available 7 days, 24 hours, measured to the operating system prompt.	99.9%
CIS Storage Gold Class with and without Remote copy option for Disaster recovery	Service available 7 days, 24 hours, measured to host adapters in servers where storage is connected to.	99.9%
CIS Disaster Recovery solution: CIS Single-Tenant Private Cloud virtual with Infrastructure Continuity option (based on spare virtualization host and twin site	Processing is measured at: Service available 7 days, 24 hours, measured to the operating system prompt.	99.9% RTO: 5 hours RPO:

Element	Measure	Service Level
cluster) incl. Storage Silver or Gold Class with Remote copy option for disaster recovery	Storage is measured at: Service available 7 days, 24 hours, measured to host adapters in servers where storage is connected to.	<1 minute
CIS	Support for Priority 1 incidents available 7 days, 24 hours. All other support and service available only during business hours, CET time.	100%

8.11 (E) DATA DISPOSAL

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

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

Cloud virtual image machines are encapsulated in files located on SAN technology; when a virtual machine is deleted from the cloud environment, those encapsulated files are no longer available to retrieve. Our standard cloud services include a virtual image snapshot performed daily and is retained for 14 days should a restore be required. Atos also can offer optional data retention services.

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.

Atos manages your infrastructure in accordance with established and proven ITIL processes to maximize the service levels that we can provide. These ITIL processes, which are largely automated, are used to support all levels in the infrastructure stack, from the virtualization layer up to, and including the operating system. The Lead State will realize improved and faster responses to fault conditions due to automation. Such automation also frees your valuable and experienced staff from much of the drudgery of managing IT infrastructure, and lets them concentrate on higher-value activities, which can more directly increase the effectiveness of your enterprise.

Atos provides a trusted first step into the cloud from which you can transform your business' legacy applications and develop new cloud applications. The Lead State receives a cloud service with enterprise SLAs, including tiered SLAs, plus monitoring and reporting. Integration across the entire cloud infrastructure and tooling stack has already been done, saving significant time, cost, and risk. A complete set of standard, pre-developed managed services is available, making the Atos solution a true end-to-end enterprise cloud solution.

Atos will assign to the Lead State a customer delivery manager who understands the Lead State, as well as the Participating Entities and the needs they have. They will communicate with the various cloud teams to ensure seasonal and project needs are met. This ensures the highest level of service to both the Lead State and the Participating Entities.

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

SLAs will vastly depend on which deployment model the client workload has been provisioned to (i.e., Private (dedicated or shared) Cloud, Public Cloud, etc.) and which service models have been deployed; however, as stated in Section 8.12.1, Atos can deliver SLAs up to 99.99%.

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.

Atos would implement the standard ITIL-based Incident Management process to enable incidents resolution, aligned to the agreed prioritization and resolution model, contained in the MSA)

Atos would accept incidents for in-scope services through the following entry channels:

- Authorized user telephone contact to the service desk
- Supplier portal self-ticket
- Automated event management-triggered incidents from the supplier's event management system
- Template form emails sent to an approved email address

The notification path for the Incident Management process would remain the same regardless of whether the support is being provided by Atos or one of Atos' subcontractors.

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

A critical component of service level management is the provision for performance penalties and incentives. Atos will put a portion of fees at risk on a monthly basis relative to performance against defined service levels; a service level shortfall may result in a financial penalty, while exceeding expectations may result in a reward. The following elements are critical to the development of a service level incentives methodology:

- Monthly At-Risk Amount—The amount of dollars that Atos puts at risk for meeting service levels. The amount of service level credits credited to the client with respect to all service level defaults occurring in a single month would not exceed, in total, the monthly at-risk amount.
- Critical Service Level—The level of service that is critical to the users and to meeting your business objectives. Service level credits for failures and Earnback apply to Critical Service Levels.

- Service Level—The service level below which a service level default occurs, resulting in a service credit.
- Target Level—The incentive level of performance to achieve Earnback rights.
- Allocation Pool Percentage—A feature that enables the client to place appropriate weights on Critical Service Levels. An amount from the Allocation Pool Percentage may be applied to any critical service level to reflect the importance of that critical service level to the client.
- Earnback—Atos' capability to earn back service credits. For example, if we incurred an outage one month that caused us to perform at less than the service level for a Critical Service Level, but for the year performed in such a manner that a 12-month performance average is greater than or equal to the Target Level for that Critical Service Level, we would earn back lost credit.

Service measures and standards are reviewed annually for historical performance and may be adjusted at your discretion.

Atos' relationship management goal is to fully meet or exceed client performance expectations and service levels in every function. To attain this goal, our employees are trained and motivated to ensure client satisfaction as we deliver services and respond to your needs and requests. Atos will provide monthly performance reports for service level monitoring, indicating actual performance compared to the performance goals established through mutual collaboration between the lead State and Atos, and inclusive of financial penalties as jointly determined.

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

Maintenance of the Atos Cloud Services is strictly controlled. Server maintenance occurs during a set of standard maintenance slots, which are spread throughout each month.

Atos assigns each server to two (2) slots per month. If the default slots given to a server are inconvenient, the customer may request a change and specify two (2) different slots from the selection provided. It is mandatory that redundant environments, including clustered servers, are assigned to separate slots.

The default maintenance calendar for all patching (including non-Microsoft patches), is based on Microsoft's patch day, which is currently the second Tuesday of the month. Maintenance 1 occurs on the Thursday and Saturday/Sunday of that week. Maintenance 2 and Maintenance 3 are the following weeks.

The following maintenance windows, as listed in Table 3, will be provided with this service.

Table 3. Maintenance Windows

Maintenance Window	Hours of Operation
Maintenance 1	
Thursday	
A: Thursday	17:00h – 18:00h
AX: Thursday	18:00h –19:00h
B: Thursday	21:00h – 22:00h
BX: Thursday	22:00h – 23:00h

Maintenance Window	Hours of Operation
Weekend	
C: Saturday	10:00h – 11 :00h
CX: Saturday	11 :00h – 12 :00h
D: Saturday	20 :00h – 21 :00h (Default primary window)
DX: Saturday	21 :00h – 22 :00h
E: Sunday	01 :00h – 02 :00h
EX: Sunday	02 :00h – 03 :00h
F: Sunday	09 :00h – 10 :00h
FX: Sunday	10 :00h – 11 :00h
Maintenance 2	
Thursday	
A: Thursday	17:00h – 18:00h
AX: Thursday	18:00h –19:00h
B: Thursday	21:00h – 22:00h
BX: Thursday	22:00h – 23:.00h
Weekend	
C: Saturday	10:00h – 11:00h
CX: Saturday	11:00h – 12:00h
D: Saturday	20:00h – 21:00h
DX: Saturday	21:00h – 22:00h
E: Sunday	01:00h – 02:00h
EX: Sunday	02:00h – 03:00h
F: Sunday	09:00h – 10:00h
FX: Sunday	10:00h – 11:00h
Maintenance 3	
Thursday	
A: Thursday	17:00h – 18:00h
AX: Thursday	18:00h –19:00h
B: Thursday	21:00h – 22:00h
BX: Thursday	22:00h – 23:00h
Weekend	
C: Saturday	10:00h – 11:00h
CX: Saturday	11:00h – 12:00h
D: Saturday	20:00h – 21:00h (Default secondary window)
DX: Saturday	21:00h – 22:00h
E: Sunday	01:00h – 02:00h
EX: Sunday	02:00h – 03:00h
F: Sunday	09:00h – 10:00h
FX: Sunday	10:00h – 11:00h
Each server must be listed in two slots from the total 36 provided. The primary slot is used for patching and the secondary is used as a fall-back window. Each slot has a code (e.g., 1C which refers to maintenance 1, Slot C - Saturday 10:00h-11:00h), so a server must always have two (2) codes. There are no restrictions on which two slots, so, for example, the following combinations are	

Maintenance Window	Hours of Operation
possible: Server 1: 1C, 2C Server 2: 3A, 3AX Server 3: 1A, 3FX	

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

Atos will put a portion of fees at risk on a monthly basis relative to performance against defined service levels; a service level shortfall may result in a financial penalty, while exceeding expectations may result in a reward. For additional information, please see Atos' response to Question 8.12.4, "Describe the consequences/SLA remedies if the Respondent fails to meet incident response time and incident fix time."

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.

The following is a sub-set of standard reports generated by Atos Cloud Services:

- Standard Change Statistics (Monthly) - Provides an overview of changes completed per month in relation to the target SLA
- Daily Resource Usage - Provides daily resource statistics per Virtual Data Center vCPU | Memory | Storage
- Monthly Resource Usage - Provides monthly resource statistics per Virtual Data Center vCPU | Memory | Storage
- Committed Resource Allocation (Monthly) - Provides statistics for committed resource allocation per Virtual Data Center vCPU | Memory | Storage
- Monthly Resource Usage (PvDC) - Provides monthly resource statistics per Provider Virtual Data Center vCPU | Memory | Storage
- Number of Portal Requests - Provides an overview of total number of portal requests that were triggered per month
- Number of Blueprints (Monthly) - Provides statistics related to vCAC blueprints/templates that are made available to a customer environment
- DR Protected VMs (Monthly) - Displays the total number of virtual machines for which the disaster recovery option is enabled

Figure 11 shows the workflow for standard reports.

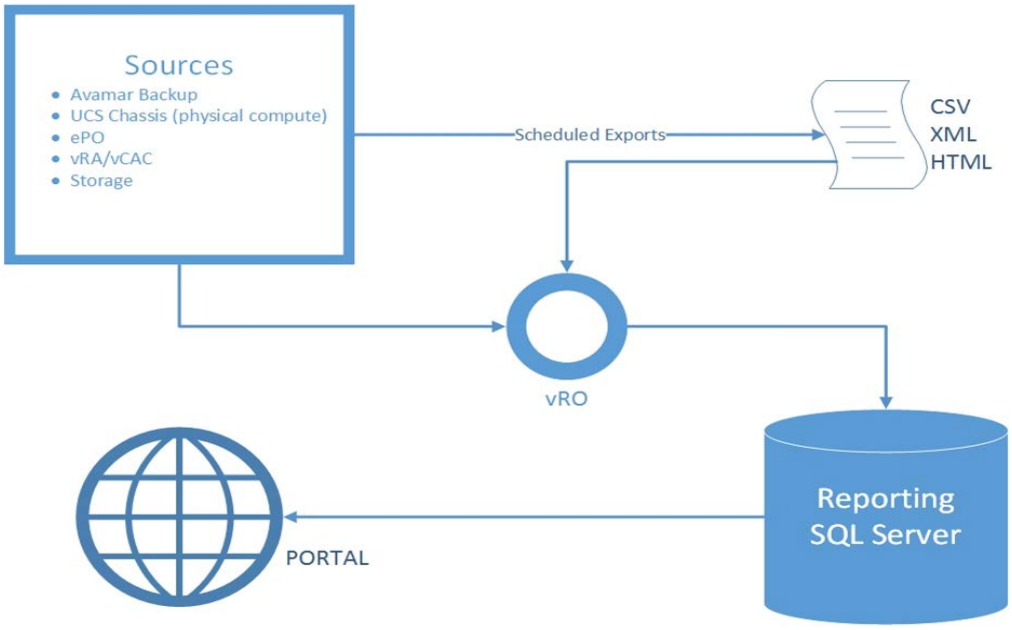


Figure 16. Report Workflow

All report information is retrieved with a workflow executed in vCenter Orchestrator and sent to a central repository as HTML-code. The customer can view these reports with a standard Internet browser.

Performance statistics for all customer-owned VMs are presented through vCOP's dashboard, which not only provides current usage statistics, but also enables browsing through the historical data that can be presented in a graphical format, as shown in Figure 12 and Figure 13.

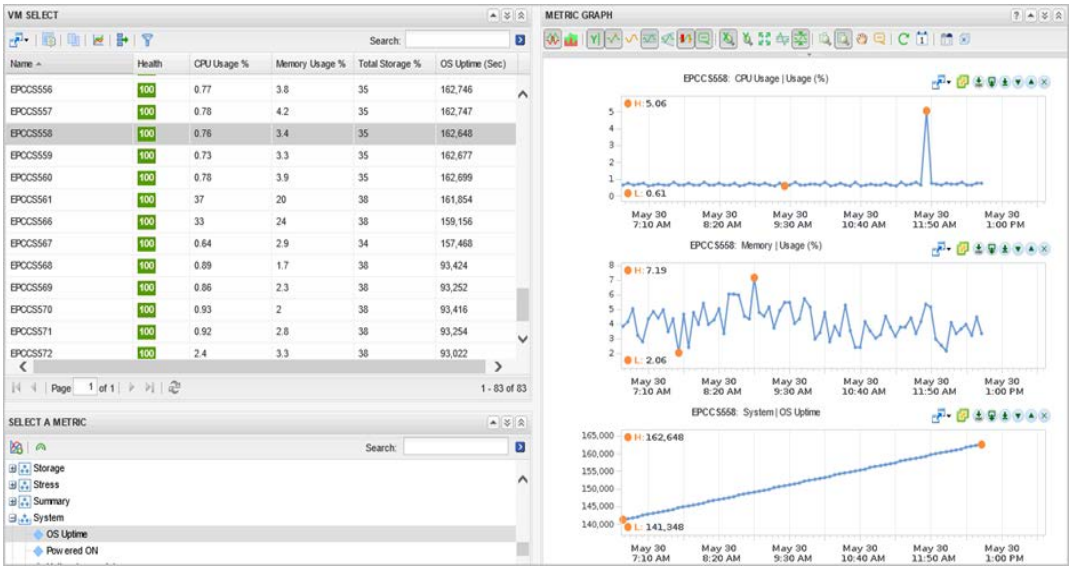


Figure 17. Performance Statistics

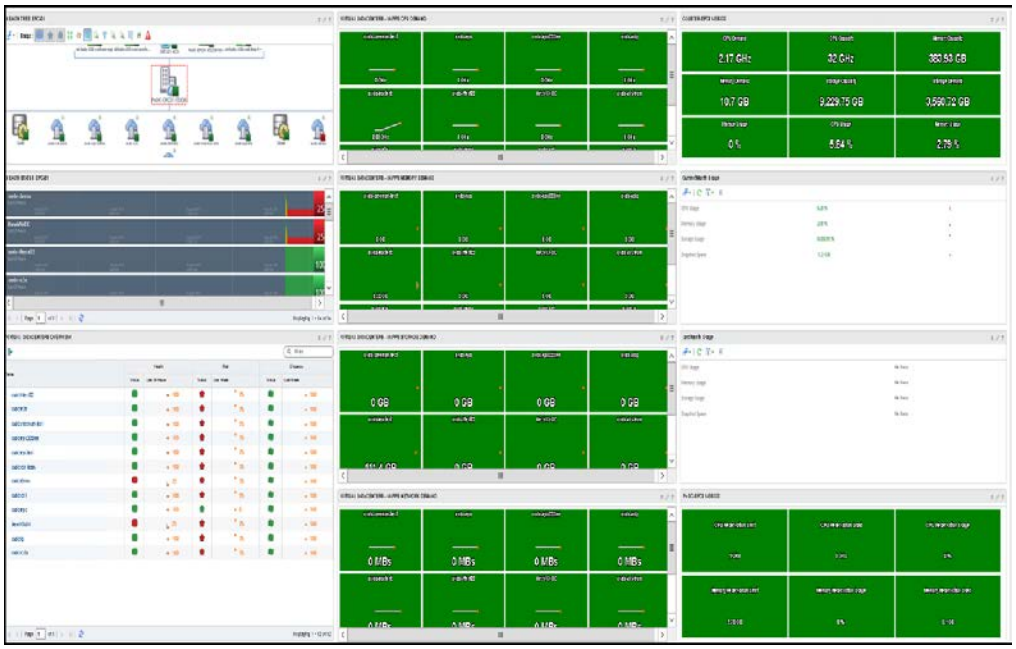


Figure 18. Performance Statistics (cont.)

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

Upon contract award, Atos works in conjunction with our clients to develop a comprehensive Governance Model and establish an AMO to control, manage, and report on all operational elements of the contract and service delivery. Typically, an Atos account executive is applied and has sole responsibility for contract administration, as well as full authority to govern the contract terms, as specified, and directly interact with the designated client liaison. Additionally, a service delivery manager (SDM) role is inserted into the governance model to manage and report upon daily activities, and address any issues that arise with operational execution of the solution applied. Historically, the Atos account executive and leverage a financial analyst or business analyst to produce usage reporting statistics on a monthly basis, and review with our clients to ensure full transparency is provided on consumption levels.

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

To ensure that Atos' Cloud Services are supported 24x365, support staff are located across the globe, allowing for a follow-the-sun (FTS) support model to be achieved.

Figure 19. Atos' Support Staff and FTS Support Model

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

Atos offers dynamic scalability, providing clients with highly flexible consumption of compute and storage resources for seasonal business demands and volatile business, as well as production transfers, year-end closing, and more. Dynamic scalability also enables rapid elasticity, enabling on-demand resizing of resources, and scale-up or scale-down for peak workloads. The Atos solution also has the unique capability to enable applications to automatically scale up and down, 24x365, without human interaction and based on a predefined policy and workloads.

8.13 (E) CLOUD SECURITY ALLIANCE

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

a. Completion of a CSA STAR Self-Assessment, as described in Section 5.5.5

Atos is a member of the Cloud Security Alliance. Details on our disclosures for our services can be provided. Documents are available on the CSA web site: (cloudsecurityalliance.org/membership/corporate).

b. Completion of Exhibits 1 and 2 to Attachment B.

Please see the attached Exhibits to Attachment B:

- 11_Exhibit 1 to Attachment B - CAIQ v3.0.1-09-16-2014;
- 12_Exhibit 2 to Attachment B - CSA_CCM_v3.0.1-09-16-2014

Documents are available on the CSA website:
https://cloudsecurityalliance.org/membership/corporate/

c. Completion of a CSA STAR Attestation, Certification, or Assessment.

Documents are available on the CSA website.
https://cloudsecurityalliance.org/membership/corporate/

d. Completion CSA STAR Continuous Monitoring.

Documents are available on the CSA website.
https://cloudsecurityalliance.org/membership/corporate/

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.

Atos takes great pride in our ability to collaborate effectively with clients in the delivery of services to meet their agility needs.

If the requested services exceed the capacity "buffers" built into Atos Cloud Service environments, Atos, through its AMO would either identify other suitable hosting platforms to temporarily host the required workload(s) until additional capacity is implemented, or escalate the request through management channels.

8.14.2 Describe in detail the standard lead-time for provisioning your Solutions.

Procurement lead times vary slightly by vendor, but Atos works diligently with these vendors to ensure that any and all lead times are kept to an absolute minimum. An example: One of our dedicated Private Cloud environment hyper-converged infrastructures has been reduced to a single SKU to streamline the procurement process.

8.15 (E) BACK-UP AND DISASTER PLAN

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

Atos currently provides this service for many other clients and as such, works actively with clients to design and approve technical and process-driven designs to meet the client's legal and business requirements, in terms of data retention periods and methods of storage (i.e., disk, tape, etc.).

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

Atos leverages the ITIL V3 risk management process definition and disciplines. Risk migration is effectively controlled inside Atos operations through rigorous change management review cycles both internal and external with our clients' IT sponsors. Risk management tasks are inherently embedded within all Atos operational frameworks, and the identification of risk factors, level of impact, and mitigation strategy drives daily execution for all production-level environments.

Risk tolerance levels are often openly discussed with our client base as that may influence certain speed-to-execution factors applied to a given effort or implementation. Based on the level of acceptable risk and associated cost factors, such as level of redundancy required for protection, Atos will craft proper mitigation strategies to control potential impacts. Risk identification and controlled monitoring is a continual task for Atos inside the operational management fabric.

8.15.4 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.

Atos owns and operates, through a number of third-party providers, a portfolio of Tier 3 and Tier 3+ data center facilities across the continental United States. To ensure maximum resiliency, Atos Cloud services are hosted within these data centers, which provide the following:

- Redundant connectivity through multiple vendor connections
- N+1 or 2N redundant power supplies, with generator backup
- N+1 redundant air conditioning and cooling systems

At the cloud infrastructure layer, resiliency within Atos' Cloud services is provided through the following:

- Redundant cloud platforms at both primary and secondary data centers
- Best-of-breed replication / synchronization / failover technologies across the storage and compute layers to meet client's RTO / RPO requirements

In the unlikely event that the primary data center became unavailable, workloads would failover to the secondary data center, in line with agreed RPO / RTO time lines.

8.16 (E) SOLUTION ADMINISTRATION

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

Atos' identity management (IDM) solution is a meta-directory approach using an LDAP V3 directory as the central data store, otherwise known as the Identity Vault. Because the Identity Vault is based on LDAP directory technology, importing data via LDAP is out-of-the-box functionality. This method is primarily used when the existing data resides in a comma separated text (CSV) file or another LDAP directory and the data does not require much manipulation.

NetIQ/Novell provides an import conversion export (ICE) utility to facilitate importing and exporting data to and from the Identity Vault. This LDAP-based utility enables you to perform the following:

- Import data from CSV or LDIF files to an LDAP directory
- Export data from the LDAP directory to an LDIF or CSV file
- Migrate data between LDAP servers (LDAP to LDAP)
- Perform a schema compare and update
- Load information into eDirectory using a template
- Import schema from SCH files to an LDAP directory

The ICE utility manages a collection of handlers that read or write data in a variety of formats. Source handlers read data, while destination handlers write data. For example, if you want to import LDIF data into an LDAP directory, the ICE engine uses an LDIF source handler to read an LDIF file and an LDAP destination handler to send the data to the LDAP directory server. Our technology set includes the following tools:

Identity Vault—Centralized and distributed identity data store and is the basis for meta-directory functionality. It will store user data coming from various authoritative sources, such SAP or PeopleSoft, and connected systems such as Active Directory using NetIQ Identity Manager Connectors. The Identity Vault may be replicated across all the main data centers.

Identity Manager—Automatically provisions users and manages their identity and passwords. Provides a bi-directional integration framework with the ability to specify flow of identity profile attributes between the Identity Vault and the connected systems. Identity Manager will be used to provide automated, real-time, bi-directional synchronization of a user's account and passwords across disparate systems such as Active Directory, LDAP, and Exchange. When you create a new user in SAP or PeopleSoft or another authoritative source, all of the user's accounts are generated automatically—according to your business rules—and any approval workflows are automated. Additionally, you can synchronize a user's passwords to provide a single password to all connected systems. Identity Manager's self-service password management features reduce the number of service desk calls, and increase security and user productivity.

Identity Manager Roles-Based Provisioning Module—Provides the ability to manage user access to secure resources through role-based and workflow-based provisioning. These resources may include digital entities such as user accounts, group memberships, computers, and databases. Identity Manager can serve a wide range of provisioning requests. Provisioning requests are user or system actions intended to grant or revoke

access to organizational resources. They can be initiated directly by the end user through the Identity Manager user application, or indirectly in response to events occurring in the Identity Vault. The Roles-Based Provisioning Module provides several out-of-the-box reports that enable you to view reports that describe the current state of roles. These reports can help you to monitor, add, modify, and delete roles or separations of duties.

Analyzer for Identity Manager—Provides the tools necessary to complete the analysis, cleansing, reconciliation, and reporting of identity-related data through the enterprise. Clean and accurate data is a critical dependency in the successful implementation of any identity management solution, and the Analyzer tool helps ensure this key task is addressed in a quicker and more effective manner than traditional approaches.

Identity Manager Resource Kit—Out-of-the-box set of components (policies, documentation, best practices, solution deployment guides, etc.) designed to accelerate the deployment and quality of business solutions based on Identity Manager, and Access Manager and Sentinel, which are described below. The Resource Kit enables quick implementations of high-quality identity solutions resulting in a higher return on investment.

Designer for Identity Manager—A visual client-based tool for designing, debugging, deploying, and documenting your identity management solutions. It gives you a full view of Identity Manager and connectors for target systems, and lets you drill down to any level of detail. Designer also automates the design and documentation process with a user-friendly GUI, and eliminates manual coding efforts necessary in competitive solutions. Designer enables you to perform the following:

- Carry projects with you, work offline, and save projects to disk
- Keep a project open for an extended period of time
- Work on multiple projects at the same time
- Experience higher performance because processing is performed on the local CPU
- Enjoy a smoother interface with fewer clicks and fewer sub-windows to resize or close
- Benefit from an included development/debugging environment and integration with other client-based tools for editing and debugging

Access Manager—Access Manager provides Web SSO so that all employees only have to remember one log-in for authorized access to all web-based applications. This will free your service desk from web-access password calls, make your users more productive, and support your security requirements. Access Manager also includes Federation. Based on industry-leading open standards such as Liberty Alliance, SAML, WS-Security, WS-Federation, and card space, each federated identity provider counts on NetIQ Access Manager for precise policy enforcement to deliver the same rights users would have if they signed into individual systems directly. NetIQ Access Manager also includes an integrated SSL VPN server so that remote users can securely access non-web services.

Access Governance Suite—Consists of the Roles Lifecycle Manager and the Access Certification Manager. These components extend the role functionality of NetIQ Identity Manager by providing advanced role management, analysis, and certification. The Access Governance Suite integrates tightly with NetIQ's Identity Manager and Roles Based Provisioning Module.

The recertification process includes a web-based progress report to show the manager or application owner how far along he or she is in the process. For each user, the manager can drill into the specific entitlements and roles that are assigned and determine if the roles or entitlements should be maintained or revoked. For systems managed by Identity Manager, these actions can then be synchronized to Identity Manager.

NetIQ Sentinel—Sentinel is a SIEM solution that automates the collection, analysis, remediation, and reporting of system, network, application, and security logs to help organizations manage IT risk. Sentinel replaces the labor-intensive manual processes associated with managing security, with automated, continuous monitoring of security and compliance events and IT controls. Sentinel can be used exclusively for monitoring and reporting on the identity environment, and can be used as an enterprise SIEM solution or in conjunction with existing SIEM solutions via integration.

Sentinel correlates and analyzes security and compliance events from data sources in your environment to help you identify security events in real time and respond quickly. Automated incident response management enables you to document and formalize the process of tracking, escalating, and responding to incidents and policy violations, and provides two-way integration with trouble ticketing systems. Sentinel enables you to react promptly, resolve incidents efficiently, and prove to auditors that your IT controls work as required.

For dashboard-type reporting, the solution provides a graphical view of raw events in "active views"—near-real time as they happen. The events appear in a graphical form in addition to a tabular format. The events are plotted in X-Y-Z axes, depending on the filters, time range, and time intervals you specify.

Identity Manager Driver for Sentinel—This component aggregates and enriches security records from multiple endpoints, providing real-time identity visibility and tracking. This is the only solution to closely tie identity to security and event monitoring.

Sentinel Identity Tracking Solution Pack—Provides an integrated set of Sentinel correlation rules, reports, and associated Sentinel content to add identity visibility and tracking to validate compliance with company policy.

RSA Envision—A SIEM used by Atos for internal and client security event collection, aggregation, analysis reporting, and auditing.

User Application—The User Application, sometimes referred to as the Identity Portal, provides self-service password administration, self-management of identity information, resource request and approvals, role management, and a white-pages interface.

Privileged User Manager—Allows visibility into all privileged user system activities across the enterprise environment. It specifically targets managing, controlling, and recording of all privileged administrator activities for UNIX, Linux, and Windows systems.

Secure Login—Gives employees secure single sign-on access to all the enterprise resources they need.

Compliance Management Platform—Uses the WorkloadIQ approach for a holistic view of all network events for automated compliance. The Compliance Management Platform offers features designed to decrease deployment costs, lower total cost of ownership, and dramatically reduce the time required to use provisioning, access management, and

security solutions. It improves governance and security by enabling common access policies across all identity repositories and provides automated validation of pre-set business rules. The Compliance Management Platform automatically logs all network activity and delivers compliance reports in an audit-ready format.

Consisting of a prepackaged set of products and integration resources, the Compliance Management Platform delivers the necessary technology to accurately monitor and demonstrate compliance levels. The products and modules are integrated into a single platform to offer a seamless solution, but they also work well as individual products in a mixed-vendor IT environment.

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

Atos provides a suite of security products—Endpoint Protection services (anti-virus, malware protection) is but one of them. Endpoint Protection services is provided utilizing the best of products from a selection of top-tier vendors. Atos security services and business technologists have successfully secured the Olympic Games since 2002.

Our experience in anti-virus monitoring and policy management is reflected by the following metrics and features of our Endpoint Protection services:

- 1,200,000+ workplaces (desktop/laptop) and 1,000,000+ mailboxes based on Exchange
- 60,000+ Windows-based server and 100+ gateways (HTTP and SMTP Scan)
- Several hundred terabytes on storage devices and 50,000+ mobile devices
- Comprehensive security functionalities around the endpoints
- Modular structure that enables clients to select the appropriate features that fit their requirements
- Protects the end-user devices and servers from malicious code
- Protects the client's intellectual property, business-critical information, and sensitive data against internal and external harassments
- Easily integrates with other services

Atos also provides the following support for secure socket layer (SSL) certificate management, secure large file transfer, and synchronization as well as middleware messaging systems, such as IBM MQ, TIBCO, etc.:

- Monitoring or managing secure Web gateways
- URL filtering (Atos Proxy Services)

Atos has the security knowledge of multiple business sectors and operating experiences coming from our support of more than 1.7 million Internet users of global clients in more than 20 countries. Atos supports our clients by analyzing the requirements and designing proxy solutions. The service offers the following standard security solutions based on individual configurable security modules:

- Forwarding and reverse proxy functionalities
- URL filtering
- Content filtering using SSL packet inspection
- Malware protection

- Media streaming support
- Scalability and high availability
- Highly secure administration infrastructure globally

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

Atos, through its AMO, will work collaboratively with the Purchasing Entity and its chosen Cloud Hosting solution provider to migrate the Purchasing Entity's data out of Atos Cloud Services.

Contract termination and or inserting a new service provider, if required, can be further discussed and agreed upon as part the MSA process.

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

Atos has the ability to administer the solution in a distributed manner to different Participating Entities, as long as doing so does not violate Atos' or any Participating Entity's security controls, policies, or procedures.

Atos implements and enforces controls across the breadth of its services to ensure the highest levels of policy compliance to the Lead State and Atos policies. Process reviews occur on a quarterly basis, and random checks and remediation steps are used to enforce policy and control compliance. Controls are embedded throughout all internal and customer-facing services within Atos.

8.16.5 Ability to apply a participating entity's defined administration polices in managing a solution.

Atos has the ability to apply a Participating Entity's defined administration policies in managing a solution, as long as doing so does not violate Atos' or any Participating Entity's security controls, policies, or procedures.

Atos implements and enforces controls across the breadth of its services to assure the highest levels of policy compliance to the Lead State and Atos policies. Process reviews occur on a quarterly basis, and random checks and remediation steps are used to enforce policy and control compliance. Controls are embedded throughout all internal and customer-facing services within Atos.

8.17 (E) HOSTING AND PROVISIONING

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

Atos will provide a cloud self-service portal, which is the customer's single point of entrance to the solution. It provides the Lead State or the Participating Entity with the ability to interact with the Atos Cloud services environment, as shown in Figure 15.

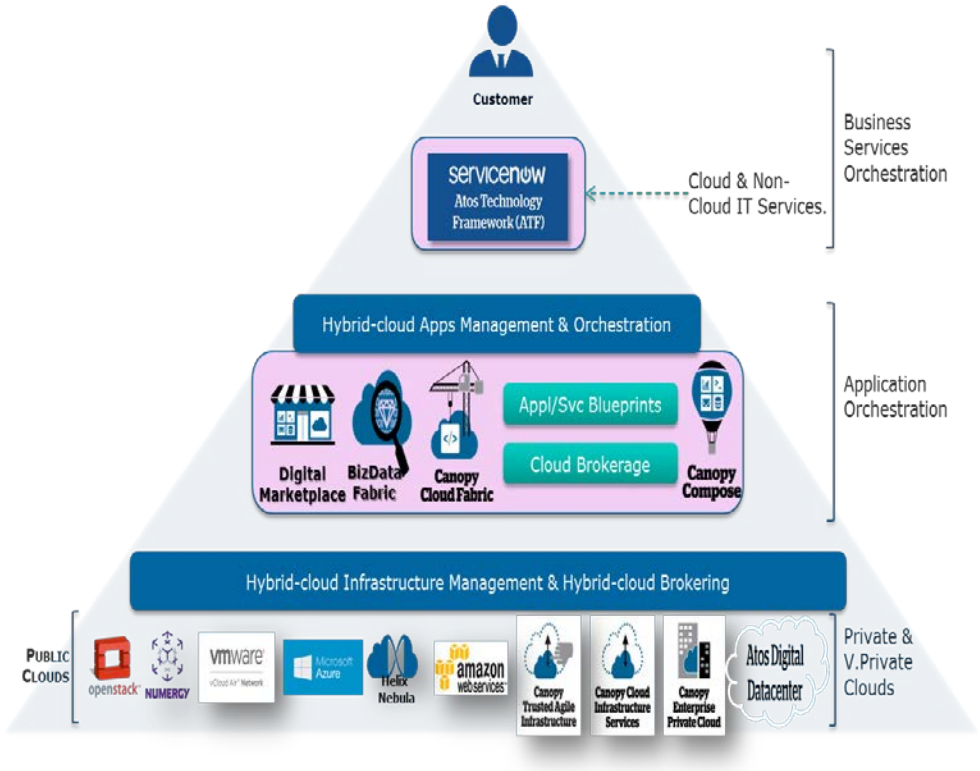


Figure 20. Atos' Cloud Services Environment

Furthermore, with the Atos Cloud infrastructure, users can browse the Service Catalog to request items they need, track their requests, and manage their provisioned items. Management and administration of the environment is also done through this portal. Service architects and tenant administrators can define new services and publish them to the catalogue; they also manage the presentation of the catalogue items to consumers. In turn, business group managers can specify business policies, such as who is entitled to request specific catalogue items or perform specific actions on the provisioned items.

Atos deploys blueprints, which facilitate authorization workflows. Standardized services are a collection of blueprints that hold all logic to provision the services in a standard and easy way. By putting different machine blueprints together, a service architect or tenant administrator can create different services and publish these in the Service Catalog.

Large software applications normally require sophisticated deployment procedures, and frequent releases and updates that are challenging to maintain with agility and consistency. With blueprinting and automation, our operations teams can manage a large number of repeated deployments to multiple cloud-based deployment targets with ease. A blueprint captures an application landscape's entire technology stack, including VM, OS, network, middleware, application, multi-tiered architecture, and data.

Atos is able to deploy the same blueprint to all supported cloud targets (private, virtual private, or public) through our cloud brokerage layer in a highly repeatable, consistent, predictable, and automated fashion. These blueprint-based deployments also help us ensure consistency between development, test, and production environments so that functionalities verified in the test environment will remain the same in production.

8.17.2 Provide tool sets at minimum for:

1. Deploying new servers (determining configuration for both stand alone or part of an existing server farm, etc.)

Atos Cloud services uses our own cloud orchestration tool suite, which includes best-of-breed and industry-standard tools, such as VMware's vRealize Automation (vRA) and vRealize Orchestration (vRO). These tools provide a large degree of flexibility for our clients, depending on requirements, as to where application and compute workloads may be positioned.

2. Creating and storing server images for future multiple deployments

Atos Cloud services comes with an extensive Service Catalogue of cloud applications ready to consume via the self-service portal. These include the following:

- Standardized architecture templates for your application landscape, such as application servers, database servers, middleware, popular application stacks, etc., enabling clients to deploy them many times
- Blueprints—Single- or multiple-node components pre-installed with specific software and accessed via the Compose catalogue, enabling clients to create their own customized environments and deploy to a target infrastructure
- Runtime policies—Various best-practice auto-recovery, auto-scale, and load-balancing policies that can be readily attached as enhanced behaviors to blueprint components

In addition to this, Atos offers the Blueprint Factory, a service delivered by our team of blueprinting experts to create custom blueprints specific to client needs. Furthermore, we offer clients the ability to customize components of existing blueprints including the effectors, sensors, policies, etc.

Atos Cloud Services is powered by open source projects like Apache Brooklyn and Apache jclouds, which are technologies aimed to accelerate cloud adoption by allowing businesses to benefit from cloud while remaining in control and having the power to model, deploy, and manage applications.

3. Securing additional storage space

Requests for additional storage resources will be made through the Atos-provided cloud self-service portal.

4. Monitoring tools for use by each jurisdiction's authorized personnel – and this should ideally cover components of a public (respondent hosted) or hybrid cloud (including Participating entity resources).

The Atos Cloud provides intuitive dashboards, views, and reports, which help align IT spending with business priorities by getting full transparency of infrastructure and application cost and service quality. Usage metering provides the requisite transparency for both the provider and consumer of the utilized service for use in dashboards, reports, and "bill of IT."

Best-of-breed, industry-standard monitoring tools are utilized across the entire platform stack, including the following:

- Virtualization layer – VMware's suite of tools
- Operating systems – UMF Nagios, Microsoft SCOM

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

Atos Cloud offerings and our partner solutions are established upon a rate card structure, and clearly published pricing is based on a given service catalogue model and compute specification level being requested. Consumption-based billing is a normal functional element of our cloud solution offerings contracts.

8.18 (E) TRIAL AND TESTING PERIODS (PRE- AND POST-PURCHASE)

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

Testing and training services are fully described in Sections 8.18.2 and 8.18.3.

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.

Atos Cloud services provide a 30-day "Trial Mode" evaluation environment for its clients to test against to ensure that they meet the client's technical and business requirements.

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

Training costs are usually incurred by the client, but Atos would be willing to include these in the MSA negotiations.

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.

Atos Cloud services comes with an extensive catalogue of cloud applications ready to consume via the self-service portal, including the following:

- Standardized architecture templates for your application landscape, such as application servers, database servers, middleware, popular application stacks, etc., enabling clients to deploy them many times
- Blueprints—Single- or multiple-node components pre-installed with specific software and accessed via the Compose catalogue, enabling clients to create their own customized environments and deploy to a target infrastructure
- Runtime policies—Various best-practice auto-recovery, auto-scale, and load-balancing policies that can be readily attached as enhanced behaviors to blueprint components

In addition to this we offer the Blueprint Factory, a service delivered by our team of blueprinting experts to create custom blueprints specific to a client's needs. Furthermore, we offer clients the ability to customize components of existing blueprints, including the effectors, sensors, policies, etc.

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

The Atos Cloud Services team prides itself on its ability to work with clients to customize and personalize solutions to meet their specific needs.

This could be as simple as personalizing client-facing portals with a corporate logo, to customizing infrastructure components to meet regulatory compliance requirements.

8.20 (E) MARKETING PLAN

Describe your how you intend to market your Solutions to the Lead State ValuePoint and Participating Entities.

Atos will be pleased to share with the State of Utah a detailed Marketing Plan during the next stage of the RFP process. The plan will fully describe how Atos will market our Cloud Solutions to NASPO ValuePoint and Participating Entities.

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.

Atos has a substantial Cloud Services organization and delivery team specifically focused on delivery of consultative and migration-based services to our client globally. Some of the core offerings are summarized below.

Cloud Consulting Services

Atos' Cloud Consulting services offer the following:

- Automated discovery of compute and application landscapes
- Cloud consultancy transformational readiness assessments
- Cloud architecture design and deployment services
- Infrastucture2Cloud assessment, planning, design, and migration services
- Hybrid cloud adoption and brokerage orchestration planning services
- SaaS integration design and deployment services
- Public Cloud adoption strategy assessment, planning, and transition services
- Cloud application assessment and transition services
- Cloud application workload migration and implementation services

Consulting delivers tangible, sustainable results to our customers, by helping them transform their behavior, business models, processes, and IT to reap the full benefits of cloud technology adoption, innovation, and improved effectiveness. Atos offers Cloud Transformation services that provide a predictable process with clearly defined outcomes, keeping risk low, all while maintaining simple and predictable costs. Our standardized process includes four major milestones, at outlined in Figure 16:

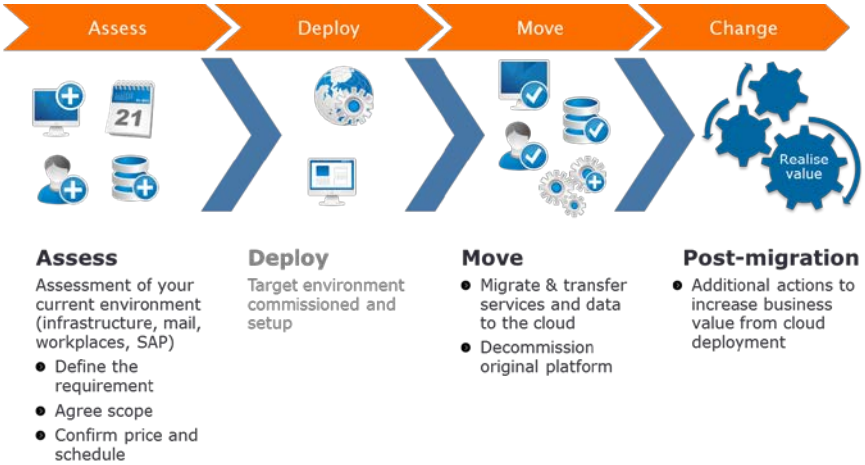


Figure 21. Cloud Transformation Process Milestones

The modular design of Atos' Cloud Transformation services enables predictability, but also allows for flexibility in solution design to fit each Purchasing Entity's needs. Some of the more common modules in the clearly defined assessment process include the following:

- Infrastructure assessment
- Infrastructure sizing assessment
- Application discovery and categorization
- Move Group definition and planning assessment
- Single sign-on requirement assessment
- Hybrid cloud usage assessment
- Cloud mail systems assessment
- Active Directory assessment

Upon completion of modular assessments, Atos has the ability to model workflows, proactively identify outcomes, and utilize fewer resources. Ultimately, the Purchasing Entity will be able to easily validate the processes, have confidence in the outcomes, and reduce costs of transformation.

As part of Atos' cloud transformation overall services portfolio, we offer Infrastructure2Cloud, which is a highly prescriptive offering for server and application workloads migration planning to cloud for Purchasing Entities. Infrastructure2Cloud ensures not only that applications and servers will be virtualized and transferred to a cloud infrastructure, but also that they are delivered fully compliant and up to the latest standards with minimal downtime and impact to business. Atos offers a number of automated tools and processes to promote accelerated migration, including P2V, V2V (X2X), virtual bulk move, storage migration, and cloud app development frameworks.

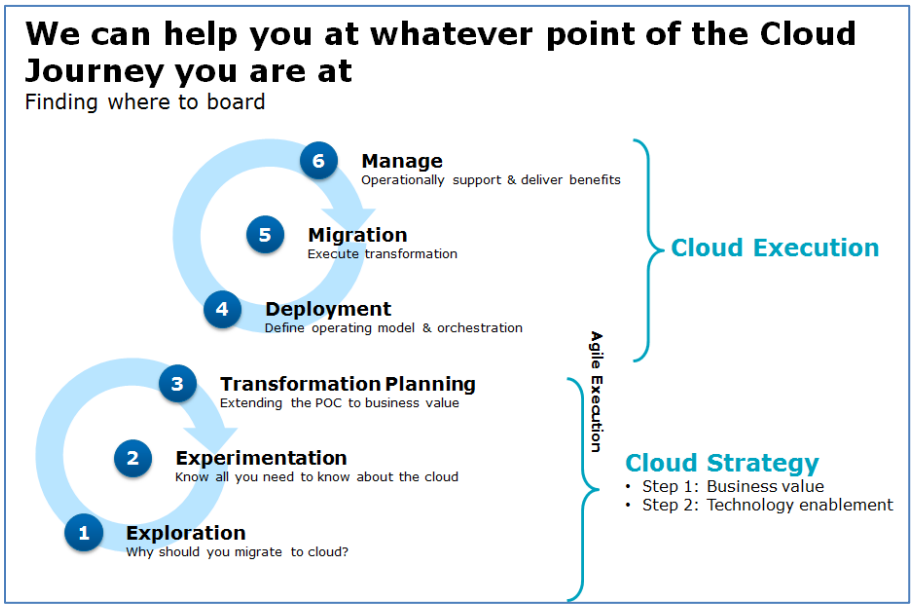


Figure 22. Atos Cloud Consulting Service Portfolio

Atos can demonstrate a great deal of flexibility in delivering our Cloud Consulting Service portfolio, shown in Figure 17, into participating the Lead State entities, whether it is executing one of our packaged service offerings or customizing an engagement into the

cloud fabric specifically based on the needs and entry point of the Lead State member entity.

8.22 (E) SUPPORTING INFRASTRUCTURE

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

The Purchasing Entity would be responsible for providing its own end-user hardware and the WAN connectivity to the Atos Cloud Services data centers.

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

The Purchasing Entity will be financially responsible for the procurement, installation, and ongoing management of the WAN circuits and associated hardware (routers, cards, etc.).

8.23 (E) ALIGNMENT OF CLOUD COMPUTING REFERENCE ARCHITECTURE

Clarify how your 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).

Atos' Cloud Services not only meets all of the criteria documented in the NIST Special Publication 800-145 (The NIST Definition of Cloud Computing), but also exceeds them in all three Service Model definitions—Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

