



Contract # AR2497

## STATE OF UTAH COOPERATIVE CONTRACT

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

NTT DATA, Inc.

100 City Square

Boston

City

Name

Address

MA

State

02129

Zip

### LEGAL STATUS OF CONTRACTOR

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

Contact Person William Baver Phone #617-241-9200 Email william.baver@nttdata.com

Vendor # VC205720 Commodity Code # 920-05

2. GENERAL PURPOSE OF CONTRACT: Contractor is permitted to provide the Cloud Solutions identified in Attachment B to Participating States once a Participating Addendum has been signed
3. PROCUREMENT PROCESS: This contract is entered into as a result of the procurement process on Bid# CH16012.
4. CONTRACT PERIOD: Effective Date: 09/16/2016 Termination Date: 09/15/2026 unless terminated early or extended in accordance with the terms and conditions of this contract. Note: Pursuant to Solicitation #CH16012, Contract must re-certify its qualifications each year.
5. Administrative Fee, as described in the Solicitation and Attachment A: The Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services.
6. ATTACHMENT A: NASPO ValuePoint Master Terms and Conditions, including that attached Exhibits  
ATTACHMENT B: Scope of Services Awarded to Contractor  
ATTACHMENT C: Pricing Discounts and Pricing Schedule  
ATTACHMENT D: Contractor's Response to Solicitation #CH16012

**Any conflicts between Attachments will be resolved in accordance with Section 1 of Attachment A.**

8. DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:
- All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this contract.
  - Utah 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 NTT DATA, Inc.

*Timothy Conway*  
Contractor's signature

9/20/2016  
Date

TIMOTHY CONWAY  
Type or Print Name and Title

STATE  
*[Signature]*  
for Director, Division of Purchasing

9.26.16  
Date

Christopher Hughes

Division of Purchasing Contact Person

801-538-3254

Telephone Number

Fax Number

christopherhughes@utah.gov

Email

(Revision 16 June 2016)



## **Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions**

### **1. Master Agreement Order of Precedence**

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

- (1) A Participating Entity's Participating Addendum<sup>1</sup> ("PA");
- (2) NASPO ValuePoint Master Agreement Terms & Conditions, including the applicable Exhibits<sup>2</sup> to the Master Agreement;
- (3) Statement of Work, if any
- (4) The Solicitation;
- (5) Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State; and
- (6) 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.

---

<sup>1</sup> A Sample Participating Addendum will be published after the contracts have been awarded.

<sup>2</sup> The Exhibits comprise the terms and conditions for the service models: PaaS, IaaS, and SaaS.

**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 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 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 may have control over operating systems, storage, deployed applications; and possibly limited

control of select networking components (e.g., host firewalls).

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

**Statement of Work** means a written statement and its exhibits in a that describes the Purchasing Entity's and Contractor's service requirements.

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

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

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

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

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

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

**8. Confidentiality, Non-Disclosure, and Injunctive Relief**

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

b. Non-Disclosure. Contractor shall hold Confidential Information in confidence, using at least the industry standard of confidentiality, and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than what is necessary to the performance of Orders placed under this Master Agreement. Contractor shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. Contractor shall use commercially reasonable efforts to assist Purchasing Entity in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the generality of the foregoing, Contractor shall advise Purchasing Entity, applicable Participating Entity, and the Lead State immediately if Contractor learns or has reason

to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Master Agreement, and Contractor shall at its expense cooperate with Purchasing Entity in seeking injunctive or other equitable relief in the name of Purchasing Entity or Contractor against any such person. Except as directed by Purchasing Entity, Contractor will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at Purchasing Entity's request, Contractor shall turn over to Purchasing Entity all documents, papers, and other matter in Contractor's possession that embody Confidential Information. Notwithstanding the foregoing, Contractor may keep one copy of such Confidential Information necessary for quality assurance, audits and evidence of the performance of this Master Agreement.

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

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

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

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

## **10. Defaults and Remedies**

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

- (1) Nonperformance of contractual requirements; or
- (2) A material breach of any term or condition of this Master Agreement; or
- (3) Any certification, representation or warranty by Contractor in response to the

solicitation or in this Master Agreement that proves to be untrue or materially misleading; or

(4) Institution of proceedings under any bankruptcy, insolvency, reorganization or similar law, by or against Contractor, or the appointment of a receiver or similar officer for Contractor or any of its property, which is not vacated or fully stayed within thirty (30) calendar days after the institution or occurrence thereof; or

(5) Any default specified in another section of this Master Agreement.

b. Upon the occurrence of an event of default, either party shall issue a written notice of default, identifying the nature of the default, and providing a period of 30 calendar days in which the other party shall have an opportunity to cure the default. The Lead State shall not be required to provide advance written notice or a cure period and may immediately terminate this Master Agreement in whole or in part if the Lead State, in its sole discretion, determines that it is reasonably necessary to preserve public safety or prevent immediate public crisis. Time allowed for cure shall not diminish or eliminate 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, but for the avoidance of doubt such Master Agreement shall remain in force for any then-current Participating Addendums, which shall not be terminated by virtue of termination of this Master Agreement; and

(3) Suspend Contractor from being able to respond to future bid solicitations issued pursuant to this Master Agreement; and

(4) Suspend Contractor's participation in this Master Agreement;

d. Unless otherwise specified in a Participating Addendum, in the event of a default under a Participating Addendum, only the Participating Entity shall provide a written notice of default and opportunity to cure 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 and Contractor under the Participating Addendum and 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 third party claims, damages or causes of action including reasonable attorneys' fees and related costs for any death, injury, or damage to tangible property arising directly or indirectly from the negligence or willful misconduct of the Contractor, its employees or subcontractors or volunteers, at any tier, relating to the performance under the Master Agreement. Notwithstanding anything to the contrary contained herein, Contractor has no obligation for any indemnification claim arising out of or resulting from the acts or omissions of Participating Entities or Purchasing Entities or any of their respective employees, contractors or agents.

b. Indemnification – Intellectual Property. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, Purchasing Entities, along with their officers, agents, and employees as well as any person or entity for which they may be liable ("Indemnified Party"), from and against third party claims, damages or causes of action including reasonable attorneys' fees and related costs arising out of the claim that Contractor's Product or its use, infringes Intellectual Property rights ("Intellectual Property Claim") of another person or entity.

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

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

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

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

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

(2) The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of an Intellectual Property Claim. Even if the Indemnified Party

fails to provide reasonable notice, the Contractor shall not be relieved from its obligations unless the Contractor can demonstrate that it was prejudiced in defending the Intellectual Property Claim resulting in increased expenses or loss to the Contractor and then only to the extent of the prejudice or expenses. If the Contractor promptly and reasonably investigates and defends any Intellectual Property Claim, it shall have control over the defense and settlement of it. However, the Indemnified Party must consent in writing for any money damages or obligations for which it may be responsible. The Indemnified Party shall furnish, at the Contractor's reasonable request and expense, information and assistance necessary for such defense. If the Contractor fails to vigorously pursue the defense or settlement of the Intellectual Property Claim, the Indemnified Party may assume the defense or settlement of it and the Contractor shall be liable for all costs and expenses, including reasonable attorneys' fees and related costs, incurred by the Indemnified Party in the pursuit of the Intellectual Property Claim. Unless otherwise agreed in writing, this section is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.

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

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

## **16. Insurance**

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

b. Coverage shall be written on a claims or 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	<b>Data Breach and Privacy/Cyber Liability including Technology Errors and Omissions</b> 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 have a condition that they not be revoked by the insurer without notice of revocation thereof having been given to Purchasing Entity and Participating Entity by the insurance carrier or 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 without the named Participating State having been given written notice, and (3) provides that the Contractor's liability insurance policy shall be primary, with any liability insurance of any Participating State as secondary and noncontributory. Unless otherwise agreed in any Participating Addendum, the Participating Entity's rights and Contractor's obligations are the same as those specified in the first sentence of this subsection. Before performance of any Purchase Order issued after execution of a Participating Addendum authorizing it, the Contractor shall provide to a Purchasing Entity or Participating Entity who requests it the same information described in this subsection.

e. Contractor shall furnish to the Lead State, Participating Entity, and, on request, the Purchasing Entity copies of certificates of all required insurance within thirty (30)

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

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

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

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

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

## **19. Ordering**

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

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

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

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

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

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

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

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

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

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

## **20. Participants and Scope**

a. Contractor may not deliver Services under this Master Agreement until a Participating

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

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

c. Unless otherwise stipulated in a Participating Entity's Participating Addendum, specific services accessed through the NASPO ValuePoint cooperative Master Agreements for Cloud Services by state executive branch agencies, as required by a Participating Entity's statutes, are subject to the authority and approval of the Participating Entity's Chief Information Officer's Office<sup>3</sup>.

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.

---

<sup>3</sup> 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.

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

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

**21. Payment:** Unless otherwise stipulated in the Participating Addendum, Payment shall 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 an amount of an invoice that is disputed in good faith. 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 may be remitted by electronic clearing house or mail. Payments may be made via a State or political subdivision "Purchasing Card" with no additional charge.

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

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

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

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

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

**25. Purchasing Entity Data:** Purchasing Entity retains full right and title to Data provided by it and any Data derived therefrom, including metadata. Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party (excluding Contractor's attorneys and auditors) 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 no more than annually (unless required by ruling), upon reasonable notice and during normal work hours, 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 (excluding personnel files, payroll records and related cost information) 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 commercially reasonable efforts to restore or assist in restoring the system to operational capacity.

**29. Title to Product:** If access to the Product requires an application program interface (API), Contractor shall convey to Purchasing Entity an irrevocable and perpetual license to use the API.

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

**31. Warranty:** 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. Contractor will perform materially as described in this Master Agreement, SLA, Statement of Work, including any performance representations contained in the Contractor's response to the Solicitation by the Lead State.

c. Contractor represents and warrants that the representations contained in its response to the Solicitation by the Lead State.



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

e. The Services provided by the Contractor are compatible with and will operate successfully with any environment (including web browser and operating system) specified by the Contractor in its response to the Solicitation by the Lead State.

f. The Contractor warrants that it will use commercially reasonable efforts to cause the Products it provides under this Master Agreement to be free of malware. The Contractor must use industry-leading technology to detect and remove worms, Trojans, rootkits, rogues, dialers, and spyware.

Contractor's sole liability for any warranty claim under Section 31(b) shall be for Contractor to re-perform the deficient Services, or, if Contractor fails to remedy such deficiency, to void the amount invoiced for the deficient Services. Contractor shall have no obligation with respect to a warranty claim if the claim is the result of third-party hardware or software failures, or the actions of Lead State, Purchasing Entity or Participating Entity, or a third party. ALL SOFTWARE AND HARDWARE PROVIDED OR INSTALLED BY CONTRACTOR ARE SUBJECT EXCLUSIVELY TO THE RESPECTIVE MANUFACTURERS WARRANTY.

### **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 Contractor, 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 Contractor, Lead State, Participating Entity, or Purchasing Entity must be in writing. Waiver by the Contractor, 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:** Except as may be set forth in a Participating Addendum, 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 in the Indemnification Paragraphs above, 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 equal to two (2) times the charges specified in the Purchase Order for the Services, or parts thereof forming the basis of the Purchasing Entity's claim, (said amount not to exceed a total of twelve (12) months charges payable under the applicable Purchase Order) or (ii) two million dollars (\$2,000,000), 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 or through insurance coverage 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 Section 42 will not apply to claims for bodily injury or death, Section 8, Section 13, and Section 30

**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.

### **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. Unless otherwise stipulated, 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: If the Contractor reasonably believes there has been a security incident, the Contractor shall report it to the Purchasing Entity identified contact (i) immediately, (ii) as soon as possible, or (iii) promptly without out reasonable delay, 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 Contractor's receipt of any subpoena, service of process or other legal request regarding 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 any such subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying 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 and subject to applicable law, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents.
- b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.
- c. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity shall have the right to request immediate replacement of the person.

#### **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. Only where specified 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, at reasonable times and intervals and upon reasonable advance written notice, 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 negatively impact service availability and performance for a material period of time. 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.

**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:** Subject to the SLA, authorized users of the Purchasing Entity with appropriate access rights shall have the ability to import or export its own 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:** As set forth in the Participating Addendum, 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.) As set forth in the Participating Addendum, 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

Offerors must complete the following form to identify the service models your firm offers under this RFP. You may provide a list of the different SaaS, IaaS, and/or PaaS services that you offer, including the Categorization of Risk that you have the ability to store and secure. This document is to provide purchasing entities and eligible users a quick snap shot of the cloud solutions your firm provides.

Service Model:	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered:
SaaS				
IaaS*	X	X	X	Private, Community, Hybrid
PaaS				

\*Compute services for Windows, Linux, AIX, iSeries (IaaS)

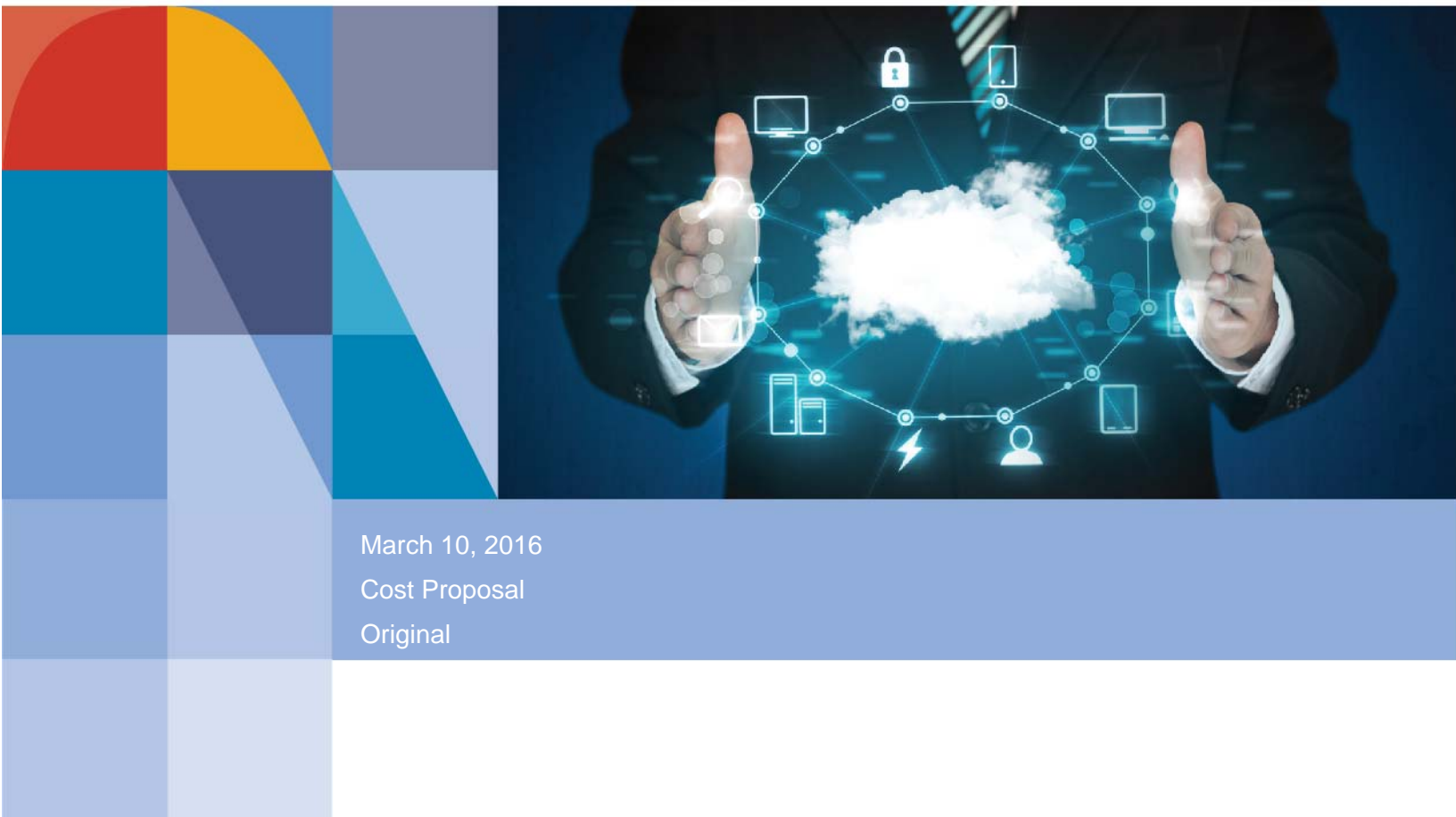
\*DR as a Service (DRaaS)

\*Desktop as a Service (DaaS or VDI)

\* Remote Infrastructure Management (RIM)

## Proposal for Cloud Solutions

Utah Solicitation Number: CH16012



March 10, 2016

Cost Proposal

Original

**NTT DATA, Inc.**

**Attention: Christopher Hughes, Assistant Director**  
State of Utah Division of Purchasing  
3150 State Office Building, Capitol Hill  
Salt Lake City, Utah 84114-1061  
[christopherhughes@utah.gov](mailto:christopherhughes@utah.gov)  
801-538-3254

Table of Contents

---

Cover Letter ..... 1

1. Cost Proposal (Attachment G)..... 2

Table of Exhibits

---

Exhibit 1. Hourly Rates .....2

Exhibit 2. IaaS Price List – Infrastructure .....4

Exhibit 3. IaaS Price List – Remote Infrastructure Management (RIM) .....6

Exhibit 4. IaaS Price List – Help Desk .....9

Exhibit 5. IaaS Price List – Computer Resources and Services ..... 10

Exhibit 6. IaaS Price List – Software ..... 11

Exhibit 7. Desktop as a Service (DaaS) Price List ..... 16

Exhibit 8. Glossary of Descriptions and Terms Used.....23



## Cover Letter

---

March 8, 2016

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

Dear Mr. Hughes:

On behalf of NTT DATA, I am pleased to present a pricing table for our cloud services based on the IaaS components we outlined in our technical response. We have developed a pricing catalog that groups our services into cloud service components, software, resources, and desktop as a service. These cost elements are for services within our cloud environment or to provide services for moves into our cloud environment. To the extent that organizations you represent require a custom-built cloud infrastructure, pricing will need to take place separately.

For this price structure, we will evaluate our cost basis on an annual basis and we reserve the right to make updates to the base price annually. The discount percentage included in our price list will remain constant and in effect for the term of the agreement.

Also, our pricing will honor the 0.25 percent fee outlined in the agreement. This is a fee we agree will be levied by the National Association of State Procurement Officials (NASPO), in accordance with the terms of the RFP.

In this document, you will also find a set of tables that itemize services and service categories, the list price, and then the discounted price. All services outlined have been discounted 5 percent.

If you have any questions, please do not hesitate to contact Bill Baver, a vice president in NTT DATA Public Sector, our business unit devoted to addressing the unique needs of government organizations. Bill can be contacted by email at [William.Baver@nttdata.com](mailto:William.Baver@nttdata.com), by telephone at 610-213-0255, or at the following address: 1660 International Drive, Suite 300, McLean, Virginia 22102.

We look forward to the opportunity to be considered as a cloud provider through your master agreement.

Sincerely,



Timothy Conway  
President, Public Sector

## 1. Cost Proposal (Attachment G)

The following tables document our hourly rates, discounts, itemized pricing and other pricing information.

### Exhibit 1. Hourly Rates

**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.

<b>Software as a Service</b>	<b>Discount %</b>	N/A
<b>Infrastructure as a Service</b>	<b>Discount %</b>	5.00%
<b>Platform as a Services</b>	<b>Discount %</b>	N/A
<b>Value Added Services</b>	<b>Discount %</b>	5.00%

The following hourly rates for Additional Value Added Services represent the AVERAGE discounted rate for a variety of disparate skills and experience levels, and are provided for illustrative purposes only. Please refer to our detailed rate tables which are included below for rates for specific skills and experience levels.

Hourly rates stated here and in the following Exhibits (price list tables) include all applicable labor rates, overhead costs, and fees, but do not include any per diem and/or travel costs. Per Diem and/or travel costs will be determined as necessary in discussion with each individual purchasing entity.

### Additional Value Added Services:

<b>Maintenance Services</b>	<b>Onsite Hourly Rate \$</b>	111.27 *
	<b>Remote Hourly Rate \$</b>	111.27
<b>Professional Services</b>		
• Deployment Services	<b>Onsite Hourly Rate \$</b>	127.93 *
	<b>Remote Hourly Rate \$</b>	127.93
• Consulting/Advisory Services	<b>Onsite Hourly Rate \$</b>	120.65 *
	<b>Remote Hourly Rate \$</b>	120.65
• Architectural Design Services	<b>Onsite Hourly Rate \$</b>	219.85 *
	<b>Remote Hourly Rate \$</b>	219.85
• Statement of Work Services	<b>Onsite Hourly Rate \$</b>	141.56 *
	<b>Remote Hourly Rate \$</b>	141.56
<b>Partner Services</b>	<b>Onsite Hourly Rate \$</b>	N/A

	<b>Remote Hourly Rate \$</b>	<u>N/A</u>
<b>Training Deployment Services</b>	<b>Onsite Hourly Rate \$</b>	<u>139.42 *</u>
	<b>Remote Hourly Rate \$</b>	<u>139.42</u>

\* Onsite rates do not include travel and expense (per diem) costs.

**Discount – 5.00%**

**Exhibit 2. IaaS Price List – Infrastructure**

Service Area	Component Code	Component	Metric Unit	Period	Type	List Price	Discounted Price
Virtual Machine (VM)	VM-CPU-No DR	CPU (with No DR)	GHz	Monthly	Technology	\$17.45	\$16.58
	VM-CPU-Cold DR	CPU (with Cold DR)	GHz	Monthly	Technology	\$19.63	\$18.65
	VM-CPU-Warm DR	CPU (with Warm DR)	GHz	Monthly	Technology	\$19.63	\$18.65
	VM-RAM-No DR	RAM (with No DR)	GB	Monthly	Technology	\$21.81	\$20.72
	VM-RAM-Cold DR	RAM (with Cold DR)	GB	Monthly	Technology	\$24.00	\$22.80
	VM-RAM-Warm DR	RAM (with Warm DR)	GB	Monthly	Technology	\$24.00	\$22.80
IBM Power 7 (AIX)	AIX-CPU-No DR	CPU (AIX with No DR)	Core	Monthly	Technology	\$872.59	\$828.96
	AIX-CPU-Cold DR	CPU (AIX with Cold DR)	Core	Monthly	Technology	\$1,036.20	\$984.39
	AIX-CPU-Warm DR	CPU (AIX with Warm DR)	Core	Monthly	Technology	\$1,036.20	\$984.39
	AIX-RAM-No DR	RAM (AIX with No DR)	GB	Monthly	Technology	\$21.81	\$20.72
	AIX-RAM-Cold DR	RAM (AIX with Cold DR)	GB	Monthly	Technology	\$24.00	\$22.80
	AIX-RAM-Warm DR	RAM (AIX with Warm DR)	GB	Monthly	Technology	\$24.00	\$22.80
IBM Power 7 (Linux)	Linux-CPU-No DR	CPU (Linux with No DR)	Core	Monthly	Technology	\$872.59	\$828.96
	Linux-CPU-Cold DR	CPU (Linux with Cold DR)	Core	Monthly	Technology	\$1,036.20	\$984.39
	Linux-CPU-Warm DR	CPU (Linux with Warm DR)	Core	Monthly	Technology	\$1,036.20	\$984.39
	Linux-RAM-No DR	RAM (Linux with No DR)	GB	Monthly	Technology	\$21.81	\$20.72
	Linux-RAM-Cold DR	RAM (Linux with Cold DR)	GB	Monthly	Technology	\$24.00	\$22.80
	Linux-RAM-Warm DR	RAM (Linux with Warm DR)	GB	Monthly	Technology	\$24.00	\$22.80
IBM Power 7 (iSeries)	iSeries-CPU-No DR	CPU (iSeries with No DR)	Core	Monthly	Technology	\$3,054.07	\$2,901.37
	iSeries-CPU-Cold DR	CPU (iSeries with Cold DR)	Core	Monthly	Technology	\$3,272.22	\$3,108.61
	iSeries-CPU-Warm DR	CPU (iSeries with Warm DR)	Core	Monthly	Technology	\$3,272.22	\$3,108.61
	iSeries-RAM-No DR	RAM (iSeries with No DR)	GB	Monthly	Technology	\$24.00	\$22.80
	iSeries-RAM-Cold DR	RAM (iSeries with Cold DR)	GB	Monthly	Technology	\$26.18	\$24.87
	iSeries-RAM-Warm DR	RAM (iSeries with Warm DR)	GB	Monthly	Technology	\$26.18	\$24.87

Service Area	Component Code	Component	Metric Unit	Period	Type	List Price	Discounted Price
M-Series Server	Physical Server-4C (2.7GHz),32GB,60GB SSD	Physical Server - 4C (2.7GHz)/32GB/60GB SSD	Per Server	Monthly	Technology	\$381.76	\$362.67
Storage (Economy)	SAN-Economy-No DR	SAN (with No DR)	GB	Monthly	Technology	\$0.22	\$0.21
	SAN-Economy-Cold DR	SAN (with Cold DR)	GB	Monthly	Technology	\$0.25	\$0.24
	SAN-Economy-Warm DR	SAN (with Warm DR)	GB	Monthly	Technology	\$0.22	\$0.21
Storage (Optimized)	SAN-Optimized-No DR	SAN (with No DR)	GB	Monthly	Technology	\$0.44	\$0.41
	SAN-Optimized-Cold DR	SAN (with Cold DR)	GB	Monthly	Technology	\$0.50	\$0.48
	SAN-Optimized-Warm DR	SAN (with Warm DR)	GB	Monthly	Technology	\$0.44	\$0.41
Provisioning	Provisioning	Provisioning (if requested)	Per Server	One-Time	Service	\$278.25	\$264.34
Data Backup	Data Backup Setup	Backup Configuration	VM	One-Time	Service	\$83.48	\$79.30
	Data Backup	Per GB Protected	GB	Monthly	Technology	\$0.27	\$0.26
Disaster Recovery (DR)	DR Setup-Cold DR	DR Configuration (for Cold DR)	VM	One-Time	Service	\$83.48	\$79.30
	DR Setup-Warm DR	DR Configuration (for Warm DR)	VM	One-Time	Service	\$83.48	\$79.30
	DR Tests	DR Tests - Amortized	VM	Monthly	Service	\$5.57	\$5.29
	Remote Site SAN-Economy	Remote Site SAN Storage (Economy)	GB	Monthly	Technology	\$0.22	\$0.21
	Remote Site SAN-Optimized	Remote Site SAN Storage (Optimized)	GB	Monthly	Technology	\$0.44	\$0.41
	Network Replication	Network Replication Costs	GB	Monthly	Technology	\$0.17	\$0.17
	Site Recovery Manager	DR Replication License	Server	Monthly	Technology	\$39.27	\$37.30
Other Infrastructure Support	Internet Bandwidth	Internet Bandwidth	Mbps	Monthly	Technology	\$32.72	\$31.09
	VPN Tunnel	VPN Tunnel (if requested)	Per Connection	One-Time	Service	\$333.90	\$317.21
	External IP	External IP	Per IP	Monthly	Technology	\$16.36	\$15.54
	Firewall - ASAv5	Firewall w/100mbps Throughput - ASAv5	Per Host Site	Monthly	Technology	\$272.69	\$259.05
	Firewall - ASAv10	Firewall w/1gbps Throughput - ASAv10	Per Host Site	Monthly	Technology	\$414.48	\$393.76
	Firewall - ASAv30	Firewall w/2gbps Throughput -	Per Host	Monthly	Technology	\$818.06	\$777.15

Service Area	Component Code	Component	Metric Unit	Period	Type	List Price	Discounted Price
		ASAv30	Site				
	Firewall Configuration	Firewall Configuration	One Time	One-Time	Service	\$333.90	\$317.21
	CSR 100v	Cloud Services Router - 100mbps - CSR 100v	Per CSR	Monthly	Technology	\$350.13	\$332.62
	CSR 250v	Cloud Services Router - 250mbps - CSR 250v	Per CSR	Monthly	Technology	\$545.37	\$518.10
	CSR 1000v	Cloud Services Router - 1gbps - CSR 1000v	Per CSR	Monthly	Technology	\$584.64	\$555.40
	CSR Configuration	CSR Configuration	Per CSR	One-Time	Service	\$333.90	\$317.21
	Load Balancer-Layer 3	Load Balancer (Layer 3)	VIP	Monthly	Technology	\$38.18	\$36.27
	Load Balancer-Layer 4	Load Balancer (Layer 4)	VIP	Monthly	Technology	\$163.61	\$155.43
	Load Balancer-Layer 7	Load Balancer (Layer 7)	VIP	Monthly	Technology	\$327.22	\$310.86
	VPN User Pack	200 User VPN Pack	200 Pack	Monthly	Service	\$44.52	\$42.29
	Cross Connect - Monthly	Cross Connect - Monthly	Each	Monthly	Technology	\$299.95	\$284.96
	Cross Connect - One-Time	Cross Connect - One-Time	Each	One-Time	Technology	\$381.76	\$362.67
	Switchport	Switchport	Each	Monthly	Technology	\$81.81	\$77.72
	Colocation Space	Colocation Space	Per RU	Monthly	Technology	\$163.61	\$155.43

**Discount – 5.00%**

**Exhibit 3. IaaS Price List – Remote Infrastructure Management (RIM)**

Service Area	Component Code	Component	Metric Unit	Period	Type	List Price	Discounted Price
RIM Services (Hosted)	RIM-Bronze-Win Srvr	Bronze (Monitoring Only)	VM	Monthly	Service	\$47.49	\$45.11
	RIM-Silver-Win Srvr	Silver (Bronze+OS)	VM	Monthly	Service	\$237.44	\$225.57
	RIM-Gold-Win Srvr	Gold (Silver + App)	VM	Monthly	Service	\$385.84	\$366.55
	RIM-Bronze-Linux	Bronze (Monitoring Only)	VM	Monthly	Service	\$47.49	\$45.11

Service Area	Component Code	Component	Metric Unit	Period	Type	List Price	Discounted Price
	RIM-Silver-Linux	Silver (Bronze+OS)	VM	Monthly	Service	\$237.44	\$225.57
	RIM-Gold-Linux	Gold (Silver + App)	VM	Monthly	Service	\$385.84	\$366.55
	RIM-Bronze-AIX	Bronze (Monitoring Only)	LPAR	Monthly	Service	\$47.49	\$45.11
	RIM-Silver-AIX	Silver (Bronze+OS)	LPAR	Monthly	Service	\$308.67	\$293.24
	RIM-Gold-AIX	Gold (Silver + App)	LPAR	Monthly	Service	\$502.19	\$477.08
RIM Setup (Hosted)	RIM Setup-Bronze-Win Svr	Bronze Service Setup	VM	One-Time	Service	\$71.23	\$67.67
	RIM Setup-Silver-Win Svr	Silver Service Setup	VM	One-Time	Service	\$237.44	\$225.57
	RIM Setup-Gold-Win Svr	Gold Service Setup	VM	One-Time	Service	\$356.16	\$338.35
	RIM Setup-Bronze-Linux	Bronze Service Setup	VM	One-Time	Service	\$71.23	\$67.67
	RIM Setup-Silver-Linux	Silver Service Setup	VM	One-Time	Service	\$237.44	\$225.57
	RIM Setup-Gold-Linux	Gold Service Setup	VM	One-Time	Service	\$356.16	\$338.35
	RIM Setup-Bronze-AIX	Bronze Service Setup	LPAR	One-Time	Service	\$71.23	\$67.67
	RIM Setup-Silver-AIX	Silver Service Setup	LPAR	One-Time	Service	\$237.44	\$225.57
	RIM Setup-Gold-AIX	Gold Service Setup	LPAR	One-Time	Service	\$356.16	\$338.35
RIM Services (Non-Hosted)	RIM - Windows - Non-Hosted - Bronze	Windows (Bronze)	Per Device	Monthly	Service	\$47.49	\$45.11
	RIM - Windows - Non-Hosted - Silver	Windows (Silver)	Per Device	Monthly	Service	\$261.18	\$248.12
	RIM - Windows - Non-Hosted - Gold	Windows (Gold)	Per Device	Monthly	Service	\$415.52	\$394.74
	RIM - Linux - Non-Hosted - Bronze	Linux (Bronze)	Per Device	Monthly	Service	\$47.49	\$45.11
	RIM - Linux - Non-Hosted - Silver	Linux (Silver)	Per Device	Monthly	Service	\$261.18	\$248.12
	RIM - Linux - Non-Hosted - Gold	Linux (Gold)	Per Device	Monthly	Service	\$415.52	\$394.74
	RIM - AIX - Non-Hosted - Bronze	AIX (Bronze)	Per Device	Monthly	Service	\$47.49	\$45.11
	RIM - AIX - Non-Hosted - Silver	AIX (Silver)	Per Device	Monthly	Service	\$339.54	\$322.56
	RIM - AIX - Non-Hosted - Gold	AIX (Gold)	Per Device	Monthly	Service	\$540.18	\$513.17
RIM Setup (Non-Hosted)	RIM Setup - Windows - Non-Hosted - Bronze	Windows (Bronze)	Per Device	One-Time	Service	\$71.23	\$67.67
	RIM Setup - Windows - Non-Hosted - Silver	Windows (Silver)	Per Device	One-Time	Service	\$237.44	\$225.57

Service Area	Component Code	Component	Metric Unit	Period	Type	List Price	Discounted Price
	RIM Setup - Windows - Non-Hosted - Gold	Windows (Gold)	Per Device	One-Time	Service	\$356.16	\$338.35
	RIM Setup - Linux - Non-Hosted - Bronze	Linux (Bronze)	Per Device	One-Time	Service	\$71.23	\$67.67
	RIM Setup - Linux - Non-Hosted - Silver	Linux (Silver)	Per Device	One-Time	Service	\$237.44	\$225.57
	RIM Setup - Linux - Non-Hosted - Gold	Linux (Gold)	Per Device	One-Time	Service	\$356.16	\$338.35
	RIM Setup - AIX - Non-Hosted - Bronze	AIX (Bronze)	Per Device	One-Time	Service	\$71.23	\$67.67
	RIM Setup - AIX - Non-Hosted - Silver	AIX (Silver)	Per Device	One-Time	Service	\$237.44	\$225.57
	RIM Setup - AIX - Non-Hosted - Gold	AIX (Gold)	Per Device	One-Time	Service	\$356.16	\$338.35
RIM Network Devices (Hosted)	RIM - Network Device - Hosted - Bronze	Bronze	Per Device	Monthly	Service	\$35.62	\$33.84
	RIM - Network Device - Hosted - Silver	Silver	Per Device	Monthly	Service	\$219.63	\$208.65
	RIM - Network Device - Hosted - Gold	Gold	Per Device	One-Time	Service	\$267.12	\$253.76
RIM Network Devices (Non-Hosted)	RIM - Network Device - Non-Hosted - Bronze	Bronze	Per Device	Monthly	Service	\$35.62	\$33.84
	RIM - Network Device - Non-Hosted - Silver	Silver	Per Device	Monthly	Service	\$219.63	\$208.65
	RIM - Network Device - Non-Hosted - Gold	Gold	Per Device	One-Time	Service	\$267.12	\$253.76
RIM Setup Network Devices (Hosted)	RIM Setup - Network Device - Hosted - Bronze	Bronze	Per Device	Monthly	Service	\$71.23	\$67.67
	RIM Setup - Network Device - Hosted - Silver	Silver	Per Device	Monthly	Service	\$237.44	\$225.57
	RIM Setup - Network Device - Hosted - Gold	Gold	Per Device	One-Time	Service	\$356.16	\$338.35
RIM Setup Network Devices (Non-Hosted)	RIM Setup - Network Device - Non-Hosted - Bronze	Bronze	Per Device	Monthly	Service	\$71.23	\$67.67
	RIM Setup - Network Device - Non-Hosted - Silver	Silver	Per Device	Monthly	Service	\$237.44	\$225.57
	RIM Setup - Network Device - Non-Hosted - Gold	Gold	Per Device	One-Time	Service	\$356.16	\$338.35



Service Area	Component Code	Component	Metric Unit	Period	Type	List Price	Discounted Price
	Hosted - Gold						

**Discount – 5.00%**

**Exhibit 4. IaaS Price List – Help Desk**

Service Area	Component Code	Component	Metric Unit	Period	Type	List Price	Discounted Price
Remedy Only	Remedy-Fixed	Fixed	Per License	Monthly	Technology	\$201.79	\$191.70
	Remedy-Floating	Floating	Per License	Monthly	Technology	\$299.95	\$284.96
Service/ Help Desk	HelpDesk Admin - Junior - US	HelpDesk Admin - Junior - US	Per Hour	Hourly	Labor	\$67.73	\$64.35
	HelpDesk Admin - Junior - Can	HelpDesk Admin - Junior - Can	Per Hour	Hourly	Labor	\$50.80	\$48.26
	HelpDesk Admin - Junior - India	HelpDesk Admin - Junior - India	Per Hour	Hourly	Labor	\$19.19	\$18.23
	HelpDesk Admin - Intermediate - US	HelpDesk Admin - Intermediate - US	Per Hour	Hourly	Labor	\$79.02	\$75.07
	HelpDesk Admin - Intermediate - Can	HelpDesk Admin - Intermediate - Can	Per Hour	Hourly	Labor	\$62.09	\$58.99
	HelpDesk Admin - Intermediate - India	HelpDesk Admin - Intermediate - India	Per Hour	Hourly	Labor	\$23.71	\$22.52
	HelpDesk Admin - Senior - US	HelpDesk Admin - Senior - US	Per Hour	Hourly	Labor	\$84.67	\$80.43
	HelpDesk Admin - Senior - Can	HelpDesk Admin - Senior - Can	Per Hour	Hourly	Labor	\$73.38	\$69.71
	HelpDesk Admin - Senior - India	HelpDesk Admin - Senior - India	Per Hour	Hourly	Labor	\$30.48	\$28.96
	HelpDesk Engr - Junior - US	HelpDesk Engr - Junior - US	Per Hour	Hourly	Labor	\$79.02	\$75.07
	HelpDesk Engr - Junior - Can	HelpDesk Engr - Junior - Can	Per Hour	Hourly	Labor	\$73.38	\$69.71
	HelpDesk Engr - Junior - India	HelpDesk Engr - Junior - India	Per Hour	Hourly	Labor	\$23.71	\$22.52
	HelpDesk Engr - Intermediate - US	HelpDesk Engr - Intermediate - US	Per Hour	Hourly	Labor	\$84.67	\$80.43

Service Area	Component Code	Component	Metric Unit	Period	Type	List Price	Discounted Price
	HelpDesk Engr - Intermediate - Can	HelpDesk Engr - Intermediate - Can	Per Hour	Hourly	Labor	\$95.96	\$91.16
	HelpDesk Engr - Intermediate - India	HelpDesk Engr - Intermediate - India	Per Hour	Hourly	Labor	\$30.48	\$28.96
	HelpDesk Engr - Senior - US	HelpDesk Engr - Senior - US	Per Hour	Hourly	Labor	\$107.25	\$101.88
	HelpDesk Engr - Senior - Can	HelpDesk Engr - Senior - Can	Per Hour	Hourly	Labor	\$95.96	\$91.16
	HelpDesk Engr - Senior - India	HelpDesk Engr - Senior - India	Per Hour	Hourly	Labor	\$36.12	\$34.32

**Discount – 5.00%**

**Exhibit 5. IaaS Price List – Computer Resources and Services**

Service Area	Component Code	Component	Metric Unit	Period	Type	List Price	Discounted Price
Computer Resources & Services	Project/Program Manager	Project/Program Manager	Per Hour	Hourly	Labor	\$169.34	\$160.87
	Technical Architect - Intermediate	Technical Architect - Intermediate	Per Hour	Hourly	Labor	\$180.62	\$171.59
	Technical Architect - Advanced	Technical Architect - Advanced	Per Hour	Hourly	Labor	\$282.23	\$268.11
	Senior Consultant -Intermediate	Senior Consultant -Intermediate	Per Hour	Hourly	Labor	\$124.18	\$117.97
	Senior Consultant -Advanced	Senior Consultant -Advanced	Per Hour	Hourly	Labor	\$169.34	\$160.87
	Consultant - Intermediate	Consultant - Intermediate	Per Hour	Hourly	Labor	\$107.25	\$101.88
	Consultant Advanced	Consultant Advanced	Per Hour	Hourly	Labor	\$107.25	\$101.88
	Sys Admin II Intermediate	Sys Admin II Intermediate	Per Hour	Hourly	Labor	\$124.18	\$117.97
	Sys Admin II Advanced	Sys Admin II Advanced	Per Hour	Hourly	Labor	\$169.34	\$160.87
	Sys admin - Junior	Sys admin - Junior	Per Hour	Hourly	Labor	\$84.67	\$80.43
	Sys admin - Intermediate	Sys admin - Intermediate	Per Hour	Hourly	Labor	\$107.25	\$101.88
	Sys admin - Advanced	Sys admin - Advanced	Per Hour	Hourly	Labor	\$107.25	\$101.88
	Database Admin - Intermediate	Database Admin - Intermediate	Per Hour	Hourly	Labor	\$169.34	\$160.87
	Database Admin - Advanced	Database Admin - Advanced	Per Hour	Hourly	Labor	\$180.62	\$171.59

**Discount – 5.00%**

**Exhibit 6. IaaS Price List – Software**

Service Area	Component Code	Component	Metric Unit	Period	Type	List Price	Discounted Price
Software	V28844	DLC-00016 - AppVrtSAL ALNG LicSAPk MVL	Per License	Monthly	Software	\$7.12	\$6.77
	QZ9415	HJA-00774 - BztlkSvrBrnch ALNG LicSAPk MVL 2Lic CoreLic	Per License	Monthly	Software	\$66.04	\$62.74
	QZ9413	F52-02144 - BztlkSvrEnt ALNG LicSAPk MVL 2Lic CoreLic	Per License	Monthly	Software	\$1,153.36	\$1,095.70
	QZ9411	D75-01979 - BztlkSvrStd ALNG LicSAPk MVL 2Lic CoreLic	Per License	Monthly	Software	\$264.45	\$251.23
	TX9033	P2Y-00001 - CloudPltfrmGuest ALNG LicSAPk MVL PerOSE	Per License	Monthly	Software	\$31.16	\$29.61
	TX9031	N5Y-00020 - CloudPltfrmSte ALNG LicSAPk MVL 1Proc	Per License	Monthly	Software	\$4.01	\$3.81
	KL3359	FUD-00009 - CISDataCtr ALNG LicSAPk MVL 1Proc	Per License	Monthly	Software	\$177.63	\$168.75
	NY9548	YJD-00007 - CISStd ALNG LicSAPk MVL 1Proc	Per License	Monthly	Software	\$36.80	\$34.96
	YM4545	FA8-00101 - DynAXHstd ALNG LicSAPk MVL 2Lic PerUsr CoreLic StdCmmrc2CoreSvr	Per License	Monthly	Software	\$650.73	\$618.20
	QQ6087	FA8-00092 - DynAXHstd ALNG LicSAPk MVL PerDvc SAL Ent	Per License	Monthly	Software	\$93.20	\$88.54
	QQ6089	FA8-00093 - DynAXHstd ALNG LicSAPk MVL PerDvc SAL Fnctnl	Per License	Monthly	Software	\$37.25	\$35.39
	QQ6093	FA8-00095 - DynAXHstd ALNG LicSAPk MVL PerDvc SAL SelfServe	Per License	Monthly	Software	\$2.82	\$2.68
	QQ6091	FA8-00094 - DynAXHstd ALNG LicSAPk MVL PerDvc SAL Task	Per License	Monthly	Software	\$13.95	\$13.25
	QQ6095	FA8-00096 - DynAXHstd ALNG LicSAPk MVL PerUsr SAL Ent	Per License	Monthly	Software	\$93.20	\$88.54
	QQ6099	FA8-00098 - DynAXHstd ALNG LicSAPk MVL PerUsr SAL Fnctnl	Per License	Monthly	Software	\$37.25	\$35.39
	QQ6085	FA8-00091 - DynAXHstd ALNG LicSAPk MVL PerUsr	Per License	Monthly	Software	\$2.82	\$2.68

Service Area	Component Code	Component	Metric Unit	Period	Type	List Price	Discounted Price
		SAL SelfServe					
	YM4543	FA8-00100 - DynAXHstd ALNG LicSAPk MVL PerUsr SAL StrSvr	Per License	Monthly	Software	\$27.90	\$26.50
	QQ6097	FA8-00097 - DynAXHstd ALNG LicSAPk MVL PerUsr SAL Task	Per License	Monthly	Software	\$9.35	\$8.88
	Q76815	QHH-00028 - DynCRMSrvPrvdr ALNG LicSAPk MVL SAL	Per License	Monthly	Software	\$36.65	\$34.82
	TE0626	QHH-00089 - DynCRMSrvPrvdr ALNG LicSAPk MVL SAL Bsc	Per License	Monthly	Software	\$13.21	\$12.55
	TE0628	QHH-00090 - DynCRMSrvPrvdr ALNG LicSAPk MVL SAL Esstls	Per License	Monthly	Software	\$3.71	\$3.52
	QV5385	65D-00122 - DynGPHstd ALNG LicSAPk MVL Cstmztn 1Proc	Per License	Monthly	Software	\$77.91	\$74.01
	QQ6083	65D-00121 - DynGPHstd ALNG LicSAPk MVL ExtdHRPayroll 1Proc	Per License	Monthly	Software	\$272.76	\$259.12
	QQ6080	65D-00118 - DynGPHstd ALNG LicSAPk MVL FullUser SAL	Per License	Monthly	Software	\$107.59	\$102.21
	QQ6081	65D-00119 - DynGPHstd ALNG LicSAPk MVL LmtdUser SAL	Per License	Monthly	Software	\$7.87	\$7.47
	TX9029	65D-00123 - DynGPHstd ALNG LicSAPk MVL Std SAL	Per License	Monthly	Software	\$92.01	\$87.41
	YM4541	4CL-00392 - DynNAVHstd ALNG LicSAPk MVL 1Proc CstmztnPk	Per License	Monthly	Software	\$31.16	\$29.61
	QQ6078	4CL-00389 - DynNAVHstd ALNG LicSAPk MVL FullUser SAL	Per License	Monthly	Software	\$107.59	\$102.21
	QQ6079	4CL-00390 - DynNAVHstd ALNG LicSAPk MVL LmtdUser SAL	Per License	Monthly	Software	\$7.87	\$7.47
	TX9028	4CL-00391 - DynNAVHstd ALNG LicSAPk MVL Std SAL	Per License	Monthly	Software	\$92.01	\$87.41
	DM3389	65F-00058 - DynSLHstd ALNG LicSAPk MVL AMESSUsr SAL	Per License	Monthly	Software	\$7.87	\$7.47

Service Area	Component Code	Component	Metric Unit	Period	Type	List Price	Discounted Price
	Q76821	65F-00011 - DynSLHstd ALNG LicSAPk MVL AMFullUsr SAL	Per License	Monthly	Software	\$107.59	\$102.21
	PJ4604	65F-00057 - DynSLHstd ALNG LicSAPk MVL AMLightUsr SAL	Per License	Monthly	Software	\$7.87	\$7.47
	DM4779	65F-00059 - DynSLHstd ALNG LicSAPk MVL BEFullUsr SAL	Per License	Monthly	Software	\$92.01	\$87.41
	GB3297	65F-00060 - DynSLHstd ALNG LicSAPk MVL BELightUsr SAL	Per License	Monthly	Software	\$7.87	\$7.47
	Q76762	9MD-00001 - ExchgBscSAL ALNG LicSAPk MVL	Per License	Monthly	Software	\$0.89	\$0.85
	Q76766	4MH-00001 - ExchgEntPlusSAL ALNG LicSAPk MVL	Per License	Monthly	Software	\$6.38	\$6.06
	Q76764	9MC-00001 - ExchgEntSAL ALNG LicSAPk MVL	Per License	Monthly	Software	\$4.45	\$4.23
	KL3358	9MC-00004 - ExchgEntSAL ALNG LicSAPk MVL forSA	Per License	Monthly	Software	\$0.45	\$0.42
	Q76768	F08-00025 - ExchgStdSAL ALNG LicSAPk MVL	Per License	Monthly	Software	\$2.82	\$2.68
	U34031	F08-00027 - ExchgStdSAL ALNG LicSAPk MVL forSA	Per License	Monthly	Software	\$0.45	\$0.42
	Q76770	F09-00018 - ExchgStdPlusSAL ALNG LicSAPk MVL	Per License	Monthly	Software	\$4.75	\$4.51
	DX5912	M3J-00104 - FrfrntEndpointPrctn ALNG LicSAPk MVL	Per License	Monthly	Software	\$1.19	\$1.13
	ZY4354	7VC-00168 - FrfrntIdnttyMgr ALNG LicSAPk MVL SAL	Per License	Monthly	Software	\$1.63	\$1.55
	DX5908	6TH-00002 - LyncSvrEntPlusSAL ALNG LicSAPk MVL	Per License	Monthly	Software	\$9.94	\$9.45
	DX5902	6RH-00002 - LyncSrvEntSAL ALNG LicSAPk MVL	Per License	Monthly	Software	\$5.64	\$5.36
	GF7445	6RH-00004 - LyncSrvEntSAL ALNG LicSAPk MVL forSA	Per License	Monthly	Software	\$0.45	\$0.42
	DX5905	6SH-00002 - LyncSvrPlusSAL ALNG LicSAPk MVL	Per License	Monthly	Software	\$5.64	\$5.36
	KL3352	6SH-00004 - LyncSvrPlusSAL ALNG LicSAPk MVL forSA	Per License	Monthly	Software	\$0.45	\$0.42
	DX5899	6QH-00002 - LyncSvrStdSAL ALNG LicSAPk MVL	Per License	Monthly	Software	\$1.34	\$1.27
	GF7442	6QH-00004 - LyncSvrStdSAL ALNG LicSAPk MVL	Per License	Monthly	Software	\$0.45	\$0.42

Service Area	Component Code	Component	Metric Unit	Period	Type	List Price	Discounted Price
		forSA					
	U35999	79H-00128 - OfficeMultiLangPk ALNG LicSAPk MVL SAL	Per License	Monthly	Software	\$4.16	\$3.95
	Q76825	79P-01747 - OfficeProPlus ALNG LicSAPk MVL SAL	Per License	Monthly	Software	\$21.96	\$20.87
	Q76823	021-08183 - OfficeStd ALNG LicSAPk MVL SAL	Per License	Monthly	Software	\$16.18	\$15.37
	U34035	T9A-00002 - ProductivitySteSAL ALNG LicSAPk MVL	Per License	Monthly	Software	\$5.94	\$5.64
	U34036	T9A-00003 - ProductivitySteSAL ALNG LicSAPk MVL ForCoreCALSA	Per License	Monthly	Software	\$2.97	\$2.82
	PJ4609	T9A-00001 - ProductivitySteSAL ALNG LicSAPk MVL ForEntCALSA	Per License	Monthly	Software	\$1.19	\$1.13
	U36001	076-04015 - Prjct ALNG LicSAPk MVL SAL	Per License	Monthly	Software	\$23.15	\$21.99
	DM4781	H30-03425 - PrjctPro ALNG LicSAPk MVL SAL w1PrjctSvrSAL	Per License	Monthly	Software	\$38.58	\$36.65
	Q76877	H22-01677 - PrjctSvr ALNG LicSAPk MVL SAL	Per License	Monthly	Software	\$11.87	\$11.28
	Q76860	K63-00006 - ProvisioningSys Win32 ALNG LicSAPk MVL Hosting 1Proc	Per License	Monthly	Software	\$155.82	\$148.03
	QV6833	V6V-00001 - SharePointHosting ALNG LicSAPk MVL	Per License	Monthly	Software	\$1,196.10	\$1,136.30
	Q76840	76P-00840 - SharePointSvr ALNG LicSAPk MVL Ent SAL	Per License	Monthly	Software	\$3.41	\$3.24
	KL3355	76P-01361 - SharePointSvr ALNG LicSAPk MVL Ent SAL forSA	Per License	Monthly	Software	\$0.45	\$0.42
	Q76842	76P-00742 - SharePointSvr ALNG LicSAPk MVL Std SAL	Per License	Monthly	Software	\$3.86	\$3.67
	U34025	76M-01134 - SharePointStdCAL ALNG LicSAPk MVL SAL forSA	Per License	Monthly	Software	\$0.45	\$0.42
	NY9537	D2M-00502 - SQLSvrBsnssIntelligence ALNG LicSAPk MVL SAL	Per License	Monthly	Software	\$28.79	\$27.35
	Q76780	228-05018 - SQLSvrStd ALNG LicSAPk MVL SAL	Per License	Monthly	Software	\$20.33	\$19.31
	NY9547	TFA-00523 - SQLSvrWeb ALNG LicSAPk MVL 2Lic CoreLic	Per License	Monthly	Software	\$11.72	\$11.14

Service Area	Component Code	Component	Metric Unit	Period	Type	List Price	Discounted Price
	NY9533	7JQ-00341 - SQLSvrEntCore ALNG LicSAPk MVL 2Lic CoreLic	Per License	Monthly	Software	\$717.07	\$681.22
	NY9535	7NQ-00302 - SQLSvrStdCore ALNG LicSAPk MVL 2Lic CoreLic	Per License	Monthly	Software	\$186.98	\$177.63
	DC0236	MFF-00504 - SysCtrCltMgmtSte ALNG LicSAPk MVL SAL	Per License	Monthly	Software	\$3.56	\$3.38
	NY9539	J5A-01228 - SysCtrCnfgMgrCltML ALNG LicSAPk MVL SAL	Per License	Monthly	Software	\$3.26	\$3.10
	NY9543	T6L-00249 - SysCtrDatactr ALNG LicSAPk MVL 1Proc	Per License	Monthly	Software	\$62.77	\$59.63
	NY9545	T9L-00249 - SysCtrStd ALNG LicSAPk MVL 1Proc	Per License	Monthly	Software	\$23.15	\$21.99
	QZ9417	W5V-00026 - UserExpVirtSAL ALNG LicSAPk MVL	Per License	Monthly	Software	\$4.60	\$4.37
	U36028	D87-03215 - VisioPro ALNG LicSAPk MVL SAL	Per License	Monthly	Software	\$19.89	\$18.89
	U36029	D86-03116 - VisioStd ALNG LicSAPk MVL SAL	Per License	Monthly	Software	\$9.05	\$8.60
	CQ5540	N5F-00074 - VSPrem ALNG LicSAPk MVL SAL	Per License	Monthly	Software	\$273.65	\$259.97
	CQ5535	C5E-00746 - VSPPro ALNG LicSAPk MVL SAL	Per License	Monthly	Software	\$32.50	\$30.87
	DM3386	125-01006 - VSTeamFndtnSvr ALNG LicSAPk MVL Bsc SAL	Per License	Monthly	Software	\$6.68	\$6.34
	U36030	125-00361 - VSTeamFndtnSvr ALNG LicSAPk MVL SAL	Per License	Monthly	Software	\$22.26	\$21.15
	CQ5538	N3F-00077 - VSTstPro ALNG LicSAPk MVL SAL	Per License	Monthly	Software	\$98.54	\$93.61
	CQ5539	N4F-00074 - VSUlt ALNG LicSAPk MVL SAL	Per License	Monthly	Software	\$596.72	\$566.88
	BU2506	6WC-00002 - WinRmtDsktpSrvcsSAL ALNG LicSAPk MVL	Per License	Monthly	Software	\$6.53	\$6.20
	Q76742	T98-02400 - WinRghtsMgmtSrvcsCAL ALNG LicSAPk MVL SAL	Per License	Monthly	Software	\$1.93	\$1.83
	Q76723	P71-01031 - WinSvrDataCtr ALNG LicSAPk MVL 1Proc	Per License	Monthly	Software	\$158.94	\$150.99
	PX2314	G3S-00566 - WinSvrEssntls ALNG LicSAPk MVL 1Proc	Per License	Monthly	Software	\$23.00	\$21.85

Service Area	Component Code	Component	Metric Unit	Period	Type	List Price	Discounted Price
	V94166	P73-04837 - WinSvrStd ALNG LicSAPk MVL 1Proc	Per License	Monthly	Software	\$23.00	\$21.85

**Discount – 5.00%** (5.00% minimum rising to 42.00% for volume)

Exhibit 7. Desktop as a Service (DaaS) Price List

Mandatory Components for Service Setup		List Price		Discounted Price	
Component	Sizing	One Time	Monthly	One Time	Monthly
Tenant Appliances (1GHz, 3GB, 20GB, Linux, Silver Support) - 2	1 pair/tenant/5000 users in each datacenter	\$864.96	\$417.34	\$821.71	\$396.48
External IP's - 2	1 pair/Tenant in each datacenter where desktops are provided	-	\$28.11	-	\$26.71
Service Support	A multiplier of the following applies: <ul style="list-style-type: none"> <li>• 1 per tenant, plus</li> <li>• 0.5 for each 5 additional Gold Pattern Templates or 100 desktops, plus</li> <li>• 0.5 for each profile server and up to 1TB of user storage</li> </ul>	-	\$370.85	-	\$352.31



## VDI Options

### 1 – 24 Desktops (5.00% discount)

Component	Sizing			OS	Backup	RIM	List Price		Discounted Price	
	CPU	RAM	Storage				One Time	Monthly	One Time	Monthly
Standard DT 1 Temp	1	2	30	Windows Server 2008R2	Yes	None	\$456.54	\$39.85	\$433.56	\$37.84
Standard DT 1	1	2	30	Windows Server 2008R2		None	-	\$99.05	-	\$94.06
Standard DT 2 Temp	1	3	35	Windows Server 2008R2	Yes	None	\$456.54	\$45.54	\$433.56	\$43.25
Standard DT 2	1	3	35	Windows Server 2008R2		None	-	\$117.27	-	\$111.36
Standard DT 3 Temp	1	4	40	Windows Server 2008R2	Yes	None	\$456.54	\$51.23	\$433.56	\$48.65
Standard DT 3	1	4	40	Windows Server 2008R2		None	-	\$134.34	-	\$127.58
Power DT 1 Temp	2	4	40	Windows Server 2008R2	Yes	None	\$456.54	\$51.23	\$433.56	\$48.65
Power DT 1	2	4	40	Windows Server 2008R2		None	-	\$145.73	-	\$138.39
Power DT 2 Temp	2	6	45	Windows Server 2008R2	Yes	None	\$456.54	\$58.06	\$433.56	\$55.14
Power DT 2	2	6	45	Windows Server 2008R2		None	-	\$175.33	-	\$166.50
Power DT 3 Temp	2	8	50	Windows Server 2008R2	Yes	None	\$456.54	\$63.76	\$433.56	\$60.55
Power DT 3	2	8	50	Windows Server 2008R2		None	-	\$207.21	-	\$196.78
Enterprise DT 1 Temp	4	8	100	Windows Server 2008R2	Yes	None	\$456.54	\$127.51	\$433.56	\$121.09
Enterprise DT 1	4	8	100	Windows Server 2008R2		None	-	\$269.82	-	\$256.24

**25 – 49 Desktops (15.00% discount)**

Component	Sizing			OS	Backup	RIM	List Price		Discounted Price	
	CPU	RAM	Storage				One Time	Monthly	One Time	Monthly
Standard DT 1 Temp	1	2	30	Windows Server 2008R2	Yes	None	\$456.54	\$39.85	\$387.07	\$34.60
Standard DT 1	1	2	30	Windows Server 2008R2		None	-	\$99.05	-	\$84.33
Standard DT 2 Temp	1	3	35	Windows Server 2008R2	Yes	None	\$456.54	\$45.54	\$387.07	\$37.84
Standard DT 2	1	3	35	Windows Server 2008R2		None	-	\$117.27	-	\$99.47
Standard DT 3 Temp	1	4	40	Windows Server 2008R2	Yes	None	\$456.54	\$51.23	\$387.07	\$43.25
Standard DT 3	1	4	40	Windows Server 2008R2		None	-	\$134.34	-	\$113.53
Power DT 1 Temp	2	4	40	Windows Server 2008R2	Yes	None	\$456.54	\$51.23	\$387.07	\$43.25
Power DT 1	2	4	40	Windows Server 2008R2		None	-	\$145.73	-	\$123.26
Power DT 2 Temp	2	6	45	Windows Server 2008R2	Yes	None	\$456.54	\$58.06	\$387.07	\$48.65
Power DT 2	2	6	45	Windows Server 2008R2		None	-	\$175.33	-	\$149.21
Power DT 3 Temp	2	8	50	Windows Server 2008R2	Yes	None	\$456.54	\$63.76	\$387.07	\$54.06
Power DT 3	2	8	50	Windows Server 2008R2		None	-	\$207.21	-	\$176.24
Enterprise DT 1 Temp	4	8	100	Windows Server 2008R2	Yes	None	\$456.54	\$127.51	\$387.07	\$108.12
Enterprise DT 1	4	8	100	Windows Server 2008R2		None	-	\$269.82	-	\$229.21

**50 - 99 Desktops (25.00% discount)**

Component	Sizing			OS	Backup	RIM	List Price		Discounted Price	
	CPU	RAM	Storage				One Time	Monthly	One Time	Monthly
Standard DT 1 Temp	1	2	30	Windows Server 2008R2	Yes	None	\$456.54	\$39.85	\$340.58	\$30.27
Standard DT 1	1	2	30	Windows Server 2008R2		None	-	\$99.05	-	\$74.60
Standard DT 2 Temp	1	3	35	Windows Server 2008R2	Yes	None	\$456.54	\$45.54	\$340.58	\$33.52
Standard DT 2	1	3	35	Windows Server 2008R2		None	-	\$117.27	-	\$87.58
Standard DT 3 Temp	1	4	40	Windows Server 2008R2	Yes	None	\$456.54	\$51.23	\$340.58	\$38.92
Standard DT 3	1	4	40	Windows Server 2008R2		None	-	\$134.34	-	\$100.55
Power DT 1 Temp	2	4	40	Windows Server 2008R2	Yes	None	\$456.54	\$51.23	\$340.58	\$38.92
Power DT 1	2	4	40	Windows Server 2008R2		None	-	\$145.73	-	\$109.20
Power DT 2 Temp	2	6	45	Windows Server 2008R2	Yes	None	\$456.54	\$58.06	\$340.58	\$43.25
Power DT 2	2	6	45	Windows Server 2008R2		None	-	\$175.33	-	\$130.83
Power DT 3 Temp	2	8	50	Windows Server 2008R2	Yes	None	\$456.54	\$63.76	\$340.58	\$47.57
Power DT 3	2	8	50	Windows Server 2008R2		None	-	\$207.21	-	\$154.61
Enterprise DT 1 Temp	4	8	100	Windows Server 2008R2	Yes	None	\$456.54	\$127.51	\$340.58	\$95.15
Enterprise DT 1	4	8	100	Windows Server 2008R2		None	-	\$269.82	-	\$201.10

**100 - 499 Desktops (32.00% discount)**

Component	Sizing			OS	Backup	RIM	List Price		Discounted Price	
	CPU	RAM	Storage				One Time	Monthly	One Time	Monthly
Standard DT 1 Temp	1	2	30	Windows Server 2008R2	Yes	None	\$456.54	\$39.85	\$309.22	\$27.03
Standard DT 1	1	2	30	Windows Server 2008R2		None	-	\$99.05	-	\$67.03
Standard DT 2 Temp	1	3	35	Windows Server 2008R2	Yes	None	\$456.54	\$45.54	\$309.22	\$30.27
Standard DT 2	1	3	35	Windows Server 2008R2		None	-	\$117.27	-	\$78.93
Standard DT 3 Temp	1	4	40	Windows Server 2008R2	Yes	None	\$456.54	\$51.23	\$309.22	\$34.60
Standard DT 3	1	4	40	Windows Server 2008R2		None	-	\$134.34	-	\$90.82
Power DT 1 Temp	2	4	40	Windows Server 2008R2	Yes	None	\$456.54	\$51.23	\$309.22	\$34.60
Power DT 1	2	4	40	Windows Server 2008R2		None	-	\$145.73	-	\$98.39
Power DT 2 Temp	2	6	45	Windows Server 2008R2	Yes	None	\$456.54	\$58.06	\$309.22	\$38.92
Power DT 2	2	6	45	Windows Server 2008R2		None	-	\$175.33	-	\$118.93
Power DT 3 Temp	2	8	50	Windows Server 2008R2	Yes	None	\$456.54	\$63.76	\$309.22	\$43.25
Power DT 3	2	8	50	Windows Server 2008R2		None	-	\$207.21	-	\$140.56
Enterprise DT 1 Temp	4	8	100	Windows Server 2008R2	Yes	None	\$456.54	\$127.51	\$309.22	\$86.50
Enterprise DT 1	4	8	100	Windows Server 2008R2		None	-	\$269.82	-	\$182.72

**500+ Desktops (42.00% discount)**

Component	Sizing			OS	Backup	RIM	List Price		Discounted Price	
	CPU	RAM	Storage				One Time	Monthly	One Time	Monthly
Standard DT 1 Temp	1	2	30	Windows Server 2008R2	Yes	None	\$456.54	\$39.85	\$278.95	\$21.62
Standard DT 1	1	2	30	Windows Server 2008R2		None	-	\$99.05	-	\$54.06
Standard DT 2 Temp	1	3	35	Windows Server 2008R2	Yes	None	\$456.54	\$45.54	\$278.95	\$23.79
Standard DT 2	1	3	35	Windows Server 2008R2		None	-	\$117.27	-	\$62.71
Standard DT 3 Temp	1	4	40	Windows Server 2008R2	Yes	None	\$456.54	\$51.23	\$278.95	\$28.11
Standard DT 3	1	4	40	Windows Server 2008R2		None	-	\$134.34	-	\$72.44
Power DT 1 Temp	2	4	40	Windows Server 2008R2	Yes	None	\$456.54	\$51.23	\$278.95	\$28.11
Power DT 1	2	4	40	Windows Server 2008R2		None	-	\$145.73	-	\$78.93
Power DT 2 Temp	2	6	45	Windows Server 2008R2	Yes	None	\$456.54	\$58.06	\$278.95	\$31.35
Power DT 2	2	6	45	Windows Server 2008R2		None	-	\$175.33	-	\$95.15
Power DT 3 Temp	2	8	50	Windows Server 2008R2	Yes	None	\$456.54	\$63.76	\$278.95	\$34.60
Power DT 3	2	8	50	Windows Server 2008R2		None	-	\$207.21	-	\$112.44
Enterprise DT 1 Temp	4	8	100	Windows Server 2008R2	Yes	None	\$456.54	\$127.51	\$278.95	\$69.20
Enterprise DT 1	4	8	100	Windows Server 2008R2		None	-	\$269.82	-	\$145.96

## Optional Components

Component	Unit	Sizing	List Price		Discounted Price	
			One Time	Monthly	One Time	Monthly
dtRAM Appliances (1GHz, 1GB, 10GB, Linux, Silver Support) - 2	Per 2 Servers	1 pair/tenant (datacenter), maximum of 500 sessions per management host.	\$864.96	\$378.42	\$821.71	\$359.50
Profile Server (1GHz, 4GB, 50GB, Windows 2012, Silver Support)	Per Server	1 per tenant if User Profile management is required, must have file storage for user data	\$432.48	\$230.30	\$410.86	\$218.78
Active Directory Server (1GHz, 4GB, 50GB, Windows 2012, Silver Support)	Per Server	1 per tenant for Active Directory Services. (If required, a pair for redundancy)	\$432.48	\$230.30	\$410.86	\$218.78
User storage	Per GB	On file server, recommend on Profile server with Profile Unity. OTC is for 1st volume	\$216.24	\$0.30	\$205.43	\$0.29
Desktop Storage	Per GB	Additional storage for the OS.	-	\$0.78	-	\$0.74
User storage Backups	Per GB	Data backed up /GB	-	\$0.30	-	\$0.29

## Software

Component	Unit	Sizing	List Price		Discounted Price	
			One Time	Monthly	One Time	Monthly
Trend Micro DS Server	Per Server	Required on Profile Server, recommended on other file servers	\$864.96	\$378.42	\$821.71	\$359.50
LWL Profile Unity	Per User	Requires Profile server and User Profile storage	\$432.48	\$230.30	\$410.86	\$218.78
MS Office Professional Plus	Per Desktop		\$432.48	\$230.30	\$410.86	\$218.78
MS Office Standard	Per Desktop		\$216.24	\$0.30	\$205.43	\$0.29
MS Project	Per Desktop		-	\$0.78	-	\$0.74
MS Visio	Per Desktop		-	\$0.30	-	\$0.29

Support Description
<b>NTT DATA RESPONSIBILITIES</b>
• The hardware, storage and network required to provide DaaS
• Troubleshooting and resolving issues caused by non-available hardware or network
• Monitoring, Maintenance and availability of all DaaS Appliances
• Maintaining Trend Micro Deep Security and assisting with troubleshooting issues related to Deep Security Anti-Malware protection (includes providing logs, maintaining user accounts, reporting monthly usage, insuring desktops/servers are protected where necessary)
• Assisting client with troubleshooting of templates, desktops, pools and networks
• Providing updated agents (DaaS, Horizon View, View Agent Direct Connect)
• Monthly usage reporting and licensing for LWL Profile Unity and providing updated license files when required (environment growth)
• Incident, Problem and Request Management for all items NTT DATA is responsible for (via Cloud Support/SOC)
• Adjusting desktop model, connectivity protocol and template quotas based on sizing change requests
<b>OUT OF SCOPE / CLIENT RESPONSIBILITIES</b>
• Patching of all desktops and templates once provided to a tenant
• Creating and updating Desktop Pools (within allotted quotas)
• Assigning users to pools
• Associating domain to DaaS environment
• Installing and updating all software. Only exception is the initial installation and patching of Microsoft OS and Office software as noted above.
• Desktop and end-user support
• Configuring LWL Profile Unity and configuring GPOs for both LWL Profile Unity and other GPOs as needed.
• Managing user data/profiles within allotted storage (or requesting additional storage to accommodate if needed)
• Requesting add/remove desktop model quotas
• Reporting issues with access/availability of desktops to the Cloud Support/SOC as soon as identified.

#### Exhibit 8. Glossary of Descriptions and Terms Used

Component	Metric Unit	Period	Component Description
CPU	GHz	Monthly	Average Gigahertz consumed per hour across the number of 24 hour days per month.
			NOTE: Utilization is calculated based on the actual resources consumed by the powered on

Component	Metric Unit	Period	Component Description
			VM regardless of the number of virtual CPUs configured to the VM. CPU utilization is measured and calculated based on the average amount of GHz consumed by all VMs associated with the Project over a given month. Please note VMs that are shut down will incur only SAN costs in this usage-based model.
RAM	GB	Monthly	<p>Average Gigabytes of RAM consumed per hour across the number of 24 hour days per month</p> <p>NOTE: Utilization is calculated based on the actual resources consumed by the powered on VM regardless of memory (RAM) configured to the VM. RAM utilization is measured and calculated based on the average of amount of RAM consumed by all VMs associated with the project over a given month. Please note VMs that are shut down will incur only SAN costs in this usage-based model.</p>
SAN	GB	Monthly	<p>Storage Area Network (SAN) is offered as an allocated cost with the ability of the customer to adjust the total allocated SAN upon request through requests to increase or decrease allocated SAN incrementally. Monthly costs are calculated based upon the average total allocated SAN used by the customer per month. Any allocated SAN volumes deleted by the customer will factor into the calculation of total SAN allocated to the customer per month, and the monthly total would be calculated by the average total allocation for that particular month, including any storage used towards swap files and VMware overheads.</p> <p>Optimized SAN: An optimized mixture of SSD, FC, and SATA drives that leverage FAST cache capabilities that leverage auto tiering capabilities to store data in a drive tier that matches its performance profile with the appropriate disk type.</p> <p>Economy SAN: A single tier solution that is optimized for large block of infrequently accessed data. There are no FAST Cache or auto-tiering features.</p>
Provisioning (if requested)	VM	One-Time	Set up VM with associated RAM and Storage within the NTT DATA Cloud
Backup Configuration	VM	One-Time	Install and configure backup agent
Per GB Protected	GB	Monthly	A measure of the designated amount of data in Gigabytes associated with a VM that is specified for protection by means of daily incremental backups
DR Configuration	VM	One-Time	Configure DR instance of production application
DR Tests - Amortized	VM	Monthly	Includes cost of services for NTT DATA to conduct one technical disaster recovery test per year.
Remote Site SAN Storage	GB	Monthly	Storage at remote DR site to which production data is replicated
Network Replication Costs	GB	Monthly	Charges for network utilization to replicate data between production and DR sites.

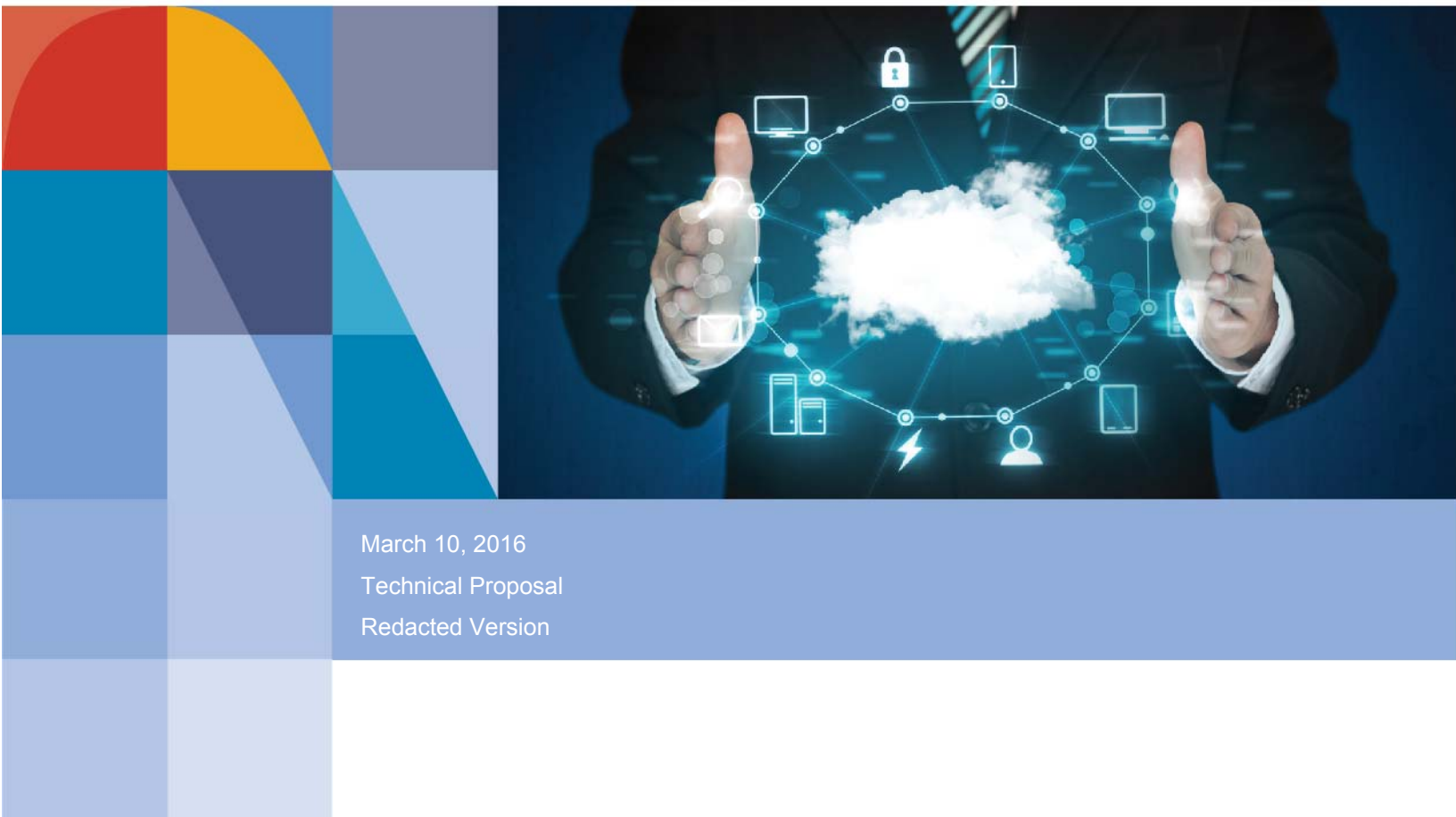


Component	Metric Unit	Period	Component Description
DR Replication License	VM	Monthly	DR Replication Tool (Zerto) license cost for DR for each VM.
Internet Bandwidth	Mbps	Monthly	Dedicated Internet bandwidth to a Customer VPN that guarantees that amount remains allocated for the Customer's use. That bandwidth (measured in Mbps) is automatically set to expand during periods where capacity exceeds the allocated bandwidth. Bandwidth will automatically return to the allocated level when usage is again reduced. Bandwidth bursting is billed at the 95th percentile.
			This is calculated in the following way: Every 5 minutes, the Customer's bandwidth is measured using a network monitoring tool. This means that over a 30-day period, 8640 samples of the Customer's bandwidth usage are taken. These 8640 samples are arranged in order from highest usage to lowest usage. Then the top 5 % of the samples (432 of them) are ignored and the remaining 95% of the samples are used to determine the monthly average.
VPN Tunnel (if requested)	Per Connection	One-Time	Configuration of a site to site VPN tunnel
External IP	Per IP	Monthly	One public IP address
Firewall + IDS/IPS Protection	Per Host Site	Monthly	Advanced security services to provide Firewall and Intrusion Detection/Prevention Services. The solution allows to detect and protect against the following type of attacks:
			<ul style="list-style-type: none"> <li>• DoS attacks</li> <li>• Buffer overflows</li> <li>• P2P attacks</li> <li>• Worms</li> <li>• Trojans</li> <li>• Backdoor attacks</li> <li>• Spyware</li> <li>• Invalid headers</li> <li>• Blended threats</li> <li>• Rate-based attacks</li> <li>• Zero-day threats</li> <li>• Port scans</li> <li>• VoIP attacks</li> <li>• IPv6 attacks</li> <li>• Statistical anomalies</li> <li>• Protocol anomalies</li> <li>• Application anomalies</li> <li>• Malformed traffic</li> <li>• TCL segmentation and IP fragmentation</li> </ul>
Firewall Configuration	One Time	One-Time	Installation and configuration of a firewall for each environment
25 User VPN Pack	25 Pack	Monthly	SSL Client based VPN for secure remote access to the environment.
Bronze Service Setup	Per Device	One-Time	Install Bronze Level Monitoring agent and monitoring software for Node or Interface
Silver Service Setup	Per Device	One-Time	Install Silver Level Monitoring agent and monitoring software for OS, Node or Interface; Configure capacity management parameters and escalation procedures

Component	Metric Unit	Period	Component Description
Gold Service Setup	Per Device	One-Time	Install Gold Level Monitoring agent and monitoring software for OS, Node or Interface Configure capacity management parameters and escalation procedures
Remedy Fixed License	Per License	Monthly	License dedicated to a single user for access to monitoring tool
Remedy Floating License	Per License	Monthly	License shared among multiple users (e.g. access for ticket creation) for access to monitoring tool

# Proposal for Cloud Solutions

Utah Solicitation Number CH16012



March 10, 2016  
Technical Proposal  
Redacted Version

**NTT DATA, Inc.**

**Attention: Christopher Hughes, Assistant Director**  
State of Utah Division of Purchasing  
3150 State Office Building, Capitol Hill  
Salt Lake City, Utah 84114-1061  
[christopherhughes@utah.gov](mailto:christopherhughes@utah.gov)  
801-538-3254

## **1. RFP Signature Page (RFP §5.1)**

---

As per your instructions we have submitted the signed vendor information form as a separate attachment to this RFP and uploaded it on the bidsync site.

## Table of Contents

---

<b>1. RFP Signature Page (RFP §5.1)</b>	<b>2</b>
<b>2. Executive Summary (RFP §5.4)</b>	<b>9</b>
<b>3. Mandatory Minimums (RFP §5)</b>	<b>12</b>
3.1 Cover Letter (RFP §5.2)	13
3.2 Acknowledgement of Amendments (RFP §5.3)	15
3.3 General Requirements (RFP §5.5)	15
3.3.1 Usage Report Administrator	15
3.3.2 Cooperation with NASPO ValuePoint	16
3.3.3 Completed Copy of CSA Star Self-Assessment Form	16
3.3.4 Sample Service Level Agreement	16
3.4 Recertification of Mandatory Minimums and Technical Specifications (RFP §5.7)	16
<b>4. Business Profile (RFP §6)</b>	<b>17</b>
4.1 Business Profile (RFP §6.1)	17
4.2 Scope of Experience (RFP §6.2)	21
4.3 Financials (RFP §6.3)	24
4.4 General Information (RFP §6.4)	25
4.4.1 Depth and Breadth of Services	25
4.4.2 Auditing Capabilities	28
4.5 Billing and Pricing Practices (RFP §6.5)	28
4.5.1 Billing and Pricing Practices	28
4.5.2 Cost Impacts	29
4.5.3 NIST Compliance	30
4.6 Scope and Variety of Cloud Solutions (RFP §6.6)	32
4.6.1 Scope and Variety of Service Models	32
4.7 Best Practices (RFP §6.7)	33
<b>5. Organization Profile (RFP §7)</b>	<b>34</b>
5.1 Contract Manager (RFP §7.1)	34
5.1.1 Contact Details of Contract Manager	34
5.1.2 Contract Managers Experience	34
5.1.3 Roles and Responsibilities	35
<b>6. Technical Response (RFP §8)</b>	<b>37</b>
Our Ability and Approach	37
6.1 Technical Requirements (RFP §8.1)	43

6.1.1	Cloud Service Models .....	43
6.1.2	NIST Characteristics .....	45
6.1.3	Solution Subcategories .....	48
6.1.4	Compliance with Attachments C and D .....	48
6.1.5	Adherence to Services, Definitions, and Deployment Models .....	49
6.2	Subcontractors (RFP §8.2) .....	50
6.2.1	Use of Subcontractors .....	50
6.2.2	Extent of Subcontractor Use .....	50
6.2.3	Qualifications of Subcontractors .....	50
6.3	Working with Purchasing Entities (RFP §8.3) .....	51
6.3.1	Working with Purchasing Entities .....	51
6.3.2	Unauthorized Marketing .....	58
6.3.3	User Test/Staging Environment .....	58
6.3.4	Accessibility for People with Disabilities .....	58
6.3.5	Browser Platforms .....	58
6.3.6	Storage of Sensitive or Personal Information .....	59
6.3.7	Project Schedule Plans and Work Plans .....	59
6.4	Customer Service (RFP §8.4) .....	62
6.4.1	Excellence in Customer Service .....	62
6.4.2	Compliance with Customer Service Requirements .....	70
6.5	Security of Information (RFP §8.5) .....	71
6.5.1	Data Protection Measures .....	71
6.5.2	Compliance with Data Privacy and Security Laws .....	72
6.5.3	Access of Purchasing Entity User Accounts and Data .....	72
6.6	Privacy and Security (RFP §8.6) .....	72
6.6.1	Compliance with NIST and Other Standards .....	72
6.6.2	Security Certifications .....	72
6.6.3	Security of Data and Applications .....	74
6.6.4	Data Confidentiality Standards and Practices .....	76
6.6.5	Third Party Attestations, Credentials, and Certifications .....	77
6.6.6	NTT DATA's Logging Process .....	77
6.6.7	Restriction of Visibility of Cloud-Hosted Data and Documents .....	77
6.6.8	Notification of Security Incidents .....	77
6.6.9	Isolation of Hosted Servers .....	78
6.6.10	Security Technical Reference Architectures .....	78

6.6.11	Security Procedures for Employees with Access to Sensitive Data .....	78
6.6.12	Confidentiality of Data at Rest and in Transit .....	79
6.6.13	Notification and Mitigation of a Data Breach.....	79
6.7	Migration and Redeployment Plan (RFP §8.7).....	80
6.7.1	Closing a Service .....	80
6.7.2	Orderly Returns of Data .....	81
6.8	Service or Data Recovery (RFP §8.8) .....	81
6.8.1	Backup and Restore Services .....	83
6.9	Data Protection (RFP §8.9) .....	84
6.9.1	Encryption and Other Options for Protecting Sensitive Data.....	84
6.9.2	Agreements to Protect Data .....	84
6.9.3	Use of Data for Defined Purposes .....	84
6.10	Service Level Agreements (RFP §8.10) .....	84
6.10.1	Negotiability of Sample SLA .....	84
6.10.2	Sample SLA .....	92
6.11	Data Disposal (RFP §8.11).....	92
6.12	Performance Measures and Reporting (RFP §8.12) .....	92
6.12.1	Ability to Guarantee Reliability and Uptime .....	92
6.12.2	Standard Uptime Service and Related Criteria.....	93
6.12.3	Obtaining Support .....	94
6.12.4	Failure to Meet Incident Response Times and Incident Fix Times.....	94
6.12.5	Procedures for Planned Downtime .....	94
6.12.6	Consequences If Disaster Recovery Metrics Are Not Met .....	94
6.12.7	Sample of Performance Reports .....	94
6.12.8	Ability to Print Historical, Statistical, and Usage Reports Locally .....	96
6.12.9	Support for On-Demand Deployment .....	96
6.12.10	Scale-Up and Scale-Down.....	96
6.13	Cloud Security Alliance Questionnaires (RFP §8.13).....	97
6.14	Service Provisioning (RFP §8.14).....	97
6.14.1	Emergency or Rush Implementation Requests .....	97
6.14.2	Lead Time for Provisioning Solutions .....	101
6.15	Back Up and Disaster Plan (RFP §8.15) .....	101
6.15.1	Applying Legal Retention Periods and Disposition Policies .....	101
6.15.2	Disaster Recovery Risks and Potential Mitigation Strategies.....	101
6.15.3	Infrastructure for Data Centers .....	103

6.16	Solution Administration (RFP §8.16)	105
6.16.1	Managing Identity and User Accounts	105
6.16.2	Anti-Virus Protection for Data Stores	105
6.16.3	Migration of Data to a Successor Cloud Provider	105
6.16.4	Distributed Administration	105
6.16.5	Applying Administrative Policies of Participating Entities	105
6.17	Hosting and Provisioning (RFP §8.17)	106
6.17.1	Cloud Hosting Provisioning Processes	106
6.17.2	Tool Sets	106
6.18	Trial and Testing Periods (Pre- and Post-Purchase) (RFP §8.18)	107
6.18.1	Testing and Training Periods	107
6.18.2	Environments for Testing and Proof of Concept	107
6.18.3	Training and Support	107
6.19	Integration and Customization (RFP §8.19)	109
6.19.1	Integration of Services to Other Complementary Applications	109
6.19.2	Customization and Personalization of Services	109
6.20	Marketing Plan (RFP §8.20)	112
6.21	Related Value-Added Services To Cloud Solutions (RFP §8.21)	114
6.22	Supporting Infrastructure (RFP §8.22)	116
6.22.1	Infrastructure Requirements	116
6.22.2	Installation of New Infrastructure	116
6.23	Alignment of Cloud Computing Reference Architecture (RFP §8.23)	116
<b>7.</b>	<b>Confidential, Protected or Proprietary Information</b>	<b>120</b>
7.1	Scope of Experience (RFP §6.2)	Error! Bookmark not defined.
7.2	Contract Manager Resume	Error! Bookmark not defined.
7.3	Claim of Business Confidentiality Form	Error! Bookmark not defined.
7.4	Additional Attachments	Error! Bookmark not defined.
<b>8.</b>	<b>Exceptions and/or Additions to the Standard Terms and Conditions</b>	<b>121</b>
<b>9.</b>	<b>Cost Proposal</b>	<b>122</b>
<b>Appendix 1</b>	<b>Overview of Transition Process</b>	<b>123</b>
<b>Appendix 2</b>	<b>Details of Migration Methodology</b>	<b>130</b>
<b>Appendix 3</b>	<b>D&amp;B Report</b>	<b>136</b>



## Table of Exhibits

---

Exhibit 1: Business Benefits of NTT DATA Cloud Services .....	10
Exhibit 2. Acknowledgement of Amendments.....	15
Exhibit 3. Key NTT DATA Service Offerings .....	18
Exhibit 4. Sampling of Public Sector Experience .....	18
Exhibit 5. NTT DATA's Corporate Organization.....	19
Exhibit 6. Case Study 1 – Remote Infrastructure Management.....	21
Exhibit 7. Case Study 2 – Data Center Migration and Program Management.....	22
Exhibit 8. Case Study 3 – Cloud IaaS and DRaaS for Global Apps Development .....	23
Exhibit 9. NTT DATA Corporation Five-Year Financial Summary.....	24
Exhibit 10. Gartner's Market Share Analysis Report.....	26
Exhibit 11. IDC Report for Cloud Services .....	26
Exhibit 12. HfS Research Report .....	27
Exhibit 13. TeleGeography Report for Largest Retail Data Center Operators .....	27
Exhibit 14. Sample Monthly Report.....	29
Exhibit 15. Contract Manager Details .....	34
Exhibit 16. Delivery Manager Details .....	34
Exhibit 17. Roles and Responsibilities of Contract Manager .....	35
Exhibit 18. Fully Integrated Cloud and Infrastructure Services .....	39
Exhibit 19. Virtual Computing Environment .....	40
Exhibit 20. IBM Power7+ Technology .....	40
Exhibit 21. Desktop as a Service .....	41
Exhibit 22. IaaS Services .....	44
Exhibit 23. Supported Network Carriers.....	46
Exhibit 24. IT Operations Management .....	52
Exhibit 25. Operations Management Flow .....	53
Exhibit 26. Incident Management Process.....	55
Exhibit 27. Critical Incident Management Process Flow .....	56
Exhibit 28. Data Center Services Phases .....	60
Exhibit 29. Data Center Migration and Relocation Services – Major Tasks.....	61
Exhibit 30. NTT DATA Migration Solution – Major Waves .....	61
Exhibit 31. NTT DATA's Quality Management Approach .....	63
Exhibit 32. NTT DATA's Migration QA Framework .....	64
Exhibit 33. Integration Between Problem Management and Other Service Management Processes .....	67
Exhibit 34. NTT DATA's Problem Management Process.....	68
Exhibit 35. Governance Model.....	70
Exhibit 36. Security Certifications .....	74
Exhibit 37. High-Level Transition Approach.....	85
Exhibit 38. SLAs and Metrics .....	86
Exhibit 39. Service Level Targets .....	86
Exhibit 40. Goal-Question-Metric Method .....	87
Exhibit 41. Key Cost Metrics .....	87

Exhibit 42. Leading Indicators .....	88
Exhibit 43. Sample SLA Metrics.....	90
Exhibit 44. Typical Facility-Level SLAs .....	92
Exhibit 45. NTT DATA Center Floor Plan .....	93
Exhibit 46. Sample Availability Reports .....	95
Exhibit 47. Change Management Roles and Responsibilities .....	98
Exhibit 48. Change Management Process Flow .....	101
Exhibit 49. NTT DATA's Data Center Topology .....	104
Exhibit 50. NTT DATA VPC Architecture .....	104
Exhibit 51. Process and Staff Integration Activities and Tasks .....	108
Exhibit 52. RIM Service Levels .....	112
Exhibit 53. NIST Reference Architecture .....	117
Exhibit 54. Cloud Service Management.....	118
Exhibit 55. Large Contracts.....	<b>Error! Bookmark not defined.</b>
Exhibit 56. Client Reference 1 – U.S. Securities and Exchange Commission...	<b>Error! Bookmark not defined.</b>
Exhibit 57. Client Reference 2 – State of Rhode Island .....	<b>Error! Bookmark not defined.</b>
Exhibit 58. Client Reference 3 – Clayton County (Georgia) Water Authority .....	<b>Error! Bookmark not defined.</b>
Exhibit 59. Client Reference 4 – Mecklenburg County, North Carolina .....	<b>Error! Bookmark not defined.</b>
Exhibit 60. Client Reference 5 – NACCO Material Handling Group .....	<b>Error! Bookmark not defined.</b>
Exhibit 61. High-level Transition Approach .....	123
Exhibit 62. Transition Planning Activities and Tasks.....	124
Exhibit 63. Knowledge Acquisition Activities and Tasks .....	125
Exhibit 64. Process and Staff Integration Activities and Tasks .....	126
Exhibit 65. Engagement Governance Activities and Tasks .....	127
Exhibit 66. Project Management Life Cycle Activities and Tasks .....	128
Exhibit 67. Project Management Details .....	128
Exhibit 68. Transition-In Critical Success Factors.....	129
Exhibit 69. Transition Out Plan .....	129
Exhibit 70. Planning Phase Deliverables .....	132

## 2. Executive Summary (RFP §5.4)

The one or two page executive summary is to briefly describe the Offeror's Proposal. This summary should highlight the major features of the Proposal. It must indicate any requirements that cannot be met by the Offeror. The Lead State should be able to determine the essence of the Proposal by reading the executive summary. See Section 5.4 of the RFP.

We welcome the opportunity for NTT DATA, Inc., to partner with the National Association of State Procurement Officers (NASPO) and with the members of your consortium by providing advanced cloud and cloud-related IT services. Specifically, with this proposal, we are offering to provide infrastructure as a service (IaaS). Accordingly, throughout this proposal, we have emphasized our capabilities in this area. With that said, as you review this proposal, bear in mind that we also offer a broad range of other services that are also relevant to organizations in your consortium.

NTT DATA is a global IT services company with more than 50 years of experience helping large organizations in the United States get the most value out of their IT systems. We help create, operate, maintain, and evolve critical systems and business processes by delivering a broad range of IT services, including cloud services. In doing so, we help our clients achieve sustainable, measurable improvements to their business operations.

NTT DATA is part of the NTT Group, one of the world's largest telecommunications and IT services companies. As a global company with offices throughout the United States, we are able to deliver a wide range of IT services both in-person and remotely as needed. We currently provide cloud services to state and local governments through two advanced U.S.-based cloud data centers in Ashburn, Virginia, and Sacramento, California—and with demand now growing for our services, we are planning additional cloud data centers in Texas, Illinois, and California.

### NTT: A Global Leader

NTT DATA's affiliation with the NTT Group gives us tremendous global reach. The NTT Group is one of the world's largest telecommunications companies, with a network presence in more than 196 countries and more than 230 data centers worldwide. Overall, the NTT Group ranks as the world's 65th-largest company, according to *Fortune* magazine.

Among the strengths NTT DATA offers NASPO:

- **A superior IaaS technical architecture.** We have deployed a high-performance, highly available cloud for IaaS-based virtualized systems that compares favorably to competing services, both in terms of both performance and reliability. NTT DATA's secure, scalable IaaS is available through our data centers in Virginia and California, both of which comply with Uptime Institute Tier IV standards. For the organizations you represent, this high Tier IV standard means that we can offer a stronger level of service than many competitors in the marketplace today, including 100 percent uptime when it comes to power delivery and cooling.
- **More choices of cloud technologies.** Most large, mature organizations use a range of technologies, and few try to rely on just Windows- or Linux-based systems. So why do some cloud providers only offer these two technologies? At NTT DATA, we support Windows and Linux on a VMWare-based cloud. But we also provide AIX, Linux, and iSeries support in a Power 7+ environment, disaster recovery-as-a-service (DRaaS), and even desktop-as-a-service (DaaS) based on VMware VDI. In addition, we can also accommodate colocation of legacy systems that are not easily virtualized. For the organizations you represent, these

choices mean the ability to select a cloud service that is an ideal fit, rather than just almost right.

- **World-class transition services.** The ongoing delivery of cloud services are important, but so is the transition. At NTT DATA, we know how to mitigate the risks associated with transitioning IT systems into the cloud. No matter how complex the system, we can migrate workloads into our IaaS environment with minimal disruption using a comprehensive transition methodology. This methodology addresses all the technology and operational details that must be dealt with in order to promote a smooth transition.
- **The ability to meet all your needs under one roof.** As a global, full service IT provider, NTT DATA can meet all of your needs for cloud services as well as disaster recovery and hot site fail-over capabilities. We also offer services that are well beyond the scope of IaaS offering—including large package integration services, software development services, and support services. Put simply, NTT DATA is a full-service IT company with services that cover the entire technology stack, from top to bottom. By working with us, members of your consortium will have the opportunity to obtain some of these interrelated services from a single vendor—and, potentially, avoid some of the finger-pointing and lack of accountability that sometimes goes along with the challenge of managing several different vendors.

We offer all of these services as part of an important tradition at our company—that of serving as an unbiased business advisor and systems integrator. At NTT DATA, we recognize that each of the organizations we work with is unique. We offer technology-agnostic recommendations and solutions that put the interests of each of our clients' interests first. This includes advisory services that help our clients adapt to changing circumstances, including challenges that may not yet be on the horizon.

Exhibit 1 summarizes some of the business benefits we can provide through our portfolio of cloud services. By working with NTT DATA, members of your consortium can reduce operating costs, improve service levels, standardize technologies, and reduce risk.

Exhibit 1: Business Benefits of NTT DATA Cloud Services

Reduce Operating Costs	Standardize Technology
<p>We can help reduce operating costs by:</p> <ul style="list-style-type: none"> <li>• Centralizing assets in an advanced data center, thus eliminating expensive multisite real estate and lease arrangements</li> <li>• Diminishing the inefficiencies associated with managing multiple vendors, resources, technologies, and infrastructures</li> <li>• Offering alternative shared resource models</li> <li>• Reducing the need for capital expenses by shifting more operations to a cloud, consumption-based model</li> <li>• Helping organizations only pay for what they use through consumption-based pricing</li> </ul>	<p>We can help standardize technology by:</p> <ul style="list-style-type: none"> <li>• Reinforcing technology standardization through an IaaS reference architecture</li> <li>• Simplifying application architectures through server consolidation and virtualization</li> <li>• Consolidating vendors, service contracts, products, and licenses</li> </ul>
Reduce Risk	Improve Service Levels
<p>NTT DATA can reduce risk by:</p> <ul style="list-style-type: none"> <li>• Providing fully redundant and resilient facilities, thus increasing availability</li> <li>• Providing disaster recovery capabilities through</li> </ul>	<p>We can improve service levels by:</p> <ul style="list-style-type: none"> <li>• Providing 24x7 user support and service management</li> <li>• Improving application recovery times by</li> </ul>

<p>our cloud architecture and replication capabilities</p> <ul style="list-style-type: none"> <li>• Enhancing IT compliance through centralized storage and data management</li> <li>• Seamlessly shifting workloads and data away from failing equipment and facilities</li> <li>• Providing proactive, “ready-for-business” health checks that monitor and manage systems and processes to ensure maximum uptime by identifying potential issues before they cause trouble</li> </ul>	<p>centralizing the location and management of hosted applications</p> <ul style="list-style-type: none"> <li>• Improving levels of service maturity</li> <li>• Tightly managing our cloud according to ITIL-based support processes, which allow us to commit to enhanced service level agreements (SLAs)</li> <li>• Using dedicated analytic and innovation teams that analyze issues, determine why incidents occur, and help prevent these problems from happening again</li> </ul>
---	---

*NTT DATA’s portfolio of data center services has produced a range of benefits for our clients, including lower costs, improved service levels, reduced risk, and more standard technologies.*

With this RFQ, you are representing the interests of a broad group of organizations—among them, state government procurement offices, other government organizations, and nonprofit corporations. Some members of this consortium have achieved IT operational maturity. Others are late adopters. But all have expressed an interest in obtaining quality cloud services, and all view this contract vehicle as an opportunity to do so at a reasonable cost.

With this proposal, NTT DATA offers the organizations you serve up-to-date, high performance, technology that is secure, easy to deploy, and flexible enough to satisfy the most demanding requirements.

We support our cloud technology with experienced delivery managers, talented technologists, and transparent reporting and metering tools, all of which makes us easy to do business with. We understand that the services we provide are about helping the organizations in your consortium serve the public more effectively. We will stand side-by-side with the members of your consortium in order to deliver the results you are looking for.

### **3. Mandatory Minimums (RFP §5)**

---

In this section, we have provided point by point responses to each of the item you described in RFP §5, concerning mandatory minimum requirements.

### **3.1 Cover Letter (RFP §5.2)**

March 8, 2016

Christopher Hughes, Assistant Director  
State of Utah Division of Purchasing  
3150 State Office Building, Capitol Hill  
Salt Lake City, Utah 84114-1061

Dear Mr. Hughes:

On behalf of NTT DATA, Inc., I am pleased to submit this proposal. With it, we are responding to the State of Utah's recent request for qualified firms to provide cloud-related services. Specifically, this proposal (along with supporting materials) is our response to Request for Proposals (RFP) No. CH16012, concerning the NASPO ValuePoint Master Agreement for Cloud Solutions.

With this proposal, we wish to be considered as a provider of IaaS through this master agreement. As we will demonstrate in the pages that follow, NTT DATA is highly qualified to provide such services.

NTT DATA is a global IT services company with more than 50 years of experience serving large organizations in the United States. We provide a wide range of professional services, including consulting services, application development services, application management services, and a variety of cloud services. In short, we can meet all of your needs for hosting services, co-location services, remote managed services, and application managed services.

Part of our strength as a cloud services provider lies in our affiliation with the NTT Group, one of the world's largest telecommunications companies and data center operators. We combine this global reach with local intimacy. NTT DATA has consultants available throughout the United States to meet the needs of our clients and we maintain a business unit devoted solely to addressing the unique needs of the public sector.

Given the breadth of services we offer, we are a natural choice for the state governments in your consortium. Specifically, by working with NTT DATA, the state governments you represent will be able to address a wide range of IT challenges through a single vendor, avoiding some of the complexity, finger pointing, and lack of accountability that can accompany projects involving multiple vendors with competing agendas.

In addition, we have a few legal notes and disclosures to share. Among them:

- We understand that NTT DATA may be required to negotiate additional terms and conditions, including additional administrative fees, with participating entities when executing a participating addendum.
- This proposal was developed solely by NTT DATA employees.
- NTT DATA—a Delaware corporation with a Federal Employer Identification Number (FEIN) of 04-2437166—is a company in good standing. We are not suspended, disbarred, or otherwise excluded from any federal or state procurement or non-procurement programs. We are a legal entity with a right to contract.



- We understand and acknowledge that a 0.25 percent NASPO ValuePoint administrative fee, as well administrative fees from participating entities, will apply to total sales for master agreements awarded from your RFP.
- We are proposing to provide IaaS, which we can provide IaaS using private, community, and hybrid deployment methods. We support self-service but we do not make our services available to the general public.
- NTT DATA is capable of storing and securing low, moderate, and high risk data as you defined it RFP Attachment D. Additionally, we have also submitted Attachment H (Identification of Service Models) as a separate attachment as part of our submission.

Finally, a note about navigating this proposal. Throughout this proposal, we have addressed each of your questions two full sections before you presented them in your RFP. For example, we address RFP Question 8.11 in Section 6.11 of this proposal. This pattern is worth bearing in mind as you navigate this proposal. In some cases, we will refer you to our answer to a particular question without referring you to a particular section of this proposal.

This proposal will be firm and binding for 180 days from the proposal opening date. Following your review of this proposal, we look forward to the opportunity to discuss it with you in more detail, and to negotiating the contract terms and conditions identified in our proposal in accordance with the RFP's instructions that are mutually acceptable to the State of Utah, the National Association of State Procurement Officers (NASPO), and NTT DATA.

If you have any questions, please do not hesitate to contact Bill Baver, a vice president in NTT DATA Public Sector, our business unit devoted to addressing the unique needs of government organizations. Bill can be contacted by email at [William.Baver@nttdata.com](mailto:William.Baver@nttdata.com), by telephone at 610-213-0255, or at the following address: 1660 International Drive, Suite 300, McLean, Virginia 22102.

We look forward to the opportunity to be considered as a cloud provider through your master agreement.

Sincerely,

A handwritten signature in blue ink, appearing to read "Timothy Conway".

Timothy Conway,  
President, Public Sector



## 3.2 Acknowledgement of Amendments (RFP §5.3)

NTT DATA acknowledges receipt of these 10 addenda, which we accept:

- Addendum 1, posted on December 22, 2015 at 3:53 PM MST
- Addendum 2, posted on December 24, 2015 at 10:47 AM MST
- Addendum 3, posted on January 5, 2016 at 1 PM MST
- Addendum 4, posted on January 12, 2016 at 3:03 PM MST
- Addendum 5, posted on January 15, 2016 at 4:17 PM MST
- Addendum 6, posted on January 28, 2016 at 8:35 AM MST
- Addendum 7, posted on February 1, 2016 at 4:40 PM MST
- Addendum 8, posted on February 3, 2016 at 2:01 PM MST
- Addendum 9, posted on February 5, 2016 at 8:37 AM MST
- Addendum 10, posted on February 10, 2016 at 12:13 PM MST

Also, please see Exhibit 2, where we have acknowledged the totality of this solicitation with a signature on the acknowledgement form that you have provided.

---

### Exhibit 2. Acknowledgement of Amendments

#### ACKNOWLEDGEMENT OF AMENDMENTS TO RFP (SOLICITATION CH16012)

This attachment represents that the Offeror has read, reviewed, and understands the totality of Solicitation CH16012, including the final RFP document posted on February 10, 2016.

By signing below, the Offeror attest to reviewing the documents listed above.

NTT DATA, Inc.  
Offeror



Representative Signature

*In this exhibit, we have acknowledged amendments to your RFP.*

## 3.3 General Requirements (RFP §5.5)

### 3.3.1 Usage Report Administrator

5.5.1 Offeror must agree that if awarded a contract it will provide a Usage Report Administrator responsible for the quarterly sales reporting described the Master Agreement Terms and Conditions, and if applicable Participating Addendums.

We agree that, if awarded a contract, NTT DATA will provide a usage report administrator who will be responsible for the quarterly sales reporting described in the terms and conditions of the master agreement (and, if applicable, participating addendums).

### 3.3.2 Cooperation with NASPO ValuePoint

5.5.2 Offeror must provide a statement that it 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.

We agree that NTT DATA will cooperate with NASPO ValuePoint and SciQuest (and any authorized agent or successor entity to SciQuest) with uploading ordering instructions.

### 3.3.3 Completed Copy of CSA Star Self-Assessment Form

5.5.3 Offeror must at a minimum complete, provide, and maintain a completed CSA STAR Registry Self-Assessment. Offeror must either submit a completed The Consensus Assessments Initiative Questionnaire (CAIQ), **Exhibit 1 to Attachment B**, or to submit a report documenting compliance with Cloud Controls Matrix (CCM), **Exhibit 2 to Attachment B**. Offeror must also represent and warrant the accuracy and currency of the information on the completed. Offerors are encouraged to complete and submit both exhibits to Attachment B.

We have completed both the CSA STAR Registry Self-Assessment (the name of the file is "NTT DATA's Report on Exhibit 1 to Attachment B - CAIQ version v 3.0.1-09-16-2014") and a report on our compliance with the Cloud Controls Matrix (named "NTT DATA's Report on Exhibit 2 to Attachment B – CSA\_CCM\_v3.0.1 09-16-2014"). Specifically, we have provided these documents as attachments to this proposal and uploaded them separately on Bidsync as part of our submission.

We represent and warrant the accuracy and currency of the information contained in those documents. We will maintain and update these documents at least annually and we will provide updated copies to a purchasing entity when requested.

### 3.3.4 Sample Service Level Agreement

5.5.4 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.

As part of this proposal, NTT DATA has provided a sample contract as a separate attachment (named "5.5.4 NTT DATA Sample Cloud Hosting Contract.pdf") that lists typical terms, conditions, and SLA-based service level objectives. We view this document is a starting point in establishing terms, conditions, and an SLA. Arriving at an actual contract and an SLA with a purchasing entity will require negotiation and a signed agreement.

## 3.4 Recertification of Mandatory Minimums and Technical Specifications (RFP §5.7)

Offeror must acknowledge that if it is awarded a contract under the RFP that it will annually certify to the Lead State that it still meets or exceeds the technical capabilities discussed in its proposal.

We acknowledge that if NTT DATA is awarded a contract under this RFP, NTT DATA will annually certify to the lead state that our company still meets or exceeds the mandatory minimum requirements and technical specifications of this RFP.

## 4. Business Profile (RFP §6)

---

### 4.1 Business Profile (RFP §6.1)

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.

#### Introduction and Overview

NTT DATA, Inc. is a leading IT services company with 50 years of experience helping large organizations get the most value out of their IT systems. All over the United States, our talented IT professionals help the large organizations we work with create, operate, maintain, and evolve mission critical systems and business processes. In the process, we help our clients achieve measurable, sustainable improvements to business operations.

Our company has provided IT services in the United States since 1965, when our U.S. founder began advising large organizations on how to take advantage of then-emerging IT technologies such as mainframe computers. Today, our company is part of the NTT Group, one of the world's largest telecommunications and IT services companies. Overall, the NTT Group has 242,000 employees in 88 countries and generates \$105 billion in annual revenue. This ranks the NTT Group as the world's 65th-largest company, according to *Fortune* magazine.

NTT DATA, Inc., is the North American IT services and systems integration arm of the NTT Group. With a team of more than 22,000 employees, our company offers a broad range of IT services that address every major aspect of providing government services. Exhibit 3 offers an overview of the services we offer government clients.

### Exhibit 3. Key NTT DATA Service Offerings

Transportation	Health and Human Services	Criminal Justice	Finance	Education	Public Utilities
					
Solutions for Government Organizations					
					
Consulting Services	Modernization Services		Managed Services		
<ul style="list-style-type: none"><li>» IT strategy</li><li>» Cloud strategy</li><li>» Enterprise information strategy</li><li>» Software selection</li><li>» Technology assessments</li><li>» Independent verification and validation</li><li>» Project management office services</li><li>» Security assessment</li></ul>	<ul style="list-style-type: none"><li>» COTS and SaaS implementations</li><li>» Legacy application modernization</li><li>» ERP implementations and upgrades</li><li>» Big data implementations</li><li>» Infrastructure modernization and migration</li><li>» Cloud migration</li><li>» Security remediation</li></ul>		<ul style="list-style-type: none"><li>» Service desk operations</li><li>» Application support and maintenance</li><li>» ERP application management</li><li>» Infrastructure management</li><li>» Cloud hosting</li><li>» Cloud management</li><li>» Customer contact center operations</li><li>» Managed security services</li></ul>		
On Premises or Cloud-Based Solutions					

*NTT DATA's menu of services for government organizations includes consulting services, modernization services, and an array of managed services. (We will offer more information about some of these services later in this section.)*

Overall, NTT DATA offers a significant amount of experience working with large and mid-sized government organizations. Exhibit 4 offers a sense of our client base in the public sector.

### Exhibit 4. Sampling of Public Sector Experience

#### Public Sector Experience and Vertical Knowledge Base

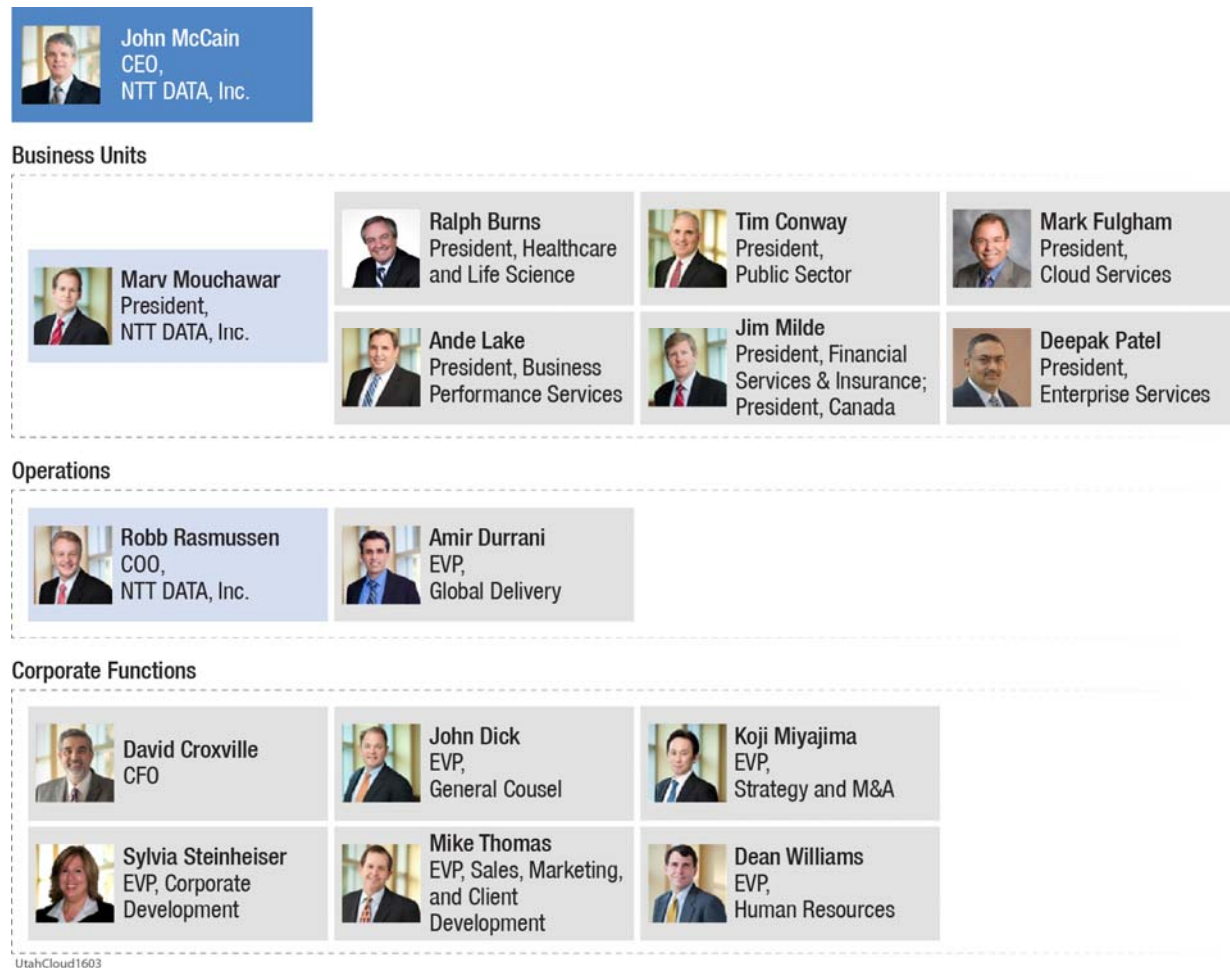
State and Local Government		Federal Government
<ul style="list-style-type: none"> <li>» Colorado</li> <li>» Indiana</li> <li>» Kentucky</li> <li>» Maryland</li> <li>» Massachusetts</li> <li>» Michigan</li> <li>» New York</li> <li>» Maine</li> <li>» North Carolina</li> <li>» Pennsylvania</li> <li>» Puerto Rico</li> <li>» Rhode Island</li> <li>» South Carolina</li> <li>» Texas</li> <li>» Virginia</li> </ul>		<ul style="list-style-type: none"> <li>» Administrative Office of the U.S. Courts</li> <li>» Dept. of Defense</li> <li>» Drug Enforcement Administration</li> <li>» Federal Bureau of Investigation</li> <li>» Dept. of Homeland Security (U.S. Customs and Border Protection)</li> <li>» Dept. of Homeland Security (U.S. Citizenship and Immigration Services)</li> <li>» Dept. of the Interior</li> <li>» Dept. of Justice</li> <li>» National Oceanic and Atmospheric Administration</li> <li>» U.S. Patent and Trademark Office</li> <li>» U.S. Securities and Exchange Commission</li> <li>» World Bank</li> <li>» U.S. Department of Veterans Affairs</li> </ul>

*During the past few years, NTT DATA has worked with a broad range of federal, state, and local government organizations, as this exhibit shows.*

## Organization of the Company

Exhibit 5 summarizes the organization of our company and some of the individuals who are responsible for leading of it.

### Exhibit 5. NTT DATA's Corporate Organization



*NTT DATA is organized into a series of business units. Each of them is oriented around a specific type of technology or a specific type of client. In this organizational structure, Marv Mouchawar, Robb Rasmussen, and the leaders of our corporate functional offices all report to John McCain, our CEO.*

As this exhibit shows, we have organized our company into several different business units, each designed to serve a different type of client or focus on a particular specialty. For example:

- NTT DATA Public Sector specializes in meeting the unique needs of government organizations
- NTT DATA Cloud Services specializes in delivering cloud solutions to organizations of all kinds.

In this engagement, we expect that both of these business units will have a role to play in meeting the needs of the organizations you represent through this contract vehicle.



## A Growing Cloud Provider

NTT DATA, Inc., is a growing company. During the past 3 years, we have experienced an annual revenue growth of about 3.2 percent overall. Our growth has been much faster as a cloud services provider, where we are seeing about 20 percent year-over-year growth.

For many years, NTT DATA has provided application and infrastructure services to large and mid-sized organizations, dating back well before the concept of “cloud” became mainstream. As more large organizations have begun to move toward conducting more of their IT operations through the cloud, NTT DATA began offering many of our cloud-based services through a single business unit, known as NTT DATA Cloud Services.

Since the fall of 2011, NTT DATA Cloud Services has provided a range of cloud services to clients on a global basis. Through these services, we have aligned infrastructure, networks, operating systems, and applications for a variety of clients—among them, public sector organizations such as Clayton County (Georgia) Water Authority, the U.S. Securities and Exchange Commission, the State of Rhode Island, and the Commonwealth of Kentucky.

For example, from June 2009 through November 2011, NTT DATA helped the State of Rhode Island design a new data center and stand up a new data center. As part of this project, we oversaw the move of more than 200 systems, more than 100 critical applications, a tape library, and personnel from eight different state departments. Later, in 2013, we helped the Commonwealth of Kentucky finish a comprehensive IT analysis and a data center consolidation roadmap and master plan.

Given this track record, NTT DATA easily meets your requirement for 3 years of experience providing cloud solutions, including government experience. This level of experience means we also offer an experienced workforce, many of whom have been with our company for years. In NTT DATA Cloud Services, for example, our overall retention rate for U.S. employees has been 92 percent over the past two years.

## Service Offerings

Today NTT DATA provides a range of IT services to large and mid-sized enterprises in all sectors of the U.S. economy, including advisory services, project-based services, and ongoing managed services. Among the services we provide:

- **Advisory Services** – NTT DATA maintains a dedicated business transformation practice that has successfully executed more than 125 different projects. We have experience providing technology evaluation services, organizational change management, IT strategy development and training, and other services.
- **Cloud Services** – NTT DATA provides a range of enterprise-class cloud services. We are fully capable of supporting mission-critical workloads backed by SLAs across the full stack of infrastructure and applications technologies. As we have described more fully in Section 6 (Technical Response) our IaaS offerings stretch beyond Windows and Linux support to also include AIX and iSeries support, DR as a service, Desktop as a service, and 24x7 remote infrastructure support. This makes us the right choice for organizations considering IaaS and who are seeking an optimal private, community, or hybrid cloud.
- **Application Management and Information Management** – NTT DATA can address all phases of application lifecycle management ranging from strategic thinking to ongoing optimization. No matter the application and information management challenge, we maintain a consistent focus on business processes, usability, quality assurance, and best practices. We offer multi-disciplinary solutions that involve business processes, operational best

practices, and technology best practices that have the potential to produce a cost savings of anywhere from 25 percent to 50 percent.

- **Enterprise Application Services** – NTT DATA maintains an Enterprise Application Services Practice that understands what it takes to implement, integrate, deploy, and rollout enterprise resource planning (ERP) systems. Our proprietary frameworks, tools, and accelerators deliver higher levels of consistency, efficiency and quality. By minimizing risk, cost, and the time needed to finish ERP projects, we help our clients flex more quickly to business changes, harness innovation, and increase their competitiveness.
- **Digital Business** – NTT DATA's enterprise-grade collection of digital business services produce dramatic (yet attainable) change for our clients by transforming end-to-end business processes. Through our digital business services, we help our clients obtain achievable business results that include improvements to customer care, greater operational efficiency, and a faster time to market for new products and services. Our rich portfolio of digital business services ranges from strategy and design to implementation and optimization.
- **Infrastructure Services** – NTT DATA takes a proactive approach to managing large organizations' infrastructure, providing comprehensive solutions and virtualizing IT infrastructure when necessary. With our cost-effective combination of skilled personnel, industry standard processes, and leading technology, we not only understand what it takes to manage infrastructure. We also understand how to improve it.
- **Business Intelligence, Analytics, and Performance Management** – NTT DATA's world-class Business Intelligence, Analytics, and Performance Management Practice helps our clients translate structured and unstructured big data into new ideas and well-timed actions with significant impact on operations. Our service offerings in this area include business intelligence; enterprise performance management; governance, risk, and compliance; data warehousing; advanced analytics; and information management.

## 4.2 Scope of Experience (RFP §6.2)

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 services identical or very similar to those required by this RFP. Government experience is preferred.

In this section, we have provided several different case studies that demonstrate our experience delivering cloud services. In addition to these case studies, we ask you to consider the references for our work that we provided in Section 7 (Confidential, Protected or Proprietary Information). In that section, we have provided five different client references that demonstrate the range of services that we can offer the organizations you represent through this contract vehicle.

In addition, in Section 7, we have provided information about our five largest cloud-related contracts within the past two years.

### Exhibit 6. Case Study 1 – Remote Infrastructure Management

<b>Client</b>	Public Transport Victoria
<b>Scope</b>	In this engagement involving the public transportation system of the Australian State of Victoria, an NTT DATA subsidiary developed and managed the new

	smart card system, known as “myki.” Myki is a contactless smartcard ticketing system that stores value that can be used as payment for public transportation fares.
<b>NTT DATA Solution</b>	<p>As part of this engagement, NTT DATA has provided a range of remote infrastructure services to Public Transport Victoria, including:</p> <ul style="list-style-type: none"> <li>• 24x7 remote monitoring and scripted support</li> <li>• Incident, service, and change management</li> <li>• Management of network endpoints, network servers, and virtual servers</li> <li>• Support of storage and database management</li> <li>• Level 1, Level 2, and Level 3 service desk support</li> <li>• Patch release and change management services</li> <li>• Security monitoring and management</li> <li>• User account management</li> </ul> <p>In this engagement, as a prime vendor we also managed a large application development team, Release management, and vendors.</p> <p>Our myki smart card solution went live on December 29, 2013. NTT DATA continues to provide hosting services (both primary services and disaster recovery) co-located at an HP data center.</p>

*In our role creating a new smart card system for the public transportation system of Victoria, Australia, NTT DATA also provided remote infrastructure management services.*

#### Exhibit 7. Case Study 2 – Data Center Migration and Program Management

<b>Client</b>	Association of Chartered Certified Accountants
<b>Scope</b>	<p>The Association of Chartered Certified Accountants (ACCA) is a global association of professional accountants. Before this project, its critical business applications were hosted on technology in the organization’s corporate data center, an uncertified facility with limited fault tolerance. Worse, ACCA’s server infrastructure was at the end of its life and prone to outages, particular at peak times of testing and customer usage.</p> <p>Before NTT DATA was brought on, an incumbent infrastructure outsourcer had been engaged to execute a technology migration to a new infrastructure in a new Tier III data center. Unfortunately, the incumbent failed to deliver a migration plan with sufficient specificity and cost controls to meet ACCA’s acceptance.</p> <p>Delays in achieving an acceptable migration strategy exacerbated issues with the ACCA’s fragile infrastructure and limited plans for functional application improvements. For this project, ACCA needed a partner that could provide a strategy, a plan, and the program management needed to successfully migrate business applications and technology on time and within budget.</p>
<b>NTT DATA Solution</b>	<p>In this project, NTT DATA first helped develop an overall strategy for a migration of ACCA’s applications from its own corporate site to a new dual data center environment, one that would provide high availability and disaster recovery.</p> <p>In this project, our consultants also facilitated consensus building and reduced gridlock with all of the service providers who were involved. Specifically, we orchestrated the project and provided leadership for the infrastructure provider in providing services for the data center infrastructure build and for the hosting service provider. We also worked closely with the wide area network (WAN) service providers; the software and hardware vendors associated with solution delivery; and with ACCA IT staff, who provided legacy systems knowledge and</p>



	<p>governance review.</p> <p>Because of NTT DATA's leadership in this project, the ACCA's migration project is now complete. ACCA's applications have been migrated to newer technology architected for high availability and with disaster recovery capabilities.</p> <p>The ACCA's new test and development environments now support the migrated production systems using NTT DATA engineered virtualization technology for expediting test environment creation, code promotion, and cloning of test configurations. By managing third party providers, NTT DATA enabled the final delivery of the technology environment sought by ACCA along with test migration processes that confirmed the full and final cutover.</p>
--	---

*NTT DATA oversaw an application migration for this global association of accountants.*

#### Exhibit 8. Case Study 3 – Cloud IaaS and DRaaS for Global Apps Development

<b>Client</b>	<p>In this engagement, a major application services provider selected NTT DATA to establish a virtual private cloud that supports a global development team responsible for creating and managing a set of health care applications.</p>
<b>Scope</b>	<p>In this project, NTT DATA built a VMware VCenter with direct access to manage the spin-up and propagation of virtual machine environments (VMs) for support use in development work and testing. We also deployed an environment network fence using appropriate technology to isolate virtual machine configurations whilst still allowing full network access as required.</p> <p>As part of our work with this client, NTT DATA also provides a snapshot capture capability for a VM or a virtual application (vApp) on request and against a calendar. With this capability, we store a backup copy and deliver the ability to restore back to a previous state. We also support the export, import, and porting of operating system (OS) level images with the ability to move images and environments across designated NTT DATA data centers.</p> <p>In this engagement, we also provide:</p> <ul style="list-style-type: none"> <li>• Fail over environment recovery of systems that is wholly independent of all other NTT DATA virtual private cloud customers</li> <li>• A virtual private network (VPN) and multi-connectivity to customer environments from globally-located developer workstations</li> <li>• A consumption-based billing model for this client's cloud computing resources</li> </ul>
<b>NTT DATA Solution</b>	<p>In this engagement, NTT DATA currently provides a self-service virtual private cloud (VPC) environment with a consumption-based usage and pricing model and detailed usage reporting. We also provide portal access to this client so that its employees can view and manage their utilization.</p> <p>We have worked with this organization to help them adopt NTT DATA's VPC as a preferred development and test platform for the health care solutions they have introduced into multiple U.S. states through Affordable Care Act-based websites. As part of this, NTT DATA delivers detailed consumption-based pricing and usage reporting by project and by vApp and VM. This allows this client to easily manage its internal chargebacks for each project.</p> <p>NTT DATA has also set up and now manages a robust customer-specified disaster recover (DR) capability for which we partnered with Zerto, a provider of VM data replication software. With Zerto, we provide cataloged VM replication of our customer's protected VMs and maintain backup/restore service within the customer's defined recovery time objective and recovery point objective defined within the SLA that guides this engagement.</p>

Also, through one of our sister companies in the NTT Group (NTT Communications), we provide a data center backbone that supports backup and DR site-to-site replication between NTT DATA and NTT Communications' RagingWire facilities.

We also have extend our collaboration with Zerto in order to develop a feature specific to this customer for the protection and recovery of the advanced VMware vApp network configurations that are used by the company's complex, multi-tiered applications.

*NTT DATA has established a virtual private cloud for this client.*

### 4.3 Financials (RFP §6.3)

Offeror must provide audited financial statements to the State and should meet 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.

#### Financial Overview

NTT DATA, Inc. is a wholly-owned subsidiary of the NTT DATA Corporation, a publicly-held corporation in Tokyo that generated about \$14 billion in revenue during our last fiscal year, which ended March 31. The NTT DATA Corporation, in turn, is part of the NTT Group, one of the world's largest telecommunications and IT companies and the world's 65th-largest company overall, according to *Fortune* magazine.

Put simply, we are a large, consistently profitable company with the ability to honor the commitments we make to our customers. For your convenience, in Exhibit 9 we have provided a five-year summary of the NTT DATA Corporation's finances.

#### Exhibit 9. NTT DATA Corporation Five-Year Financial Summary

**Note:** All figures are expressed in millions of yen, and all fiscal years shown ended on March 31 of that year.

	2011	2012	2013	2014	2015
<b>Net Sales</b>	1,161,962	1,251,177	1,301,941	1,343,772	1,511,812
<b>Operating Income</b>	78,306	80,416	85,696	62,583	84,013
<b>Net Income</b>	37,313	30,446	43,517	23,287	32,144
<b>Total Assets</b>	1,468,617	1,474,894	1,524,309	1,689,940	1,822,837
<b>Shareholders' Equity</b>	620,370	634,006	660,771	666,742	690,113
<b>Operating Cash Flows</b>	229,077	190,247	161,327	234,524	183,880
<b>R&amp;D Expenses</b>	10,742	13,507	12,105	12,831	12,911

DC1509

*The NTT DATA Corporation is a large, consistently profitable company with the ability to honor the commitments we make to our customers.*

For a more detailed look at the NTT DATA Corporation's financial results during our last fiscal year and for previous years, you may wish to review the annual reports dating back to 1999 available at the following link:

<http://www.nttdata.com/global/en/investor/library/annual-reports/>

For a quarterly summary of NTT DATA Corporation financial results, including quarterly information for the current fiscal year, visit the following link:

<http://www.nttdata.com/global/en/investor/library/financial-results/>

These audited financial statements should help you evaluate the strength of our company. With that said, if you require more information, we would be happy to provide it.

### **Credit Rating**

In your RFP, you specifically inquired about our Dun & Bradstreet (D&B) credit rating.

D&B has not rated the credit of NTT DATA, Inc., or of our parent companies. This is in part because D&B regards the NTT Group as a "public utility" given the group's role as the pre-eminent provider of landline and mobile telephone services in Japan.

Even so, other credit rating agencies have rated the credit of the NTT Group's flagship company, the Nippon Telephone and Telegraph (NTT) Corporation. For example:

- Moody's has rated NTT's long-term obligations as Aa3. Obligations in this category "are judged to be of high quality and are subject to very low credit risk."
- Standard & Poor's has rated NTT's long-term obligations as AA-. An obligation with this rating "differs from the highest-rated obligations only to a small degree" and the "obligator's capacity to meet its financial commitment on the obligation is very strong."

Either of these ratings compare favorably to a D&B rating of 3A2 or better. For example, our Moody's and Standard & Poor's ratings are both generally regarded as "high grade," whereas a 3A2 is generally regarded as a "good" (rather than a "high") rating.

For more information about the NTT Corporation's financials, including audited statements, please visit the following website: [http://www.ntt.co.jp/ir/library\\_e/results/](http://www.ntt.co.jp/ir/library_e/results/)

We would welcome the opportunity to share more information about our credit worthiness. In the meantime, for more information on D&B's assessment of our company, please see Appendix 3 (D&B Report), which contains our D&B report and our D&B number for your reference.

## **4.4 General Information (RFP §6.4)**

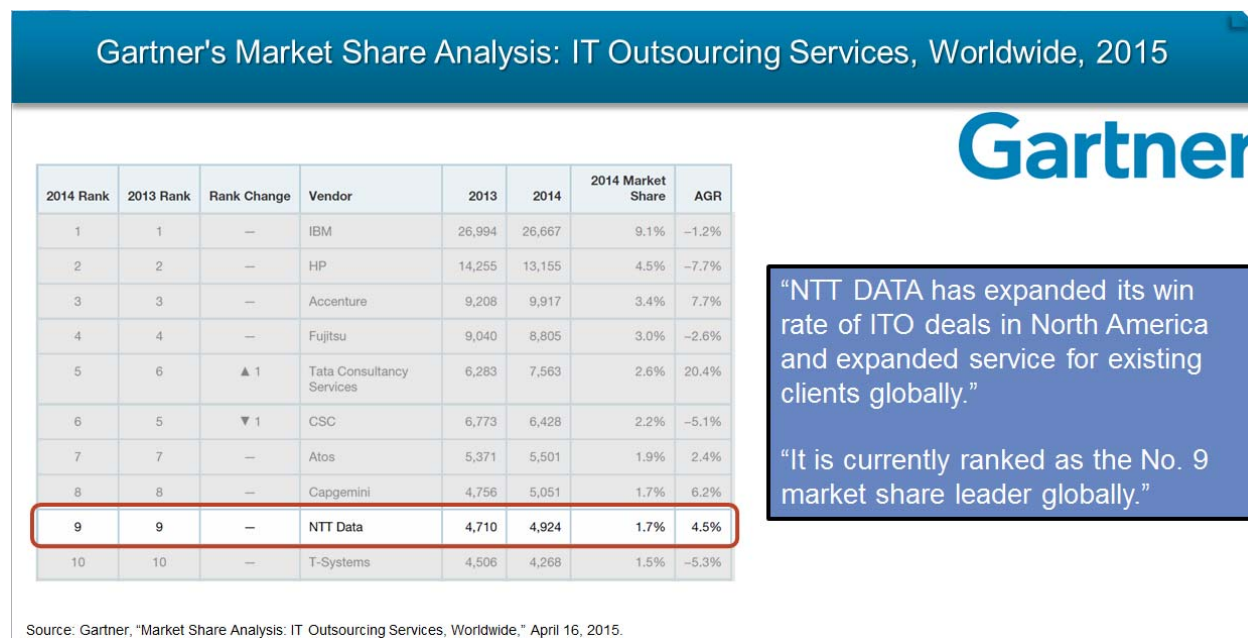
### **4.4.1 Depth and Breadth of Services**

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

NTT DATA is a world-class IT provider. Our offerings range from data center space and carrier-class bandwidth to infrastructure services, application development, and support. Respected third-party IT analysts agree that NTT DATA is a respected leader in the industry, as the following exhibits show.

For example, Exhibit 10 shows that NTT DATA (including our parent company) is the world's ninth-largest provider of IT outsourcing services.

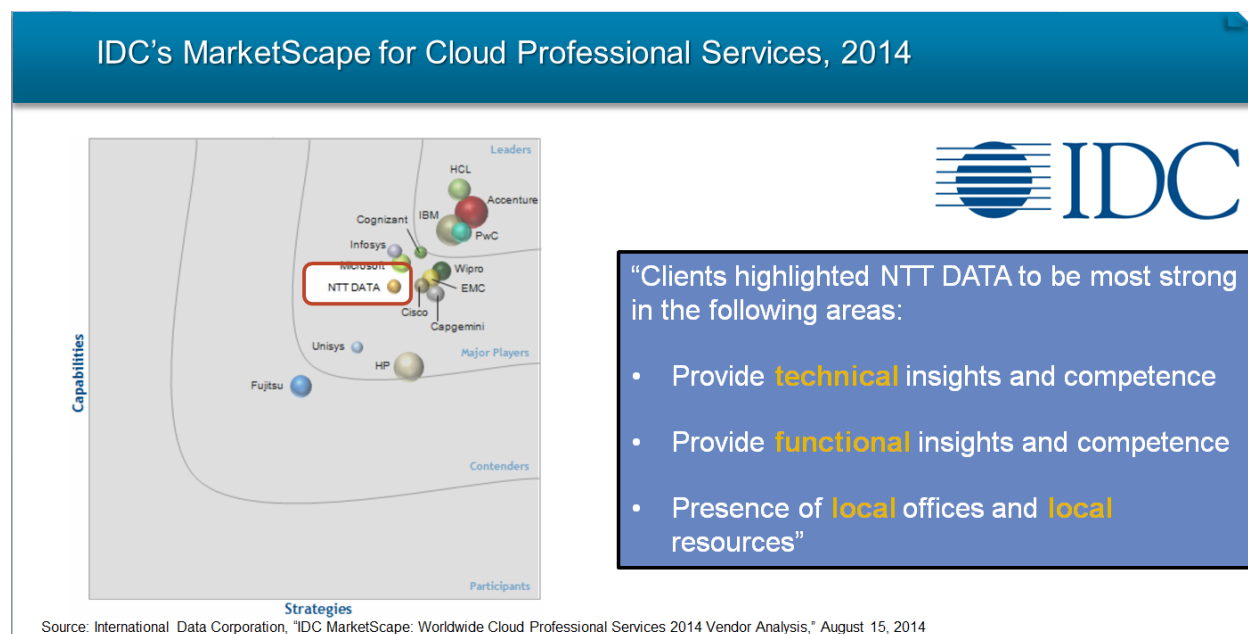
Exhibit 10. Gartner's Market Share Analysis Report



*NTT DATA is the world's ninth-largest provider of IT outsourcing services.*

Also, as Exhibit 11 shows, a third-party analyst ranks NTT DATA as a major player in the field of cloud professional services.

Exhibit 11. IDC Report for Cloud Services

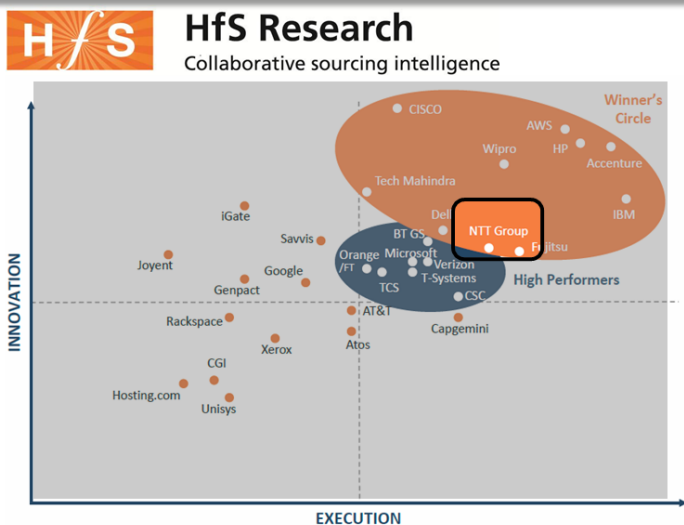


*IDC ranks NTT DATA as a major player in the field of cloud professional services.*

The NTT Group, of which NTT DATA is a part, is highly-ranked as a cloud infrastructure services provider, as Exhibit 12 shows.

Exhibit 12. HfS Research Report

HfS Research's Blueprint for Cloud Infrastructure Services, 2014



"When it comes to **Cloud Infrastructure Services**, NTT has been a bit of a hidden secret for a long time. This is now over. Today, NTT needs to be **considered on RFP shortlists** for Cloud Infrastructure Services."

- Dr. Thomas Mendel, SVP IT Services Research, HfS

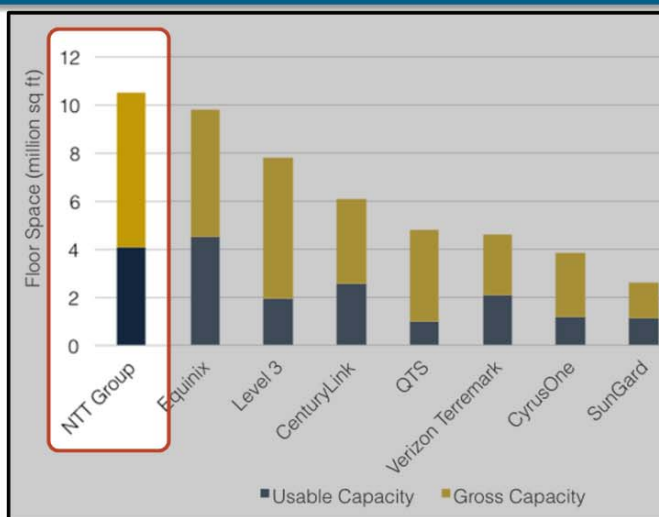
Source: HfS Research, "HfS Blueprint Report, Cloud Infrastructure Services," May 2014.

*The NTT Group is part of HfS Research's winner circle for cloud infrastructure services.*

The NTT Group is also largest retail data center operator in the world, as measured in gross floor space. Exhibit 13 offers more detail.

Exhibit 13. TeleGeography Report for Largest Retail Data Center Operators

Largest Retail Operators by Gross Floor Space, 2014



NTT Group has **10.5 million** square feet of gross floor space worldwide.

"If only tallying its international footprint outside Japan, NTT would still be counted among the **ten largest** global operators."

Source: TeleGeography, "Colocation Database," 2014.

*The NTT Group has 10.5 million square feet of gross floor space worldwide, more than any other provider.*



NTT DATA also has more than 120 IaaS clients hosted in our IaaS virtual private cloud. This cloud supports more than 220 clients overall in a variety of industries.

#### 4.4.2 Auditing Capabilities

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.

NTT DATA's auditing capabilities and reports are consistent with SAS 70 or later versions, including SSAE 16 6/2011 or greater.

### 4.5 Billing and Pricing Practices (RFP §6.5)

#### 4.5.1 Billing and Pricing Practices

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

For this engagement, we recommend using a pay-as-you-go method of subscription to our cloud (IaaS) services. In this method, sometimes known as a consumption model, a purchasing entity will be charged only for the computing and services actually consumed (as measured by GHz, RAM, SAN storage, and backups, for example). In other words, when all or part of the environment is idle, this method will incur just storage costs for data and for those servers and virtual machine "templates" that remain idle.

Specifically, in our pricing methodology:

- NTT DATA virtual machine (VM) pricing is based on the average daily usage of compute (GHz) and RAM consumed in a 24-hour day averaged across the number of days per month.
- SAN pricing is per gigabyte (GB) allocated or consumed per month.
- Backups and DR replication are priced based on the amount of data or VMs protected.
- Virtual desktop pricing is based on the average daily usage of desktops averaged across the number of days per month.
- Monitoring and managed services are priced per VM and according to the level of service requested (gold, silver, bronze or some variation).
- Dedicated client technology is based on an amortized cost per month spread over the term of the hosting agreement.

#### Pricing on average use, not peak bursts

Note that NTT DATA's pricing is based on **average daily use**. It is not based on peak burst utilization during the month, as in some other pricing models.

Our standard practice is to develop and present invoices in the month following the services and outline the details as appropriate for professional and usage-based services. Depending on customer requirements, we can present pricing information within an acceptable level of detail. For example, a purchasing entity can receive detailed billing by project or by cost center. We will work with each purchasing entity to develop a suitable report format early in the transition process. Pricing is available in Excel spreadsheet form as:

- A monthly summary (rollup)
- Monthly by pricing component (rate card line item), listing units consumed per month

- Daily by pricing component (rate card line item). (Note that this daily report can be voluminous; many of our clients only request daily reporting in special cases.)

Exhibit 14 contains sample line items from a monthly report.

Exhibit 14. Sample Monthly Report

Service Area	Component	Metric Unit	Period	Unit Rate	Quantity	Extended Price
Virtual Machine (VM)	CPU (No DR)	GHz	Monthly	\$XX.XX	Y.Y	\$ZZZ.ZZ
	CPU (with DR)	GHz	Monthly	\$XX.XX	Y.Y	\$ZZZ.ZZ
	RAM (No DR)	GB	Monthly	\$XX.XX	Y.Y	\$ZZZ.ZZ
	RAM (with DR)	GB	Monthly	\$XX.XX	Y.Y	\$ZZZ.ZZ

*These are sample lines from a sample monthly report.*

In addition to our billing practices, all clients have access to Cloud Cruiser metering software at no charge. This software permits our clients to gather metering information about their environments to support sophisticated analyses. With this software, a purchasing entity can break down usage, costs, and revenue associated with cloud services by organization at the department or even at the individual level. Purchasing entities will also be able to construct chargeback regimes so that cloud usage can be accounted for and properly assigned.

Please refer to the file we have attached with this technical proposal (named “6.5.1 Cloud Cruiser Overview.pdf”) for a more complete description of Cloud Cruiser’s extensive capabilities.

#### 4.5.2 Cost Impacts

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

Implementing a cloud solution can cause cost increases or decreases, depending on the specific situation. The three most common reasons for decreases we have seen, based on our work with other clients, include:

- **Decreased facilities costs.** Moving workloads into our cloud can permit clients to reduce floor space or even close facilities dedicated to hosting equipment.
- **Decreased operational costs.** With NTT DATA assuming responsibility for many remote infrastructure management (RIM) functions, our clients are often able to rationalize support staff, sometimes resulting in significant cost savings.
- **Decreased capital costs.** Moving to a consumption-based cloud model converts many capital expenditures to operating expenditures. This reduces interest charges and permitting charges covered by different budgets, often resulting in lower overall expenditures.

The three most common reasons for cost increases we have seen include:

- **One-time transition costs.** Such costs are needed to migrate systems and data as well as to transition support services to our Service Operations Center.

- **System reconfiguration and rationalization costs.** Often, changes must be made to the way things work today to accommodate a new environment. The size of these one-time costs vary greatly depending on the situation.
- **Network and bandwidth charges.** Reconfiguration may require new circuits and increased WAN bandwidth to support access to the production and DR sites.

Again: The impact of a cloud solution on costs can vary greatly, depending on the situation. In order to determine the exact requirements and the impact on costs, a detailed analysis is required during the project proposal and planning phases for both the client and the cloud provider.

### 4.5.3 NIST Compliance

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.

#### Overview

We certify that NTT DATA's offering is compliant with the IaaS service model described in NIST Special Publication 800-145. Using our services, a cloud consumer can provision processing (server or desktop), storage, network and other fundamental computing resources from a resource pool. This provisioning can either be done by the consumer or in cooperation with NTT DATA's Service Operations Center team.

Specifically, the consumer can run arbitrary software, including Windows, Linux, AIX and iSeries operating systems and applications on our V+C+E and Power 7+ Architectures. The consumer cannot manage or control the underlying infrastructure, but has control over operating systems, storage, and deployed applications, including limited control of select networking components. In the rest of this section, we will share more information illustrating how we achieve compliance.

#### Provisioning

Customers can orchestrate the provisioning (or de-provisioning) of compute and storage resources in two ways:

- Customers can enter a service request for changes to their environment by entering a ticket in our BMC Remedy ticketing system. That request is reviewed as part of our change management process. Non-emergency changes are implemented within 5 days. This process is recommended for changes to production environments and is required for environments guided by an SLA.
- Our infrastructure and performance monitoring portal allows clients to create and destroy virtual machines and associated storage and storage protection levels (such as backup and replication). (See the attached users manual for our cloud portal, named "3.6.3 Create a vApp with VMs v1.2".)

Note that logical network segmentation via firewall, if required as part of a change, must be created through the established cloud technical change process. That typically takes 5 days. In addition to our cloud portal, which is used for managing virtual instances, our Cloud Cruiser usage analytics portal (see the attached document, named "6.5.1 Cloud Cruiser Overview", for more detail) can be used to measure consumption of business and technical resources in detail.

In our approach, all portals are customized to the client's requested services and contractual SLAs. These portals include easy-to-use interfaces provided by BMC and EMC and customized by NTT DATA.



## Resource Pool

Our IaaS offering is based on two technologies: the V+C+E architecture enabled by VMware and the Power 7 Architecture implemented on IBM 770 and 780 equipment. Our V+C+E environment enables our customers to rapidly create (and destroy) Windows and Linux workloads from templates using VMware vCenter supervisor software. Our Power 7 environment enables our customers to rapidly create (and destroy) AIX and Linux workloads. We rely on EMC virtualized storage to provide a pool of allocatable storage. These compute and resource pools can be billed on a consumption basis so our customers are only billed for resources they actually consume.

Both of these architectures provide dynamic pools of compute and storage resources that can be intelligently provisioned and managed to address changing demands (through scalability). This empowers our customers to be nimble enough to pursue a fleeting business opportunity, or to deftly manage an administrative crisis.

## Run Arbitrary Software

NTT DATA can provide private cloud hosting. When we do, cloud consumers can stand up arbitrary hardware to support any software based on any operating systems they choose. NTT DATA can provide RIM services to manage such an environment.

NTT DATA also provides the following listed IaaS Community Cloud services:

- **Compute.** NTT DATA provides Windows, Linux, AIX and iSeries compute resources drawn from our pools hosted on V+C+E and Power 7 systems.
- **Storage.** NTT DATA provides a pool of storage compute resources drawn from our pool hosted on our SAN containing EMC Enterprise storage frames
- **Backup and Recovery.** We provide backup and recovery services through our Avamar/Data Domain infrastructure with automatic replication of backups to our DR site. We also provide Zerto-based disaster recovery from replicated data. For more information on our capabilities here, see our responses to Question 8.8.1 and Question 8.8.2, in Section 6.8 (Service or Data Recovery) of this proposal.
- **Services Management.** NTT DATA provides service management capability through our BMC toolset. This allows clients to monitor and manage infrastructure performance and capacity. We offer such service in three levels (bronze, silver, and gold), depending on the level in the technology stack of management required.
- **Platform Services.** Services for managing platforms running within our VPC are available for infrastructure directly through our Service Operations Center. For other platforms, NTT DATA has 50 years of experience managing a wide variety of technologies. We can provide platform management services from large scale systems, including both packaged platforms (such as SAP, PeopleSoft and Oracle EBS) to unique software applications.
- **Content Delivery.** In this proposal, we assume that content delivery services will be available through the Cloud Carrier. We recommend that our clients contact bandwidth service providers for connectivity to our site and for content delivery network (CDN) services

When we provide these services, our clients can stand up arbitrary software that runs on designated operating systems that we provide. Subject to that constraint, cloud consumers can run any software supported by those operating systems with full administrative control of virtual servers, storage, and network devices.

## 4.6 Scope and Variety of Cloud Solutions (RFP §6.6)

### 4.6.1 Scope and Variety of Service Models

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

#### Overview of Services

NTT DATA offers IaaS as defined by NIST. Our IaaS includes:

- Windows and Linux virtual machine pools on a VMWare enabled V+C+E architecture
- AIX, iSeries, and Linux machine pools on a Power 7 architecture
- Storage pools on an EMC VNX architecture
- Backup and restore services on an Avamar/Data Domain architecture
- Virtual network components such as firewalls and load balancers

We also supply security services, as we have described throughout the document. Our IaaS offering can also support production, test/development/staging, and disaster recovery environments. We also offer disaster recovery as a service (DRaaS) and virtual desktop as a service (VDI/DaaS).

NTT DATA also offers 24x7 access, monitoring, and management of infrastructure through our Service Operations Center. These services include:

- Monitoring services for IT infrastructure
- Server, operating system, and storage management
- Database administration for SQL, Oracle, and other technologies
- Desktop services through our VDI-based DaaS
- Network management
- Infrastructure application management (such as messaging and DNS services)
- Application support (such as for SAP Basis, Oracle E-Business suite or PeopleSoft)

Our Service Operations Center includes a service desk that reduces the cost and complexity of service management with a single point of accountability. NTT DATA consolidates responsibility for vendor management and service delivery across the entire technology stack, including hardware, networks, and applications.

NTT DATA's end-to-end service desk support includes:

- First-level support for desktops and laptops, infrastructure, and applications issues
- Second-level management of more complex issues
- Third- and fourth-level support through our consulting services group and our center of excellence (These areas of our company contain expertise for common technologies such as server configuration and architecture, storage architecture and database support for common database types such as SQL, Oracle, and DB/2.)
- A single point of contact for all IT-related issues.

## 4.7 Best Practices (RFP §6.7)

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.

The NTT DATA virtual private cloud relies on an architecture, tools, and policies and procedures that protect data from threats at the appropriate risk level.

**Architecture.** NTT DATA has implemented a defense-in-depth architecture with several layers of data protection and monitoring points. Protections include network intrusion detection and protection services at network and virtualization layers allow to better protect data against known attacks. Also, strict data segregation prevents data breach across organizations and firewalls further segment data access to prevent unauthorized access.

**Tools.** NTT DATA provides tools at the IaaS level so that application developers can implement encryption within their applications. For instance, encryption is offered at the operating system level; any client that wishes to encrypt their servers can use encryption to protect their data from exposure. NTT DATA can encrypt data at rest using AES 256-level encryption for storage and backups.

NTT DATA does not have visibility into the actual content of data, so tokenization should be implemented at the application level.

**Policies and Procedures.** As we indicated in a couple of attachments that we submitted along with this technical proposal (specifically, “NTT DATA’s Report on Exhibit 1 to Attachment B - CAIQ v3 0 1-09-16-2014” and “NTT DATA’s Report on Exhibit 2 to Attachment B - CSA\_CCM\_v3 0 1-09-16-2014.xlsx”), NTT DATA has an extensive array of defined policies to promote visibility, compliance, data security, and ongoing monitoring of threats.

Our vulnerability assessment monitoring promotes up-to-date notification of new threats and successful remediation of potential vulnerabilities. Also, our incident management policies and procedures are designed to surface issues rapidly and with all the information needed to address the issue at hand. We perform reviews at appropriate frequencies ranging from yearly to quarterly to whenever circumstance change.

## 5. Organization Profile (RFP §7)

### 5.1 Contract Manager (RFP §7.1)

#### 5.1.1 Contact Details of 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.

Our contract manager, Brian Nicolson, will fulfill the roles and responsibilities synonymous to the definition of contract manager. Exhibit 15 contains more information about Brian.

Exhibit 15. Contract Manager Details

Contract Manager Name	Brian Nicolson
Phone Number	469-441-1270
E-mail	<a href="mailto:Brian.Nicolson@nttdata.com">Brian.Nicolson@nttdata.com</a>
Work Hours	7 a.m. to 7 p.m. Mountain Time, Monday through Friday

*This table shows contact information for Brian Nicolson, our proposed contract manager.*

We have also identified a delivery manager who will serve as the focal point for delivery activities. This individual is Dan Peet. Exhibit 16 contains more information about Dan.

Exhibit 16. Delivery Manager Details

Delivery Manager Name	Dan Peet
Phone Number	902-403-0080
E-mail	<a href="mailto:Daniel.Peet@nttdata.com">Daniel.Peet@nttdata.com</a>
Work Hours	7 a.m. to 7 p.m. Mountain Time, Monday through Friday

*This table shows contact information for Dan Peet, our proposed delivery manager.*

We will provide more information about Brian and Dan in the next section.

#### 5.1.2 Contract Managers Experience

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.**

As we indicated, our plan is for Brian Nicholson to serve in the role of contract manager and for Dan Peet to serve as delivery manager.

**Brian Nicolson** is an IT professional with more than 37 years of experience ranging from computer center operations and programming to strategic business planning using IT as a core enabler for innovation, expansion, efficiency, and cost management.

In his long career Brian has developed wide experience in the design, implementation and support of full business enterprise program suites. He is particularly skilled when it comes to SAP's Enterprise Core Component (ECC), Customer Relationship Management (CRM), and Supplier Relationship Management (SRM) suites. These skills are in addition to his understanding of fundamental IT infrastructure and business processes.

Most recently Brian has contributed to successful implementations of public sector-specific SAP applications for Public Budget Formulation (PBF) and Procurement for Public Sector (PPS). For more than 7 years, Brian has been engaged as an operations director based in the Denver area, where he has helped a public sector client develop a center of excellence (COE) and grow internal skills when it comes to the responsible manage of SAP applications. He has also provided teams of consulting professionals to deliver outsourced application managed support and the implementation of new SAP functionality for this client.

In his current and previous positions, Brian has been responsible for managing all application consulting team delivery across North America. He has also served as program director for key clients, provided hands-on management of joint client/consultant teams, and taken direct responsibility for team performance reporting to his client's executive management.

For a detailed resume for Brian, please see Section 7 (Confidential, Protected or Proprietary Information).

**Dan Peet** works as a senior delivery manager for several different NTT DATA clients, where he is responsible for all aspects of delivery and account operations globally. He is also responsible for managing NTT DATA's Canadian operations for cloud infrastructure services, which are based in Halifax, Nova Scotia.

Dan offers experience providing managed service delivery on the evening and overnight shifts for an outsourced project team. His responsibilities include staffing and training, workflow and SLA management, and client communications. His outsourcing experience includes service management migrations, new project implementations, and operations management.

### 5.1.3 Roles and Responsibilities

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.

In Exhibit 17, we have summarized the roles and responsibilities of our contract manager and our delivery manager as they apply to the NASPO ValuePoint master agreement.

#### Exhibit 17. Roles and Responsibilities of Contract Manager

Roles	Responsibilities
Contract Manager	<ul style="list-style-type: none"><li>• Implement and maintain the agreement as written and within the spirit of the agreement</li><li>• Comply with applicable laws and regulations</li><li>• Provide guidance to NTT DATA account teams related to contract specifics</li><li>• Manage contract related issues in a timely and complete manner</li><li>• Make sure contract deliverables are agreed to and completed</li><li>• Manage Contract Change Controls</li><li>• Manage Contract Issues/Disputes/Clarifications</li><li>• Ensure Root Cause Analysis /Corrective Action Plans are completed</li><li>• Manage work associated with Government Audits and Open Records requests</li></ul>

Roles	Responsibilities
	<ul style="list-style-type: none"> <li>• Work with the NTT DATA legal team and the State of Utah/NASPO's purchasing/contract manager</li> <li>• Become familiar with each purchasing entity's rules policies and procedures for compliance purposes</li> <li>• Make sure an SLA document is approved according to the law of the purchasing entity</li> <li>• Resolve payment disputes</li> <li>• Monitor compliance to Data Access Controls</li> <li>• Monitor that Records Administration and Audit is implemented and working</li> <li>• Oversee compliance to Data Privacy and Data Classification as agreed upon in the SLA or Statement of Work</li> <li>• Establish required reporting</li> </ul>
Delivery Manager	<ul style="list-style-type: none"> <li>• Will have overall responsibility for managing the engagement and interfaces regularly with the purchasing entity relationship or project manager.</li> <li>• Tracks status, and escalates and resolves issues and risks.</li> <li>• Coordinate with the contract manager for contractual issues.</li> <li>• Has deliverable acceptance and engagement change management process authority on behalf of NTT DATA.</li> <li>• Participates in the stakeholders' and project sponsors' meetings</li> <li>• Serves as a single point of contact at NTT DATA for the purchasing entity relationship</li> <li>• Track overall progress of project execution and quality deliverables</li> <li>• Manage NTT DATA personnel</li> <li>• Manage scope change through change management process</li> <li>• Act as a primary contact for the client for project-related tasks, issues, and information needs.</li> </ul>

## 6. Technical Response (RFP §8)

---

### Our Ability and Approach

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

#### Introduction

NTT DATA is a premier provider of private and virtual private cloud (VPC) computing infrastructure. We provide a range of managed cloud services, including physical and virtual computing services, cloud storage, a range of backup, replication and restore capabilities virtual desktop services, disaster recovery support and the remote infrastructure management services needed to assure the integrity and availability of the information processed by our clients using our cloud.

#### Our Understanding

Our understanding is that NASPO—through the State of Utah, serving as lead state—is requesting proposals for cloud solutions in furtherance of the ValuePoint Cooperative Purchasing proposal. The purpose of these proposals is to provide information about the cloud services that can be purchased by NASPO participating entities through a ten year master agreement.

The participating entities that comprise NASPO vary greatly in size, complexity and technological maturity and therefore their requirements for cloud services differ significantly from one to another. Therefore NASPO has asked proposal respondents to describe a complete menu of the cloud services they provide so that participating entities can select cost effective solutions that are appropriate for their needs. NTT DATA can accommodate purchasing entities' requirements.

NASPO expects that these cloud solutions will be compliant with the NIST Reference Architecture and will meet the NIST essential characteristics, including:

- **Storage available by Risk Categories.** Purchasing entities—meaning a participating entity that uses the master agreement through a participating addendum—classify storage by risk category according to their own unique requirements. NTT DATA provides storage to support low, medium and high risk data classifications as to integrity, confidentiality and availability as an integral part of our cloud services. We provide multiple levels of backup and disaster recovery services that accommodate different availability risk levels as well as data segregation services to accommodate different integrity and confidentiality requirements.
- **NIST characteristics.** NTT DATA's cloud offering meets the five essential NIST characteristics of on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service as described in our response to Question 8.1.2 (in Section 6.1.2). Purchasing entities can rapidly access our cloud instances over broad networks to quickly add or subtract cloud computing and storage resources. We provide transparent measurement of service consumption.



- **Service model.** NTT DATA provides IaaS, which will provide purchasing entities the ability to run arbitrary software (including operating systems and applications) in server or desktop environments. Our capabilities in this area are described throughout this response.
- **Deployment methods.** NTT DATA deploys private, community and hybrid clouds, as we will describe in more detail in our response to Question 8.1.5. While we provide self-service capability, we do not provide arbitrary public access to cloud resources.

### Cloud Hosting Services

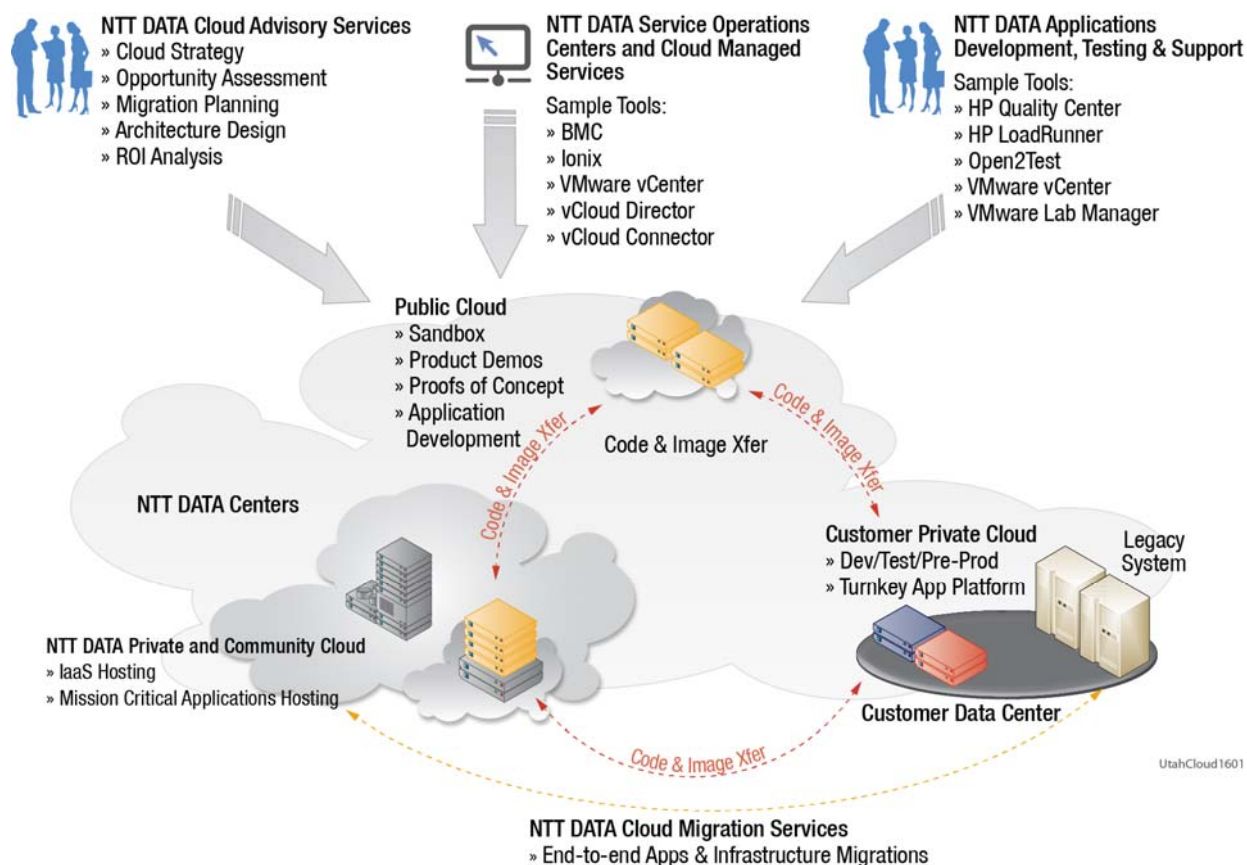
NTT DATA provides a hosting solution that spans all infrastructure models, operating from multiple datacenters with full data replication and disaster recovery capabilities. Specifically, we offer:

- Vendor-agnostic hosting of client or NTT DATA-developed applications in our secure virtual private cloud
- Support for Windows, Linux, AIX, iSeries server open systems
- Support for Windows or Linux virtual desktops
- Available mission-critical applications hosting and support with custom service level agreements
- Migration services to move client systems and data into the VPC.

We offer customized cloud implementations, with applications hosted in private, community or hybrid environments as shown in the following exhibit. These services are based on our customers' specific business and security priorities.



## Exhibit 18. Fully Integrated Cloud and Infrastructure Services



*Our Cloud services span the entire Cloud lifecycle, from advisory services to migration and managed services.*

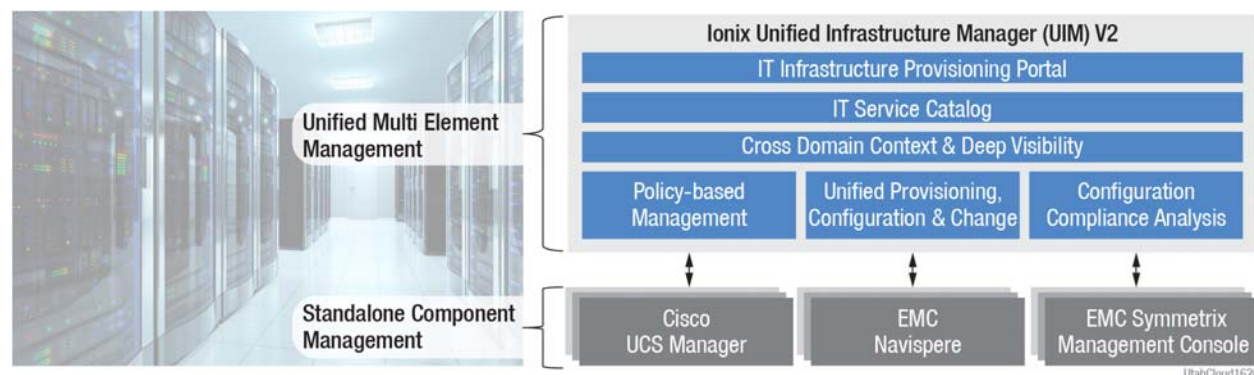
## Cloud Platforms

NTT DATA's virtual private Cloud computing capabilities are based on two platforms: the V+C+E Systems and the IBM Power7 pSeries described below. Our DaaS service offering is based on a hybrid subset of our V+C+E architecture. We develop new platforms as technology permits and market demand dictates.

## V+C+E Systems

NTT DATA provides private Cloud computing services for the Windows and Linux platforms by making use of the integrated technology offerings of VMware, Cisco, and EMC. The Virtual Computing Environment (VCE) coalition's architecture represents an integrated solution for Cloud, based on best-in-class computing, network, and storage technologies.

## Exhibit 19. Virtual Computing Environment



NTT DATA uses V+C+E architecture to rapidly scale up or scale down all resources and deliver the efficiency and business agility of virtualization and Cloud computing. Using this architecture, we seamlessly integrate powerful computing, networking, and storage technologies from industry leaders such as Cisco, EMC, and VMware.

Our solution also provides dynamic pools of resources that can be intelligently provisioned and managed to address changing demands (through scalability). This empowers our customers to be nimble enough to pursue a fleeting business opportunity, or to deftly manage an administrative crisis.

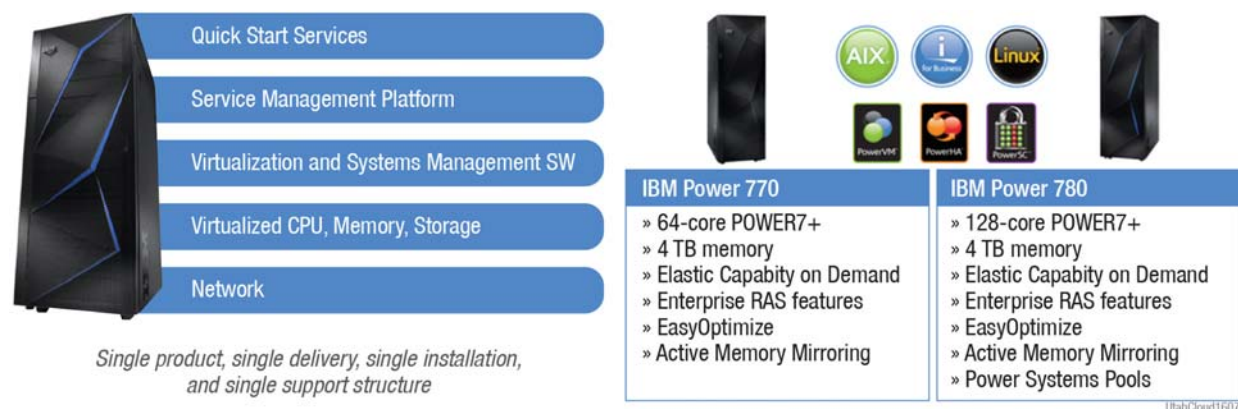
From a business and operations standpoint, our platform is both rapidly deployable and simple to upgrade. It is also secure.

The platform integrates end-to-end security, and VMware vShield to provide a comprehensive set of security services at the host, network, application, data, and endpoint levels via a single management framework. This reduces the need to piece together a patchwork of point solutions for legacy equipment.

### Power7 (pSeries)

NTT DATA uses IBM Power7+ technology capable of hosting enterprise AIX, iSeries, i5/OS and Linux workloads and applications and fast private Cloud deployment. An overview of this technology is depicted below.

## Exhibit 20. IBM Power7+ Technology

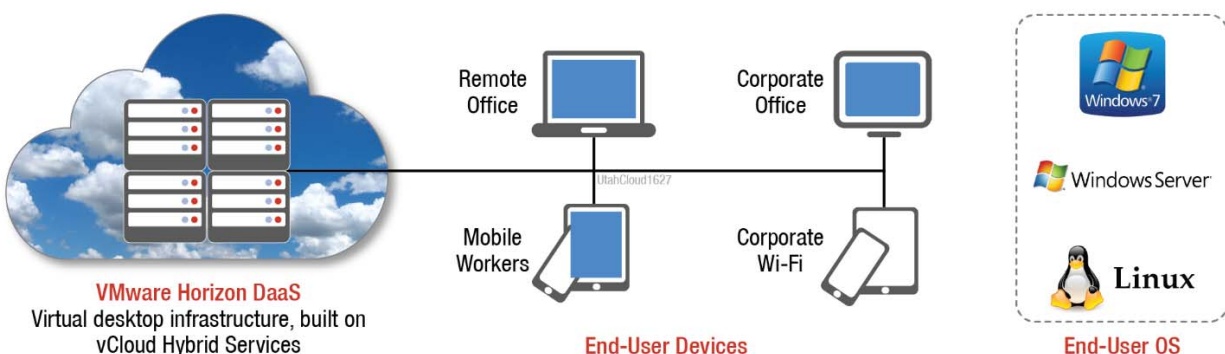


*Among the IBM Power7+ technologies used by NTT DATA are the IBM Power enterprise models such as 770 and 780.*

## Desktop as a Service

NTT DATA uses VMWare Horizon desktop-as-a-service (DaaS) to implement a virtual desktop infrastructure (VDI) that can support hundreds of desktops as a cloud service. A DaaS management dashboard provides a single point of control facilitates three click deployment of virtual desktops from templates that can be seamlessly connected to Active Directory or other access protocols.

Exhibit 21. Desktop as a Service



*This exhibit summarizes our DaaS offering.*

## Other Cloud Technologies

Our virtual private Cloud uses a number of other technologies, including:

- **SAN**– We have standardized our storage area network (SAN) with EMC VNX2 8K SAN arrays. Also:
  - This enterprise solution offers redundant storage processors, power supplies, drive paths, and SAN switches.
  - It also uses battery backup storage processors to ensure write cache completions and has the ability to support all types of RAID scenarios, proactive hot sparing, and instantaneous fault detection using call home features to the vendor.
  - Our SAN includes a combination of SSD, Fiber Channel, and SATA drives leveraging EMC's Auto-Tiering and FAST VP technologies to intelligently place data on the appropriate drive type.
- **Network** – Our entire network architecture, based on Cisco Nexus switches, is designed to support N+1 fault tolerance. Also:
  - All switches have a redundant partner working in an active/active manner.
  - This includes Ethernet switches, SAN switches, firewalls, and Internet connections.
- **Power** – All of our equipment uses a minimum of two power feeds per device. Also:
  - Each feed is supplied to cages from distinct locations using separate UPS devices and generators so that a single power event on one feed will not impact our service offering.
  - The data center in which our production equipment is hosted provides 2N+2 power and cooling, providing Tier IV+ capability as described by the Uptime Institute.

- **Virtual Technology** – Our VMware-based platform uses the latest in virtual technology and clustering for supporting Windows and Linux systems as well as a Virtual Desktop Infrastructure (VDI). Also:
  - All physical hosts in an ESX cluster are redundantly dispersed across multiple blade chassis.
  - This provides us the ability to handle entire blade chassis failures without disrupting services to our customers.
  - Utilizes vCenter vCloud Director and VMware's HA auto-recover technology
  - VDI in the Cloud Offering

In the event of a single host or blade chassis event, the virtual machines on the effected host will be brought back online automatically utilizing VMware's HA technology. These VMs will act as if they have recovered from an unexpected reboot and will be back online supporting connections within minutes.

We can leverage VMware's and Zerto's fault tolerance technology for Windows and Linux systems. Our Power7 platform can virtualize AIX systems into logical partitions using technology that IBM has deployed since the early 1970s.

### Platform Services

We supplement these Cloud technologies with several important services. Among them:

- **Proactive Monitoring.** We will provide proactive capacity and performance monitoring of the Purchasing Entity's production environment. As part of this service, we will establish thresholds for CPU, data storage, RAM and other resources. Once these thresholds are exceeded, our team will be notified that upgrades are required. This allows us to perform standard change process in making these upgrades before performance is impacted. Any additional capacity requests—including servers, RAM, and storage—will be installed and ready for integration in less than 5 business days, emergency and self-service deployments can be completed more quickly.
- **Patch and Release Management.** Under available silver support, the NTT DATA team will be responsible for patch and release management of all hardware, firmware, operating systems, and, under gold support, database software. (See our response to Question 8.19 for a discussion of available support levels.) Schedules for upgrades and patches will be jointly defined between the NTT DATA team and the Purchasing Entity at the outset of our engagement. Our team will make no changes to the system without following proper change management and approval processes that typically involve thorough testing before promotion to production. We prefer, to the extent practicable, to follow a timely upgrade and patch management schedule that prevents our customers from lagging behind current releases unless we jointly make the decision to postpone upgrades regarding specific releases.
- **Data Backup and Recovery.** The NTT DATA's data backup and recovery pricing for data within the VPC is based on providing perpetual incremental backups of designated data. Also:
  - NTT DATA uses EMC Avamar software and appliances with advanced de-duping technology and agents installed on the servers to perform the backup/restore process.
  - The NTT DATA storage services architecture is designed for high availability with redundant switching and host bus adaptors, and it uses enterprise class storage arrays from EMC and other vendors.



- These safeguards enable NTT DATA to meet the throughput and input/output requirements of the Purchasing Entity without affecting performance.
- NTT DATA adheres to industry storage standards, including proper disk and storage management, managing disk cache, read/write times and disk utilization.
- **Capacity and Sizing.** Our team can develop estimates for base disk and CPU capacity and sizing requirements based on your system environments. We will then monitor capacity and work, with purchasing entity's approval, to bring additional resources on line (or remove excess resources) in a timely manner.

## 6.1 Technical Requirements (RFP §8.1)

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.

### 6.1.1 Cloud Service Models

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.

#### Overview

We will provide infrastructure as a service (IaaS) to eligible users. We will deploy this service using a private, community, or hybrid model, depending on user requirements

Our virtual private cloud (VPC) and our production instance is hosted in our world-class Tier IV+ datacenter located in Ashburn, Virginia. Our disaster recovery instance is located in our Tier IV datacenter located in Sacramento, California. (Tier IV is a strong standard; if you seek more information on Uptime Institute standards, we can provide you more information on the institute's definition of data center tiering.)

Our proposed datacenters have an enterprise class cloud environment capable of hosting *Fortune* 500 companies, state government agencies and other entities.

NTT DATA is a premier provider of VPC computing infrastructure as a service. We provide a range of managed services associated with our VPC, including the generation of virtual machines (VMs) for various operating systems, the management of compute, storage, network and a range of backup, disaster recovery and restore services.

NTT DATA provides a single hosting solution that spans all infrastructure models, operating from multiple datacenters with full data replication and disaster recovery capabilities. Specifically, we offer:

- Vendor-agnostic hosting of client or NTT DATA-developed applications in our secure private Cloud

#### NTT DATA VPC: A Community Cloud for Large Organizations Across the U.S.

NTT DATA offers a technologically advanced, electrical infrastructure with patented 2N+2 redundancy, which is twice the redundancy of a standard Tier III datacenter

Our cloud is highly secure, with three-factor identification required for data floor access, a 24x7 armed, in-house security team, and exterior barriers that include 12-foot security fencing and perimeter bollards

Our primary datacenter is SSAE 16 Type 2 and Payment Card Industry Data Security Standard (PCI DSS) certified. It also complies with the standards of the Federal Information Security Management Act of 2002 (FISMA)

Our primary data center offers high-density power backed by a 100 percent availability for power and cooling.

- Mission-critical applications hosting with custom service level agreements
- A platform for delivering NTT DATA software development lifecycle (SDLC) services
- Commercial software solution hosting and licensing services for application suites such as SAP, Oracle, PeopleSoft, SharePoint, and Infor
- Hosting, either for commercial products or client-developed solutions.
- Migration services to move client systems and data into the VPC. We expect migration to require three months of effort in typical cases

We offer customized Cloud implementations, with applications hosted in public, private, or community environments as shown in the following exhibit. These services are based on our customers' specific business and security priorities.

### IaaS Services

Exhibit 22 lists the services we offer, presented as you as you listed them in RFP Attachment C along with any applicable exceptions or additions.

Exhibit 22. IaaS Services

Service Category	Service Sub-Category	Comment
Computer/Infrastructure Services	Operating systems	Linux, Windows, AIX, iSeries
	Hypervisors	VMWare, Power 7
Disaster Recovery	Business Continuity	Offered. See our response to Question 8.15.
	High Availability / Failover	Offered
GIS		NTT DATA does not offer GIS services. We do not classify these as infrastructure and expect the client to provide these systems.
Storage	File	Offered
	Block	Offered
	Object	Offered
	Archive	Offered
	Cache	Offered
	Content Delivery Networks (CDN)	NTT DATA assumes content delivery services will be available through the Cloud Carrier. We recommend that our clients contact bandwidth service providers for connectivity to our site and for CDN services.
	Litigation Hold	Varying retention periods and backup plans offered. Overall management of litigation hold responsibility of Client
Network	Virtual network	Offered
	Load balancer	Offered
	DNS	Offered

Service Category	Service Sub-Category	Comment
	Gateway (e.g. VPN or Application)	Offered
	Firewall	Offered
	Traffic manager	Offered
	Direct link	Offered. Client responsible for contracting with carrier
PC/Desktop DaaS		Offered through VMWare VDI
Security	Identity & Access Management	Management offered. Overall responsibility of client
	Encryption	Offered in motion and at rest. See our response to Question 8.8.
	Data Loss Prevention (DLP)	NTT DATA can support the client's DLP plan and requirements
	Web Security	Management offered. Overall responsibility of client
	Email Security	Management offered. Overall responsibility of client
	Network Security	Management offered. Overall responsibility of client
	Security Information and Event Management (SIEM)	Management offered. Overall responsibility of client
	Intrusion Management	Management offered. Overall responsibility of client
	DDOS Monitoring / Management	Management offered. Overall responsibility of client
Other (identify additional sub-categories and/or descriptors)	DR as a Service (DRaaS)	DR offered for VMWare-based production environments hosted elsewhere

*This exhibit summarizes the IaaS services NTT DATA provides.*

## 6.1.2 NIST Characteristics

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:

### 6.1.2.1 On-Demand Self-Service

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.

Our infrastructure and performance monitoring self-service portal will allow purchasing entities, if they wish, to unilaterally create and destroy virtual machines and associated storage and storage protection levels (such as backup or replication) without human intervention from NTT DATA. See the attached users manual for our cloud portal, named "3.6.3 Create a vApp with VMs v1.2". In addition to our cloud portal that is used for managing virtual instances, our Cloud Cruiser usage analytics portal (which we describe in more detail in our response to Question

8.1.2.5) can be used on a self-service basis to monitor manage business and technical capacity and resource metering in real time. Self-service is not available for Power 7-based AIX and iSeries cloud instances at the present time.

### 6.1.2.2 Broad Network Access

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.

#### Communications and Network Connectivity

Our datacenter's Internet connection IP services use blended bandwidth from three tier 1 carriers, with Border Gateway Protocol (BGP) and statically-routed options also available. These bandwidth services consistently exceed 99.9999 percent availability, which means our datacenter can provide highly reliable Internet connection services to datacenter customers with a wide variety of bandwidth requirements.

Exhibit 23. Supported Network Carriers

Carrier Connect	Colo Connect	Campus Connect	Internet Connect
<ul style="list-style-type: none"> <li>» Carrier neutral facility</li> <li>» Multiple diverse entrances</li> <li>» Freedom of choice</li> </ul>	<ul style="list-style-type: none"> <li>» Cage-to-cage cross dark fiber connectivity to other Northern Virginia data centers</li> <li>» Direct access to 200+ carriers in Northern Virginia</li> </ul>	<ul style="list-style-type: none"> <li>» Private, redundant 10G point-to-point connections</li> <li>» Level 3, XO Communications and Zayo</li> </ul>	<ul style="list-style-type: none"> <li>» Ethernet, private line, dark fiber and telephony service</li> <li>» Level 3, XO Communications, TW Telecom and Zayo</li> </ul>

UtahCloud1602

*The Ashburn datacenter we are offering in this proposal supports 17 network carriers as well as NTT. For the Purchasing Entities, this means a wide range of connectivity options.*

Our datacenter is carrier neutral. The center's Carrier Connect product provides access to a range of carriers, as shown above. The most common option for connectivity between our datacenter facilities and your network is multiprotocol label switching (MPLS), but other methods, such as dedicated circuits, can also be used. Bandwidth levels available include T1, T3, MPLS (up to 1 Gigabit), Metro Ethernet (up to 1 Gig) and IPsec Tunnel connected over the internet.

As pricing is complex and depends on customer's needs, we will be happy to discuss this subject with the Purchasing Entities, once bandwidth requirements are determined. Circuit redundancy to both Ashburn and Sacramento is usually provided by Internet VPN, but some clients implement direct connectivity

We support a variety of connectivity: T1, T3, Metro Ethernet, MPLS circuits can be installed and terminated in our Cloud environment. We can work with a variety of vendors to connect into the datacenter.



NTT DATA's fiber carrier entrances to the facility that are terminated on fully redundant SONET DWDM multiplexers, each with redundant power supplies, as well as redundant termination cards. Our datacenters include:

- Three diverse path fiber entrances into the datacenter for a complete expanded SONET ring
- Carrier neutral facility that provides a total of 16 redundant conduits for carrier entrance into the facility
- Fiber carrier entrances to the facility that are terminated on fully redundant SONET DWDM multiplexers, each with redundant power supplies, as well as redundant termination cards.

NTT DATA conducts routine maintenance according to a pre-determined schedule that is available well in advance of downtime and all equipment in our datacenters including communication systems, data network systems, compute and storage platforms are under maintenance contracts/ warranty with the original equipment manufacturer (OEM). We allow customers to bring in their own carriers. If the customer does so, the Service Operations Center will interface with the client's carrier to troubleshoot issues.

The data connections are secured via an IPsec VPN tunnel. If connections are going over a dedicated MPLS circuit, it will be encrypted in a VPN tunnel. This is also true for T1, T3, and other dedicated data circuits. We do not accept any unencrypted connection over the Internet; only IPsec or SSL VPN connections are accepted.

### 6.1.2.3 Resource Pooling

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.

Our IaaS offering is based on two technologies: the V+C+E architecture enabled by VMWare and the Power 7 Architecture implemented on IBM 770 and 780 equipment. Our V+C+E environment enables our customers to rapidly create (and destroy) Windows and Linux workloads from templates using our web portal. Our Power 7 environment enables our customers to work with us to rapidly create (and destroy) AIX and Linux workloads. We rely on EMC virtualized storage to provide a pool of allocatable storage. These compute and resource pools can be billed on a consumption basis so our customers are only billed for resources they actually consume.

Both of these architectures provide dynamic pools of compute and storage resources that can be intelligently provisioned and managed to address changing demands (through scalability). This empowers our customers to be nimble enough to pursue a fleeting business opportunity, or to deftly manage an administrative crisis.

### 6.1.2.4 Rapid Elasticity

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.

Customers can orchestrate the provisioning (or de-provisioning) of compute and storage resources in two ways:

- Customers can enter a Service Request for changes to their environment by entering a ticket in our BMC Remedy ticketing system. That request is reviewed as part of our Change Management process. Non-emergency changes are implemented within five days. This

process is recommended for changes to production environments and is required for environments under SLA.

- Our Infrastructure and Performance Monitoring portal allows you to create and destroy virtual machines and associated storage and storage protection level (backup, replication, etc.). See the attached user's manual for our cloud portal, named "3.6.3 Create a vApp with VMs v1.2". Logical network segmentation via firewall, if required as part of the change, must be created through the established cloud technical change process. That typically takes 5 days. In addition to our cloud portal that is used for managing virtual instances, our Cloud Cruiser usage analytics portal (which we will describe more in the next section) can be used to manage monitor and manage business and technical.
- All portals are customized to the client requested services and contractual SLA's. They are easy to use interfaces provided by BMC and EMC and customized by NTT DATA.

### 6.1.2.5 Measured Service

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

The NTT DATA Virtual Private Cloud is integrated with "Cloud Cruiser", a billing and metering package that permits an NTT DATA customer to track many statistics related to usage and capacity in real time through a web portal. This package continuously meters storage, processing, bandwidth and other cost drivers and enables the client to break these down to the department or even individual user level. The customer and NTT DATA thus have full transparency into those services being provided and consumed.

In addition to tracking usage, the NTT DATA VPC environment built around VMWare VCenter permits addition, modification and deletion of compute resources, storage and user accounts.

See the attachment named "6.5.1 Cloud Cruiser Overview.pdf" for a full description of Cloud Cruiser's capabilities.

### 6.1.3 Solution Subcategories

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.

NTT DATA will provide an IaaS offering. As the IaaS service model allows the consumer to deploy and run arbitrary software, this service model is undifferentiated as to service category (education, e-procurement, etc.).

### 6.1.4 Compliance with Attachments C and D

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

We certify that NTT DATA is willing to comply with the requirements of Attachment C and Attachment D. The applicability of our proposal is described throughout this response document.

### 6.1.5 Adherence to Services, Definitions, and Deployment Models

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**.

The ways NTT DATA adheres to the definitions identified in Attachment D are described in several places within our response. We have summarized them in this section.

- **Cloud Based Service Provider.** NTT DATA provides the computing infrastructure required for providing the cloud services described in our response to Question 8.23. Our client, the Cloud Consumers, can access this infrastructure through the broad network access described in our response to Question 8.1.2.2.
- **Categorization of Risk.** As a provider of IaaS services, NTT DATA makes available the tools that a cloud consumer may require to manage its data in accordance with the low, medium and high risk categories that the consumer has assigned. We address:
  - **Availability.** NTT DATA provides four tiers of availability protection ranging from best effort recovery from backups to 15 minute recovery from replicated data. Consumers can select the level of availability they require on a server-by-server basis. See our response to Question 8.8.1 in Section 6.8 (Service or Data Recovery) for a description of our data protection services.
  - **Confidentiality and integrity.** All data is physically protected from access to the data center, the colocation hall and the cage within the hall by physical access controls that include, among others, perimeter security, electronic and biometric access controls with associated review of physical access logs. Data is protected logically through logical access control and associated review of access logs. Data is segregated from access by other customers through methods that depend on the deployment method (see below for definitions). In a private cloud deployment, data is stored on separate storage frames within separated environments. In a community cloud environment, data is logically separated from other customers through enforced logical segregation. If a customer desires more granular separation of stored data (e.g. PCI data) within its own environment, NTT DATA provides tools to create those logical and/or physical separations.
- **Services and Models.** We described our alignment with the five essential NIST service characteristics in our response to Question 8.1.2. We will describe our alignment with the IaaS service model in our response to Question 8.23. We are not offering SaaS or PaaS services.
- **Deployment methods.** We offer several different deployment methods, including forms of:
  - **Public Cloud** – NTT DATA does not provide a public cloud that is described in the NIST Reference Architecture as being made available to the general public. We do provide self service capability so that our customers can unilaterally deploy or destroy resources.
  - **Private Cloud** – A private cloud is dedicated to a cloud consumer's exclusive use either on-site or outsourced. In an onsite model, NTT DATA works with clients (cloud consumers) to design physical cloud infrastructure located on premises. We manage the infrastructure remotely using either our or a client's tools. In an outsourced model, the physical infrastructure is located in our data center. (NTT DATA also manages cloud environments where clients have outsourced infrastructure to data center providers other than NTT DATA.)

- **Community Cloud** – A community cloud serves a group of cloud consumers with shared concerns such as performance, availability and security policy. Each consumer organization is separated from all others by properly configured LANs and SAN resources. NTT DATA's terminology for this is "virtual private cloud" (VPC) because to any single cloud consumer, their cloud appears to be private even though they share resources with other consumers. The "community" in this case consists of *Fortune* 500 corporations or non-federal government entities with a need for high availability and performance and stringent security requirements.
- **Hybrid Cloud** – A hybrid cloud is composed of two or more clouds that remain distinct entities, but are bound together by standard technologies—in NTT DATA's case, by VMWare or Power 7 technology. We are able to assist cloud consumers with advisory services to configure and manage their cloud environments and our Service Operations Center to provide RIM services wherever the cloud is situated.

## 6.2 Subcontractors (RFP §8.2)

### 6.2.1 Use of Subcontractors

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

NTT DATA plans to provide all services outlined in this agreement. The services we are offering will be provided by NTT DATA, Inc., or by our sister companies within the NTT Group.

NTT DATA, Inc. is a subsidiary of the NTT DATA Corporation, a publicly-held corporation. The NTT DATA Corporation, in turn, is part of the NTT Group. All services outlined in this response are to be provided by the personnel of NTT DATA, Inc., or the NTT Group, without subcontractors.

### 6.2.2 Extent of Subcontractor Use

8.2.2 Offeror must describe the extent to which you intend 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.

NTT DATA and the NTT Group companies plan to provide all services related to this agreement and the services outlined.

### 6.2.3 Qualifications of Subcontractors

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.

NTT DATA and the NTT Group companies plan to provide all services related to this agreement and the services outlined.

## 6.3 Working with Purchasing Entities (RFP §8.3)

### 6.3.1 Working with Purchasing Entities

8.3.1 Offeror must describe in detail 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 (refer to the persons/roles identified in Section 7 will be involved);
- Response times;
- Processes and timelines;
- Methods of communication and assistance; and
- Other information vital to understanding the service you provide.

#### Incident Management

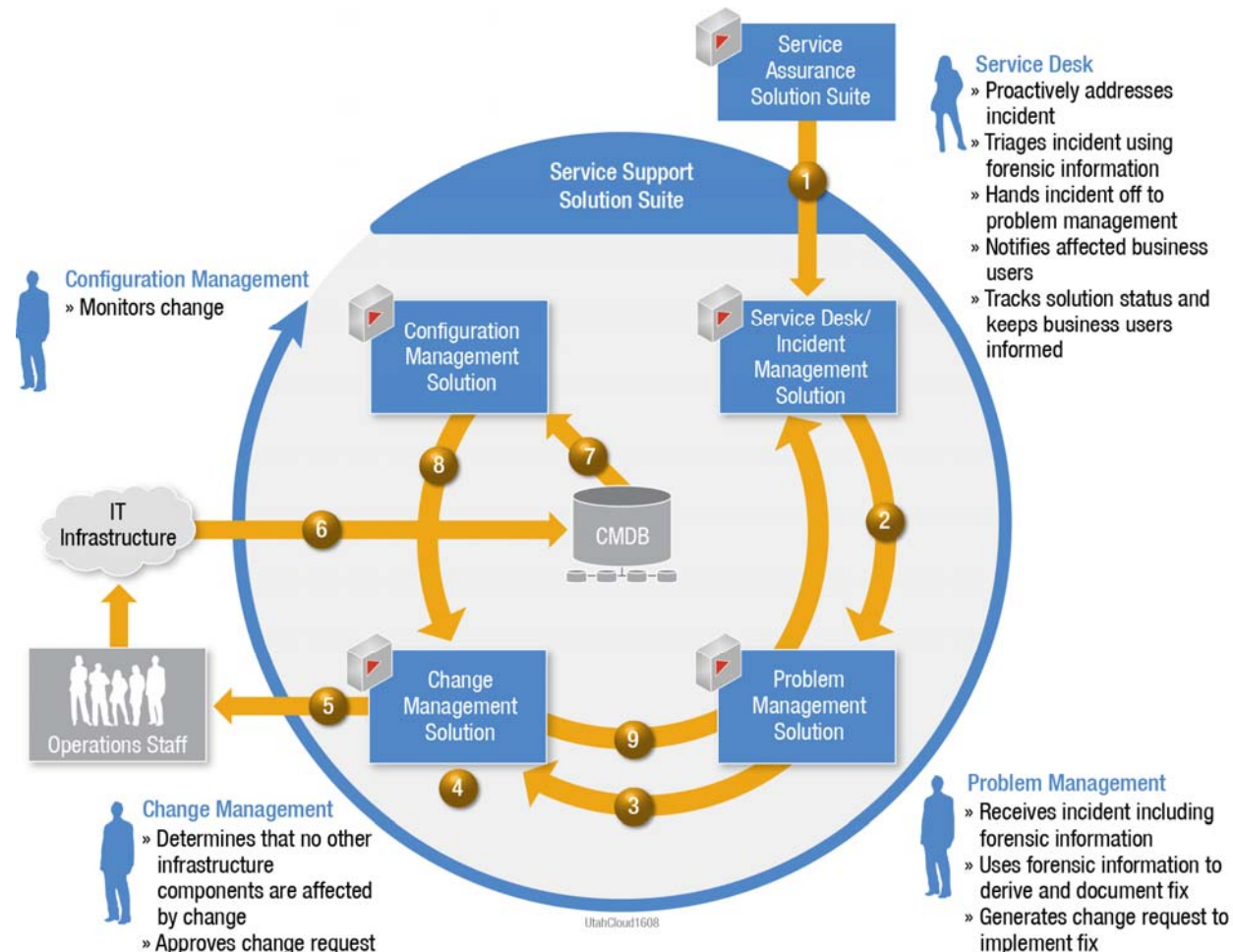
NTT DATA's Service Operations Center responds to data breaches, other security incidents, equipment alerts and other events. Therefore, if purchasing entities wish to understand how we will work with them during Data Breaches, they should first understand our overall approach to incident management. Data Breaches have special handling requirements, which we will discuss below, but the overall response process is similar for all incidents.

NTT DATA's response to Data Breaches generally follows our defined Incident Management process which is part of our overall support process with specific incident-related procedures defined below. We focus on support processes that allow seamless integration and provision of comprehensive alignment to our delivery services. NTT DATA opts for support processes based on the ITIL framework to ensure quality of service and continuous measurement and improvement of the IT service quality.

The following exhibits illustrate several important IT operations and process flows with supporting high-level procedures. The use case in the following Exhibit 24 illustrates the scenario of closed-loop, end-to-end processes. This scenario highlights tightly integrated service desk solutions, accessing a single change management database (CMDB), which acts to orchestrate and automate end-to-end processes in a closed-loop fashion. These processes are integrated across multiple groups.



## Exhibit 24. IT Operations Management



*In this use case scenario, the service assurance solution alerts the service desk support solution suite to a server performance slowdown beyond the limit allowed by the associated SLA.*

The integration of the purchasing entity, the NTT DATA team and any third-party service provider components ensures best practice interaction, collaboration, and successful completion of service delivery and operations.

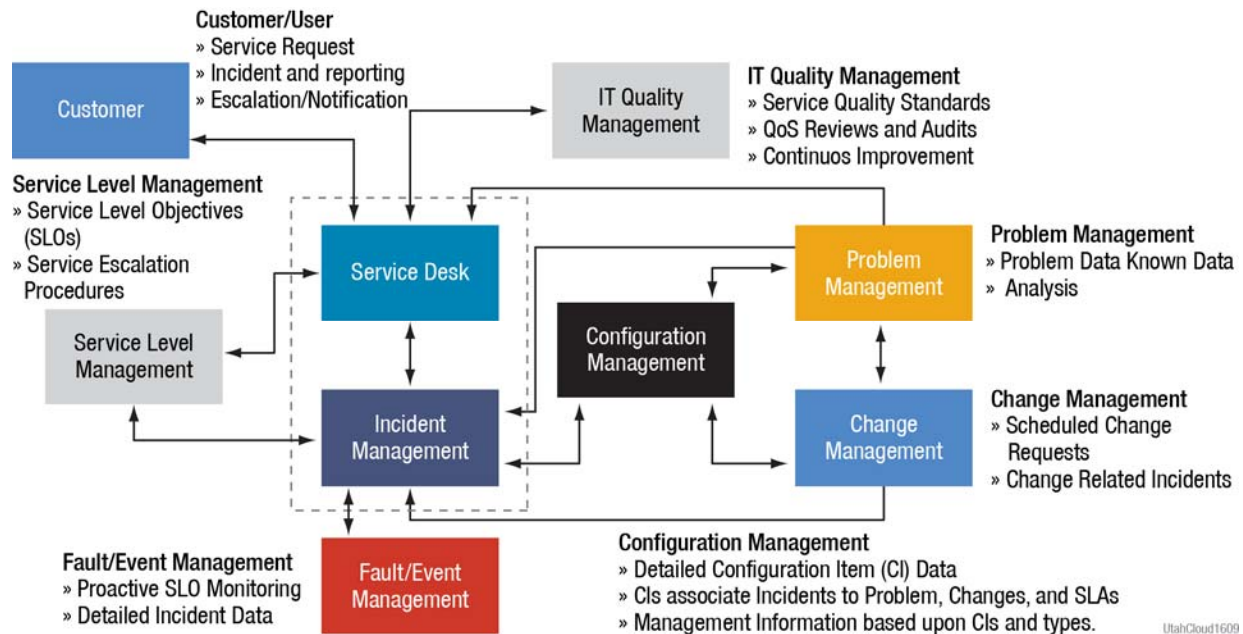
- The ITSM suite, which includes security incident monitoring agents, automatically generates an incident ticket in the service desk solution; the incident ticket will include forensic information.
- The service desk agent opens the incident in the service desk solution using the forensic information, triages the problem, and sends it to the right problem management technician. The service desk solution will then forward the incident to the problem management solution and tracks the incident status.
- The problem management technician uses the forensic information to derive a fix, which requires replacement of the problem server with a higher-capacity server. From the problem management solution, the technician generates a change request to implement the fix. The

problem management solution forwards the change request to the change management solution.

- The change management technician consults the infrastructure view provided by the CMDB and sees that the requested change does not affect any other infrastructure components; then the technician approves the request. In response, the change management solution automatically gathers any other required approvals.
- The change management solution then forwards the approved request to the operations staff for implementation and tracks change progress. The operations staffs make the requested change.
- The auto-discovery feature of the CMDB updates it with the new server configuration.
- Through the CMDB, the change management solution validates ensures that the change does not violate standard configuration.
- The change management solution then closes the change request in the change management solution.
- The change management solution closes the associated incident in the Service Desk solution, closing the loop.

If no one in the process flow accepts the appropriate assignment within the time period in the appropriate SLA, the assignment will be automatically escalated to the lead for the group; and escalations will continue, as necessary until the assignment is accepted. Exhibit 25 depicts our Operations Management flow.

Exhibit 25. Operations Management Flow



*NTT DATA's operation management is responsible for the day to day operations and management of IT infrastructure. Operations management works through or closely with the service desk and provides the Purchasing Entity and its clients with a single point of contact for all the service requests and incidents*

## Incident Management

NTT DATA uses BMC Remedy, which is a service management and ticketing tool for incident management in our environment. Remedy is configured to manage both the auto tickets created by the tools and the one created by the users or on behalf of the users.

Remedy has features that enable service desk agents to identify any new tickets, through screen popups. All service desk agents monitor the Remedy screen continually. Once a new ticket popup appears, the service desk agent selects the ticket and starts working on the same.

The incident management activities performed by the service desk include these activities:

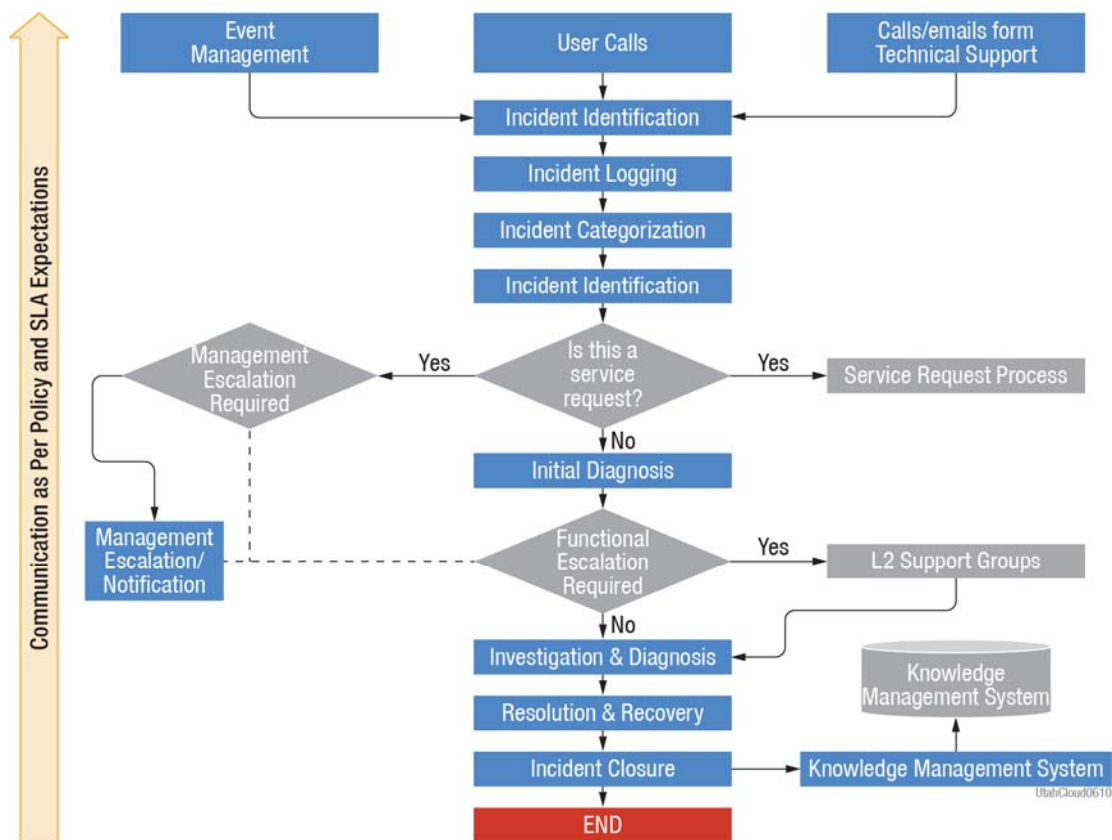
- Record incident and assign the incident/ticket ID to the end user
- Classify the incident, according to a predefined set of category standards
- Prioritize the incident, according to standard priority/severity definitions
- Provide initial investigation and diagnosis
- Provide initial support – problem isolation and troubleshooting
- Incident ownership, monitoring, and closure for incidents for which the resolution is known and the solution documented
- Triage incident to the appropriate resolver group based on the incident classification

For critical incidents after the incident is triaged on Remedy, the Service Desk agent also calls the resolver group to inform them of the newly triaged ticket. If the resolver group is not available on phone, an email is sent to the resolver group's email id, informing of the newly triaged ticket. The service desk also:

- Provides regular coordination with all resolver groups including third parties to ensure on-time and within-SLA closure of the incidents, regardless of the cause of the incident/problem
- Allows incident tracking and end-user communication with respect to the current status of the incident and resolution
- Maintains and records an audit trail of all the transactions and communications between the end user, Service desk, site support, and any third parties involved in problem resolution
- Sees to it that the end user is satisfied with the solution provided and the incident is closed only after the consensus of the end user



Exhibit 26. Incident Management Process



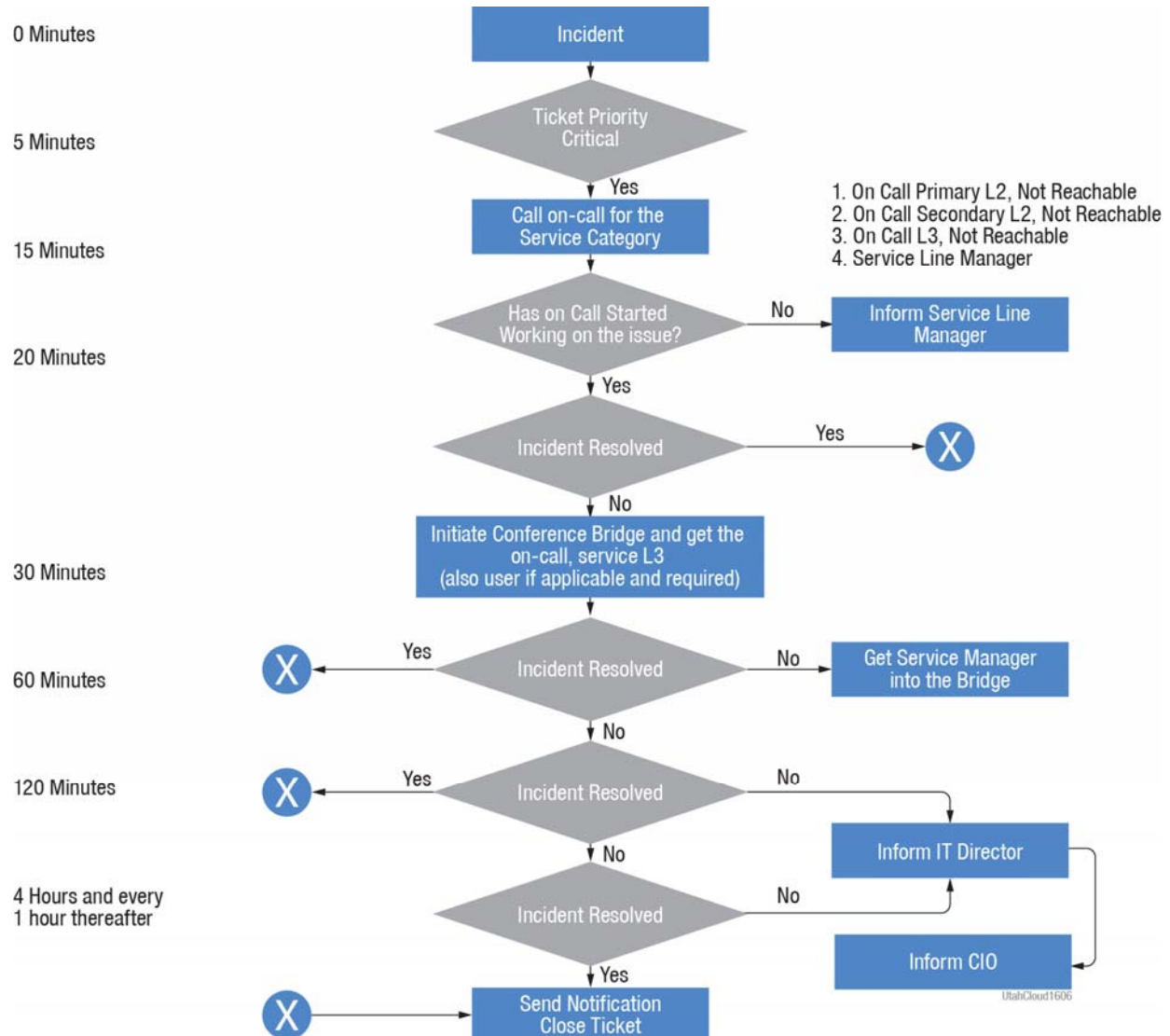
*Our incident management is used to provide value to business operations, align organizations' ability to detect and resolve incidents, align IT activity to real-time business priorities, and identify potential improvements to services.*

### Critical Incident Management

For high-impact critical incidents, which include security intrusions and Data breaches, the service desk team initiates a conference bridge between all the stakeholders (from both the client's end and the resolver group's end), to allow the technical and subject matter experts to coordinate directly on the conference bridge and arrive at the next steps, which will allow incident isolation and resolution at the earliest.

Exhibit 27 provides an example of the process flow which will be finalized and base-lined during discussions with the purchasing entity during the transition phase. This process requires buy-in from all the resolver groups, and we assume the purchasing entity will take care of getting all the required buy-ins under their control.

## Exhibit 27. Critical Incident Management Process Flow



*NTT DATA's standard incident management approach is a set of processes to restore normal service operation as quickly as possible and minimize adverse impact on business operations within SLA limits. Depending on the severity of the issue, and agreement with our client on certain SLA and escalation processes, we engage our delivery manager or our contract manager, depending on prior agreement and the criticality of the incident.*

### Incident Reporting

NTT DATA uses interactive mechanisms and generates management reports to monitor and report the engagement performance. On a weekly, monthly, and quarterly basis, these reports are generated with accurate and updated measurement and monitored data.

At a minimum, NTT DATA generates the following reports on incident management:

- Total incidents by category, location, and priority
- The number of incidents not closed or resolved with workarounds

- The first-call resolution rate
- The number of incidents closed
- The number of incidents reopened (repeat incidents)
- The number of incidents missing the SLA for response
- The number of incidents missing the SLA for closure
- Response time statistics by resolver group
- Top ticket categories
- Top ticket volume locations

All required reports, formats, and frequencies will be discussed and agreed with the purchasing entity during the transition phase and will be implemented during ongoing support.

### **Response to Security Incidents**

NTT DATA has a documented response program with policies and procedures to address privacy incidents, unauthorized disclosure, access or breach of client confidential information. We follow our internal Intrusion reporting procedures that outline steps taken to isolate and block the potential breach or intrusion.

The threat detection database is updated daily with the latest threat signatures, so the newest threats are detected. All received alerts are logged and the IPS also captures all the detected packets which can be used for further investigation into traffic patterns.

The IPS is configured to alert based on the severity of detected threats. Once the alert is received, initial triage is performed, and depending on the severity of the threat, the customer is notified. The client CIO on file and the escalation team will be notified of all high priority security events within four hours after the incident occurs.

All lower priority events will be assessed and notification will be sent out to the client CIO on file and escalation team within 1 business day of the incident.

Our security breach response is the process and action we take in response to a security incident to protect ourselves, our customers and partner's if/when a security incident occurs. This includes:

- Receiving, reviewing and responding to a security breaches
- Working with the customer to understand the incident
- Preparing and planning for handling the incident
- Setting clear priorities
- Executing a response to the incident
- Finding and correcting the root cause of the incident
- Determining of the implications of past incidents
- Recording and preserving the analysis of past incidents and learned lessons
- Reviewing and appropriately updating the policy at least once every 6 months or as changes in policies, procedures, or technology occur.

Incidents of any major category—which would include a major facility incident, major network incident, security incident, data breach or client specific incident—are classified as a “Priority 0”

and addressed by representatives from each department including department heads, directors, and executive management. This core team is empowered to execute on every aspect of remediation and coordinates all activity through an open bridge line allowing fully and clear communication among all parties.

The specific makeup of the core team is determined during discussion between NTT DATA and the purchasing entity during the transition period and would at least the following participants:

- The **client manager**, who manages the business relationship between NTT DATA and the purchasing entity.
- **The delivery manager**, who manages the day-to-day delivery of services to the purchasing entity.
- **Individual SMEs** who possess domain-specific knowledge, notably the **security manager**.

In addition, **executive sponsors** may become involved as required by unfolding events.

Details of our escalation process are contained in our response to Question 8.4.

### 6.3.2 Unauthorized Marketing

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.

NTT DATA certifies that it shall not engage in nor permit its agents to push adware, software, or marketing not explicitly authorized by the purchasing entity or the master agreement.

### 6.3.3 User Test/Staging Environment

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

NTT DATA certifies that its application-hosting environments also support a user testing/staging environment that is identical to production. As an IaaS provider, NTT DATA provides the tools and advice to implement testing, development, and staging environments, the actual design of which is the responsibility of the purchasing entity.

### 6.3.4 Accessibility for People with Disabilities

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

NTT DATA certifies that computer applications and web sites will be accessible to people with disabilities, and will comply with participating entity accessibility policies and the Americans with Disability Act, as applicable.

### 6.3.5 Browser Platforms

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

NTT DATA certifies that its applications and content delivered through web browsers will be accessible using current released versions of multiple browser platforms (such as Internet Explorer, Firefox, Chrome, and Safari at a minimum).

### 6.3.6 Storage of Sensitive or Personal Information

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.

We certify that NTT DATA will, prior to the execution of a service level agreement, meet with the purchasing entity in question and cooperate and hold a meeting to determine whether any sensitive or personal information will be stored or used in the Service that is subject to any law, rule or regulation providing for specific compliance obligations.

NTT DATA employees will meet with officials of the purchasing entity as part of the transition process we will describe in Section 6.10 (Service Level Agreements) to review information that may be sensitive, confidential or subject to any law, rule, or regulation. Any issues arising from this review will be discussed and mitigated as part of system design and deployment.

### 6.3.7 Project Schedule Plans and Work Plans

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.

#### Proposed Migration/Relocation Approach

The level of effort and hence timeline for developing, testing and implementing solutions for customers depends on the size and complexity of the infrastructure and associated planning that must be developed so that the purchasing entity's existing assets can be migrated into the new environment. The following summarizes our approach to migrating assets into our IaaS cloud; further detail can be found in Appendix 2 (Details of Migration Methodology). The discussion below also covers physical equipment that may be collocated within the NTT DATA center to support the purchasing entities IaaS environment. Most complex environments contain infrastructure such as appliances or legacy systems that are incompatible with an IaaS cloud and therefore must be implemented as collocated physical instances. Our migration methodology is designed to handle complex, worst case, situations.

NTT DATA follows a five-phased approach for migration projects with emphasis on early results leveraging our experience and knowledge to guide the direction of an IaaS project. This proprietary methodology allows us to improve the effectiveness of the engagements by reducing the risk of schedule delays and resulting cost impacts while meeting the objectives of the project. This approach assumes the cooperation and support of the purchasing entity, who is the current holder of information about and requirements for the existing environment.

We use this methodology to leverage the collective experience and materials from prior engagements including deliverable templates, and best practices. The primary steps of an IaaS migration or relocation solution are summarized in Exhibit 28.

## Exhibit 28. Data Center Services Phases

Plan	Design	Build	Deploy	Operate
<ul style="list-style-type: none"> <li>» Project Initiation</li> <li>» Current State Assessment</li> <li>» Requirement Verification</li> <li>» Target State Recommendations</li> <li>» Migration/Virtualization Strategy</li> </ul>	<ul style="list-style-type: none"> <li>» Final Engineering and Application Migration Assessment</li> <li>» Specification and Procurement (if required)</li> </ul>	<ul style="list-style-type: none"> <li>» Procurement</li> <li>» Installation &amp; Configuration</li> <li>» Integration Testing</li> <li>» Migration</li> </ul>	<ul style="list-style-type: none"> <li>» Testing and Ops Transition</li> <li>» Final Production Cut-over</li> <li>» Final Sign-off</li> </ul>	<ul style="list-style-type: none"> <li>» Ongoing Operations</li> <li>» Stabilization</li> <li>» Optimization</li> </ul>

UtahCloud1629

*This exhibit shows the standard phases of data center service delivery.*

The standard phases are:

- **Plan** – Project Initiation, Current State Assessment, Requirement Verification, Target State Recommendations; and Migration/Virtualization Strategy
- **Design** – Final Engineering and Application Migration Assessment, Specification and Procurement (if required)
- **Build** – Procurement, Installation & Configuration, Integration Testing, and Migration
- **Deploy** – Testing and Ops Transition, Final Production Cut-over, and Final Sign-off
- **Operate** – Ongoing Operations: Stabilization and Optimization

NTT DATA's methodology comprises work streams to provide a multi-team approach for this co-location and managed services project. The lifecycle work streams address specific competencies while providing overall integration across the full engagement lifecycle.

### Project Team Tracks

The workstreams span four domains: project management, infrastructure, data center facilities and logistics, and applications.

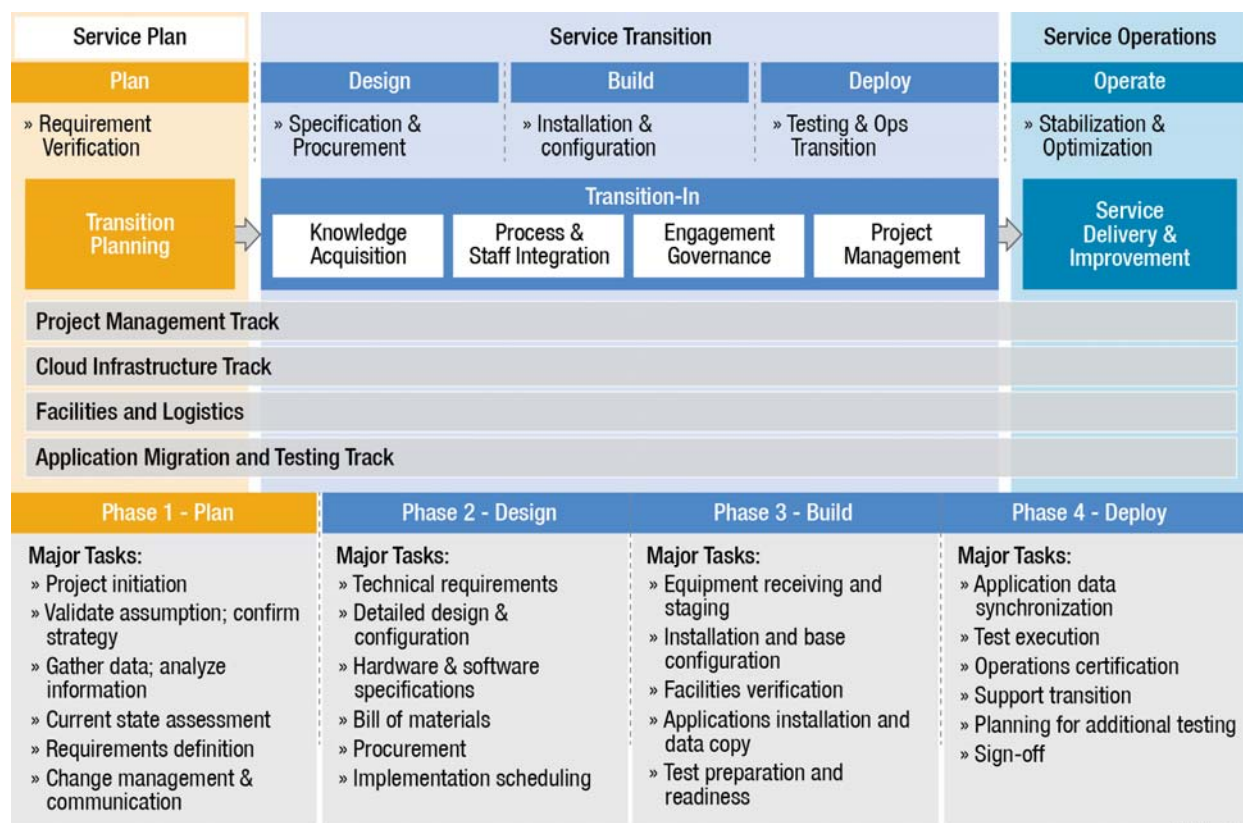
- The **Project Management Track** will provide overall day-to-day management support for the co-location and managed services project, through the PMO, with a specific focus on project planning, project control (work scope, schedule and budget), quality assurance, change management, risk mitigation and project communication.
- The **Infrastructure Track** will focus on the technology infrastructure design and implementation of physical and virtual components required to implement the co-location and managed services project. The planning and design will be based on the architectural principles and overall design guidelines.
- The **Facilities and Logistics Track** will focus on the physical characteristics of the buildings, data centers, computer rooms and wiring closets, along with the types of cables, and wiring structure used in those same sites. Logistics assistance will comprise providing coordination and management of the shipping, receiving, verification, coordinating, tracking, installation coordination, operations readiness, and proper dispensation of all physical assets that are purchased for installation into the NTT DATA's co-location data centers. This track is only required if collocated physical assets are required to support IaaS cloud services.
- The **Application Migration and Testing Track** will drive the planning, analysis, design, and implementation migration materials required to implement the applications systems,



configuration settings and application data from pre-production and production environments.

Exhibit 29 shows the major tasks associated with NTT DATA's data center migration and relocation services.

Exhibit 29. Data Center Migration and Relocation Services – Major Tasks



UtahCloud1628

*This exhibit summarizes the major tasks associated with NTT DATA's data center migration and relocation services.*

### Wave Migration Strategy

The first stage waves of migration are based on swinging virtual-to-virtual (v2v) migrations estimated with the purchasing entity physical and virtual inventory and how it is configured.

Second stage waves will include V2V and Physical-to-Virtual migrations. Applications with dependencies on physical and virtual servers will be moved during these waves.

Final stage waves will be reserved for physical server migrations, if required, with special requirements or legacy hardware.

Exhibit 30. NTT DATA Migration Solution – Major Waves

Migration Type	Description
Virtual-to-Virtual (V2V) Swing Migration	Virtual machines in the purchasing entity's data center will be virtually migrated to systems in the NTT DATA data center. If collocated physical equipment is required, following the migration, physical equipment in the purchasing entity's data centers will be shipped to

Migration Type	Description
	the NTT DATA data center and reused.
Physical-to-Virtual (P2V) Swing Migration	Physical Machines in the purchasing entity's data center will be converted to virtual machines and migrated to systems in the NTT DATA data center. If collocated physical equipment is required, following the migration, equipment in the purchasing entity's data center will be shipped to the NTT DATA data center and reused.
Physical-to-Physical (P2P) Swing Migration	Physical servers will be built in the NTT DATA data center to replace physical servers in the purchasing entity's data center. Data will be replicated and synchronized between servers for the migration. If collocated physical equipment is required, following the migration, equipment in the purchasing entity's data center will be shipped to the NTT DATA data center and reused.
Lift and Ship Migration (L&S)	If collocated physical equipment is required on a "lift and shift" basis, physical servers will be shut down in the purchasing entity's data center and shipped to the NTT DATA data center. Servers will be reconfigured for the new network environment and brought back on-line.

*This table summarizes the major waves of NTT DATA's migration solution.*

To optimize the migration process, NTT DATA recommends that various teams within the migration tracks focus on individual sets of repeatable processes to develop specialization skills for their function. This results in the creation of a "factory assembly line" migration process that will expedite the timeline.

### Wave Migration Assumptions

- The makeup and server count for each wave will be identified during the planning and design phases of the project.
- If physical equipment is required, the purchasing entity will purchase capital assets to support the first migration wave and to replace any assets decommissioned after migration.
- Migration type will be determined during the design phase of the project. Migration type will be selected to reduce risk and minimize any required outage.
- The structure of the migration waves may changes as NTT DATA gains more insight into The purchasing entity's application dependencies.
- Migration waves will be executed in parallel with two dedicated migration teams supported by a shared pool of administrators.

As mentioned above, the length of time needed for migration from planning through test and validation is heavily dependent on the size and complexity of the environment as well as other factors such as technology freeze periods. The overall timeline can range from a several weeks to over a year. In our experience, an environment with a few hundred servers and a dozen Terabytes of storage can usually be migrated in about three months.

## 6.4 Customer Service (RFP §8.4)

### 6.4.1 Excellence in Customer Service

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



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

NTT DATA has decades of experience in managing infrastructure and developing associated support processes. We offer:

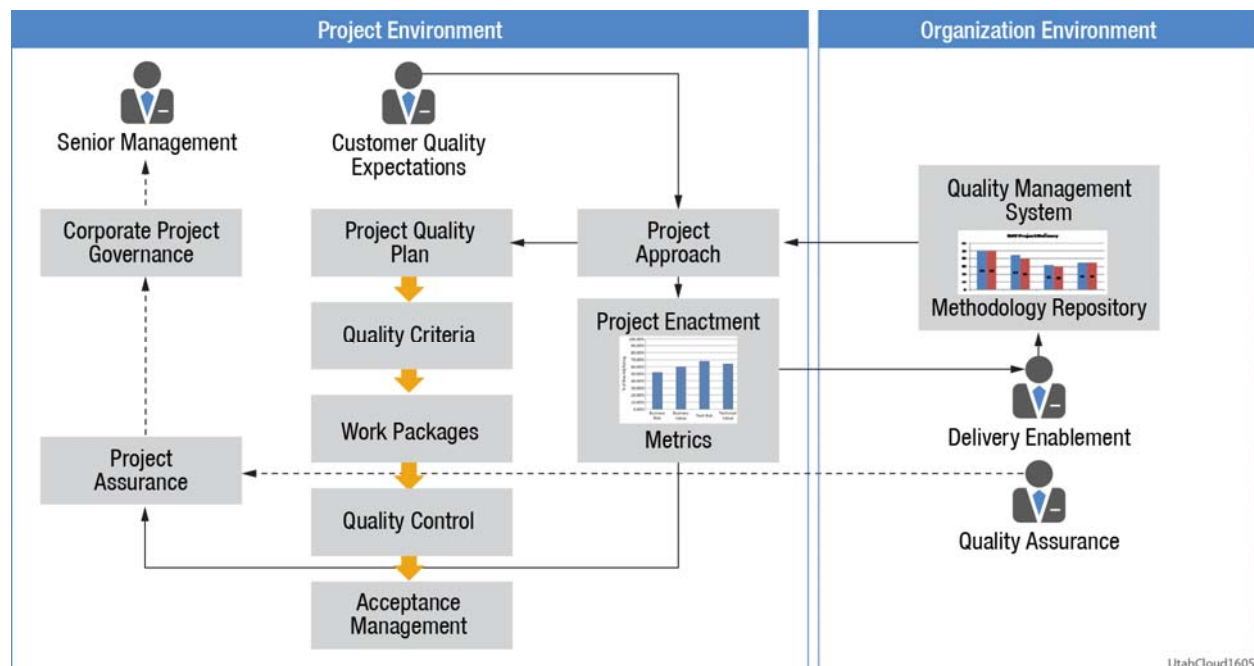
- An overall approach to quality management, including problem management process that is based on our ITIL framework. Our problem management process is focused on identifying the root cause of single or recurring issues and developing mitigation strategies.
- An engagement governance structure that monitors engagement progress, identifies and addresses problems, and provides an escalation path for complaints.
- An approach to SLA management, which we will describe in more detail in Section 6.10 (Service Level Agreements).

### 6.4.1.1 Quality Assurance Measures

#### Overview

NTT DATA's quality management approach focuses on effective business outcomes by incorporating continuous improvements driven by objective metrics. NTT DATA leverages and continuously improves/adapts leading industry standards and maintains effective project insight and control. At NTT DATA, project methodologies are tailored to meet the client's specific environment and project needs. Through this, we define a software quality plan to facilitate fulfillment of the project's quality requirements and expectations. Exhibit 31 shows the key components of the approach.

Exhibit 31. NTT DATA's Quality Management Approach



*This exhibit summarizes NTT DATA's quality management approach.*

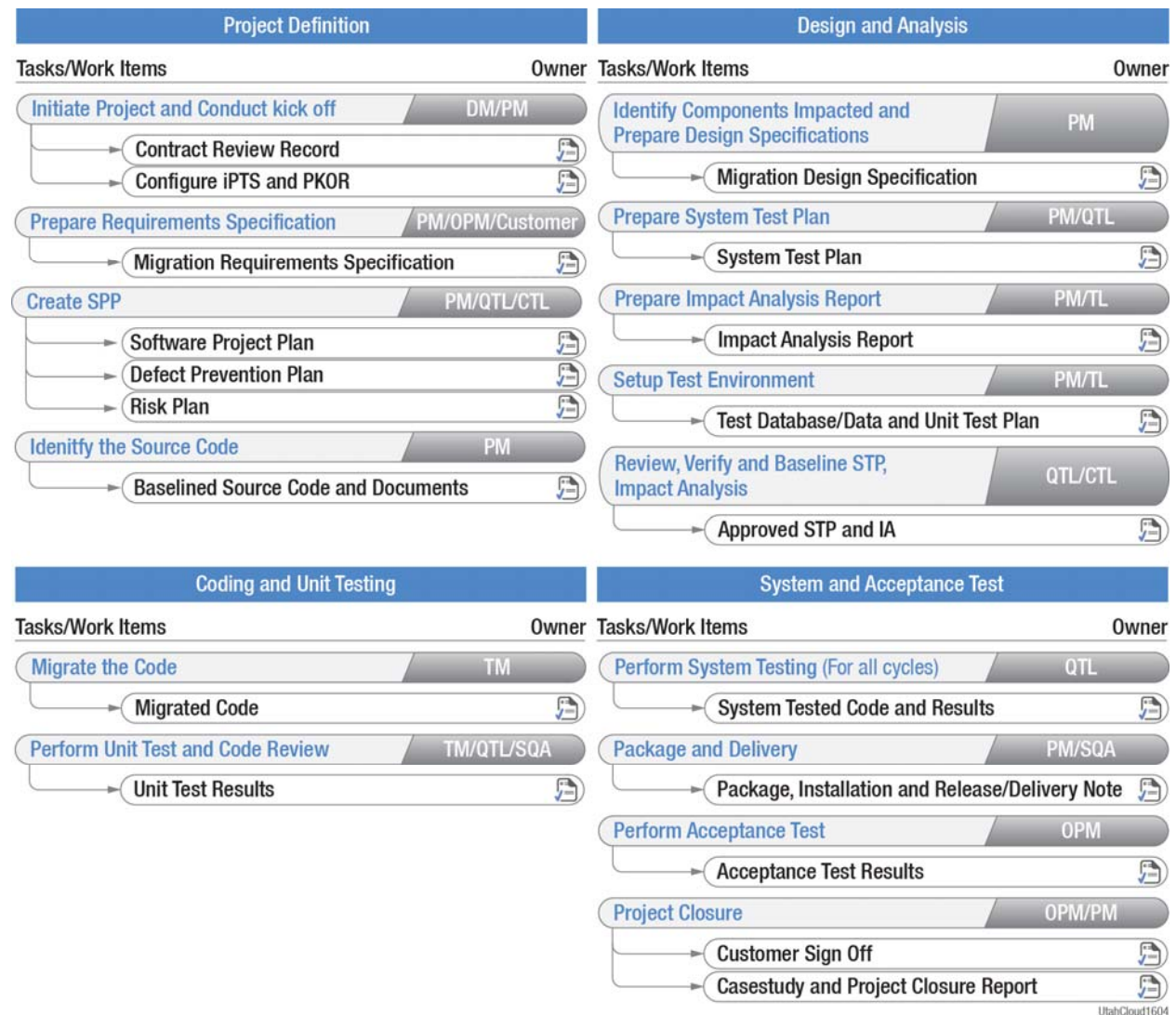
## NTT DATA's Quality Assurance Process

NTT DATA's deliverables undergo a three-level quality assurance process. NTT DATA has in-house tools for aiding the quality review and a dedicated Software Quality Assurance (SQA) group to govern the quality assurance (QA) process. Tools are available for tracking of the projects for the entire duration of the life cycle.

A Process Management Group (PMG) and the SQA ensure quality at the organization and account level, whereas the delivery, testing, and training groups contribute towards quality at the account and individual resource level. A representative from the senior management is the quality sponsor for the organization and is responsible for driving quality programs at the organization, account, and individual resource level.

Exhibit 32 depicts NTT DATA's continuous approach to assure quality in its migration service delivery.

Exhibit 32. NTT DATA's Migration QA Framework



*This exhibit summarizes our migration quality assurance framework.*

The continuous improvement programs ensure that processes and quality standards are constantly enhanced based on collective experience gained from executing client engagements across the organization. Highlights of various groups that are a part of the NTT DATA's quality system are described herein.

NTT DATA's quality system comprises the delivery organization, collaborating with numerous groups within the organization including the Process Management Group (PMG), the SQA group, testing groups, and training groups for promoting quality in client deliverables:

- **PMG** – PMG is the corporate body responsible for:
  - Establishing and institutionalizing process, standards, and metrics across the organization
  - Identifying process models for project execution
  - Identifying and analyzing metrics that are applicable to the project
  - Conducting audits and verifying process compliance. In-house tool available for tracking of the audit findings to closure
  - Identifying and spearheading new process initiatives and certifications programs (such as ISO 20000)
  - Driving renewal, re-certification and periodic assessments conducted by external auditors
  - Project closure including project post-mortem analysis and lessons learned.
- **Quality Assurance and Testing (QAT)** – QAT is an independent corporate group that provides test planning and implementation, test automation, testing execution to various ongoing client engagements. In addition, QAT provides independent testing services for development projects undertaken by other vendor partners of our clients.
- **Delivery Organization** – Our delivery organization leverages institutional frameworks throughout NTT DATA (for example, PMG, SQA, testing, and training) in providing services to our clients. This ensures quality of deliverables at NTT DATA accounts. Our Delivery Managers and Project Managers play a key role in ensuring quality in client deliverables as well as strict adherence to processes and quality standards during the project lifecycle.
- **Training Group** –To promote quality at the individual resource level, employees undergo training programs and workshops in addition to on-the-job training on processes, quality standards, and frameworks. Our employees are required to be trained on sharp, Information Security and Quality (ISQ) in addition to quality standards and procedures. Individuals also undergo training on various aspects of project initiation, tracking, configuration management, and metrics.

### Common Quality Management Methods

Some commonly used quality management methods include:

- **Technical Review Board** – This board includes the engagement team members representing various roles, and is tasked with identifying, prioritizing, documenting, and implementing improvements to NTT DATA's processes and supporting tools. The technical review board is often active during the early stages of an engagement when processes are newly established and more opportunities are available to eliminate waste and optimize performance.

- **Engagement Audits and Reviews** – There are types of reviews or audits conducted by resources external to the engagement, but internal to NTT DATA that can be performed to assess the team performance and recommend actions for improvement. These include periodic audits conducted by NTT DATA's SQA group. Operational reviews of engagement performance, and how the team is progressing and working to bring additional value to client, are also conducted periodically with NTT DATA management.
- **Peer Reviews** – Peer reviews, which we also sometimes refer to as documentation reviews, is a highly effective quality technique that is performed by team members at different points during project execution to help ensure high-quality work products and requirements traceability.
- **Defect Tracking and Root Cause Analysis** – Testing is used to identify and correct defects as early in the process as possible. Defect tracking is used to record defects and track them through to resolution as well as to capture data for statistical analysis. Statistical analysis may be performed to identify trends such as the most frequent types of defects and to establish action plans to reduce or eliminate them. Within this category is root cause analysis, which is a problem solving method aimed at identifying and eliminating the root causes of recurring problems or events, as opposed to just addressing the symptoms. By driving out recurring problems, the NTT DATA team is able to focus its attention on more value-added activities and as a result increase its overall productivity.
- **Product and Operational Improvement** – NTT DATA teams bring innovative ideas to help improve both its performance and the client's performance. Identifying and implementing approved product and operational improvements is a way to demonstrate the value and commitment that NTT DATA will bring to its client. To enable this, the NTT DATA team establishes a process to collect, gain approval for, track, and report progress on these improvements.
- **Customer Satisfaction Surveys** – Our performance is evaluated by the customers we serve. As such, NTT DATA periodically conducts customer satisfaction interviews and/or surveys to understand its customers' perception of the service performance. In addition, our clients often perform their own analysis of vendor performance.

During due diligence and transition, NTT DATA's management teams will work with purchasing entities to assess the current processes in place, compare and contrast with those of NTT DATA, and determine an appropriate best-of-breed mix of the quality processes and activities that are warranted for the requirement.

### Problem Management

NTT DATA's standard problem management approach is a set of processes used to identify the unknown cause(s) of one or more incidents and eliminate recurring Incidents. NTT DATA's problem management process defines the different activities that should be executed throughout the lifecycle to ensure that problems are managed effectively, and results in minimizing incident occurrences related to the affected service/infrastructure. The following are key activities within NTT DATA's problem management process:

- Problem identification and registration
- Problem classification
- Investigation and diagnosis
- Error identification and recording
- Error assessment and resolution

- Error closure
- The process also identifies continuous monitoring of problems
- Status of currently active problems
- Communication of problems status to related stakeholders
- Improvement in services/infrastructure/process by fixing root cause of problems
- Continuous improvement of the problem management processes

Root cause analysis (RCA) is a fundamental component of problem management and part of NTT DATA's managed service culture, focused on identifying and fixing the underlying causes of issues rather than only addressing the symptoms on the surface. By focusing remediation on root cause, NTT DATA seeks to minimize the probability that the issue will recur. RCA is considered an iterative process and part of an overall continuous improvement and TCO reduction approach.

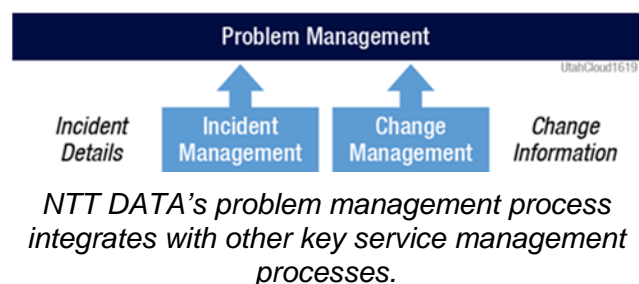
There are numerous useful issues solving techniques that can be used to help diagnose and resolve problems. NTT DATA recommends use of the following techniques as appropriate case-by-case basis.

- **Chronological Analysis** – When dealing with a difficult problem, there is often inadequate information about exactly what has happened and when. In such cases, it is helpful to document all events briefly in chronological order – to provide a timeline of events. This often makes it possible to see which events may have been triggered by others, or to discount any claims.
- **Brainstorming** – It can often be valuable to gather together the relevant people, either physically or by electronic means, and to 'brainstorm' the problem – with people throwing in ideas on what the potential cause may be and potential actions to resolve the problem. The problem manager documents the outcome and any agreed actions and keeps a degree of control in the session(s).
- **Ishikawa Diagrams** – A method of documenting causes and effects that can be useful in identifying a root cause. Such a diagram is typically the outcome of a brainstorming session where problem solvers can offer suggestions. The main goal is represented by the trunk of the diagram, and primary factors are represented as branches. Secondary factors are then added as stems.
- **Pareto Analysis** – This is a technique for separating important potential causes from trivial issues.

NTT DATA classifies problem management into two categories:

- **Avoidance (proactive) Management** – This process deals with proactively identifying potential problems that have not occurred to date but can occur in the future. While remedy management is more of a reactive approach, avoidance management is proactive in nature. The main approach to identify, analyze, and mitigate these kinds of problems is based on the fact that a similar type of

Exhibit 33. Integration Between Problem Management and Other Service Management Processes



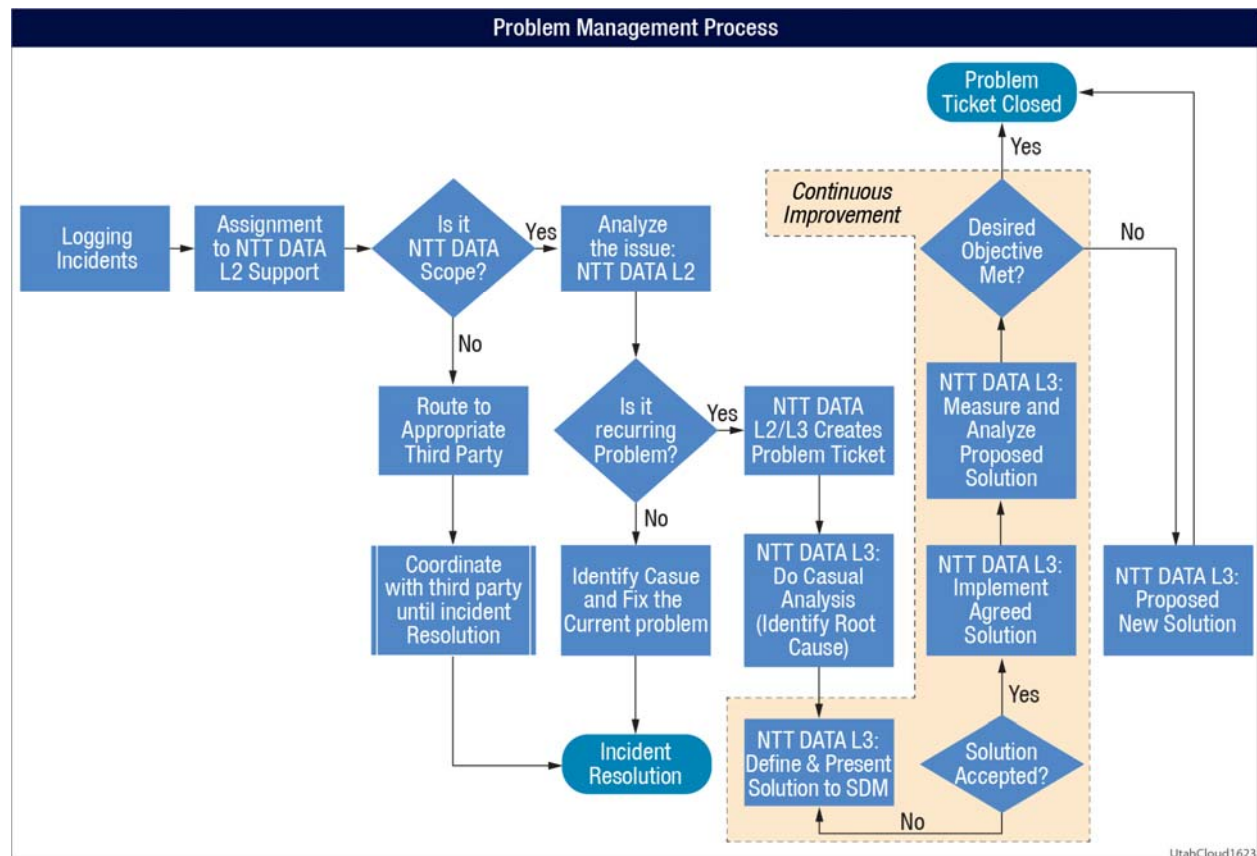


incident occurred in the past and has a similar type of root cause but not the exact one.

- **Remedy (reactive) Management** – This process deals with identifying high-occurrence incidents and addressing the causal analysis for the occurrence of such incidents. After identifying the root cause of such occurrences, corrective actions are implemented to eliminate these problems from repeating in future. This approach is based on the widely acclaimed Pareto Rule (80-20 Rule), which states that 80 percent of the problems are due to 20 percent of the causes.

NTT DATA's problem management process is summarized in Exhibit 34.

Exhibit 34. NTT DATA's Problem Management Process



*This exhibit summarizes NTT DATA's problem management process.*

#### 6.4.1.2 Escalation

##### Overview

For all engagements, NTT DATA implements a tiered engagement model designed to discuss and examine progress and issues at the appropriate frequency and level of authority throughout the duration of the engagement. Managerial guidance flows downward in this structure, while customer complaints and other issues flow up. Key roles within this structure on the NTT DATA side include the delivery manager (responsible for day-to-day operational matters) and the client manager (responsible for the business relationship). These roles will be matched by equivalent project managers and steering committees on the purchasing entity side.

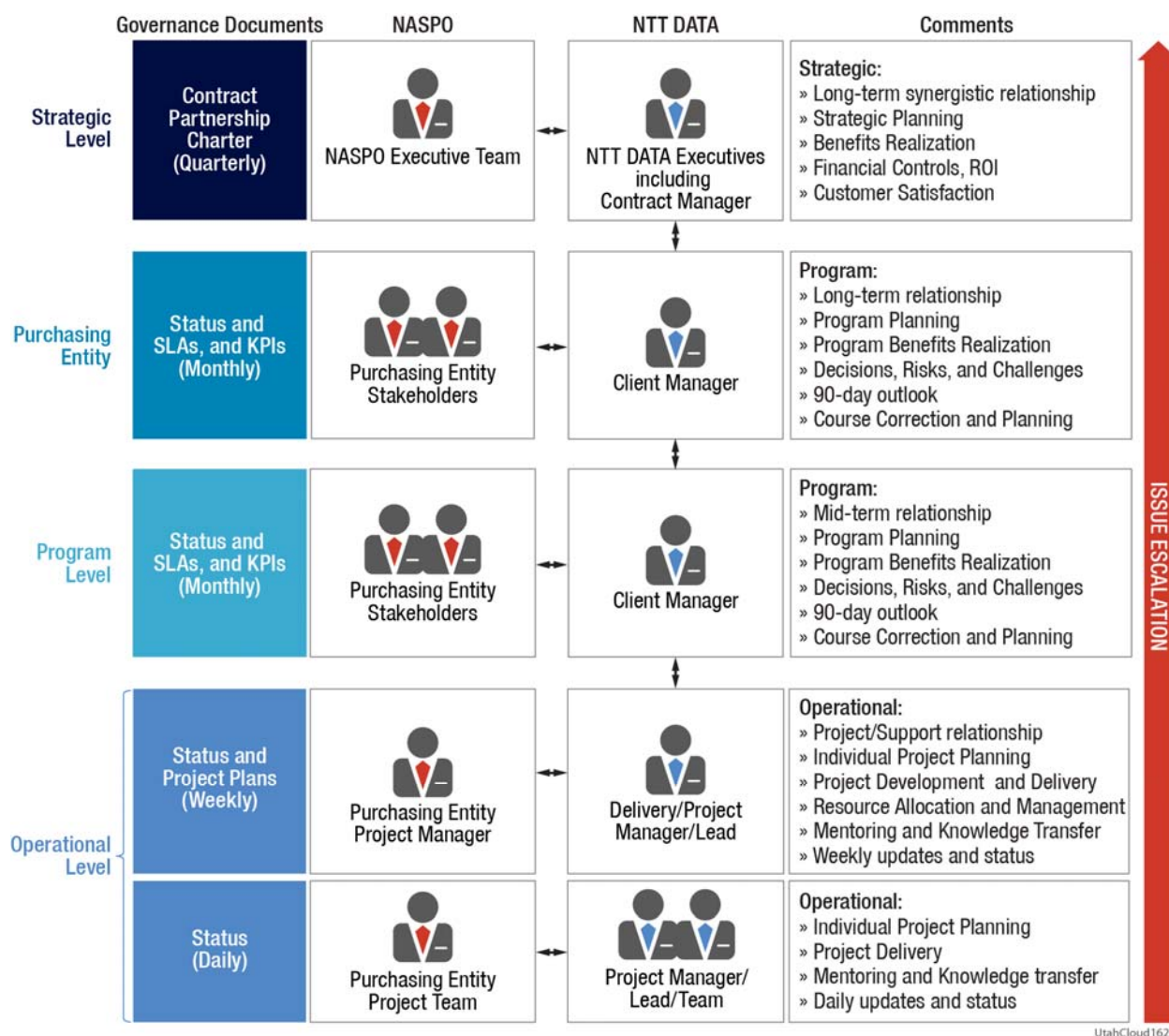
Our expectation is that we will have delivery teams working under the delivery manager's direction that will handle issues and day-to-day work at individual purchasing entities. These teams will keep the delivery and client managers informed of the status of the engagements at Purchasing Entities. We tailor our delivery structure to the needs of our clients, so we may deviate from this general structure if specific purchasing entity circumstances require.

### Governance

Thus, in terms of governance, we would likely implement a tiered governance model such as that shown in Exhibit 35. This is a three-tiered model with:

- An **Operational Level** – This is the base level of this engagement. It includes day-to-day operational matters on delivery. A delivery manager at the purchasing entities will represent NTT DATA at this level and will report on status to the client manager.
- A **Program Level** – The level includes managing multiple project and organizational issues and contacts across a purchasing entity. This level exists even if there is only one project at a purchasing entity. In some cases, NTT DATA will already have a client manager assigned to a purchasing entity; in cases when an entity new to NTT DATA purchases services, a client manager will be assigned.
- A **Strategic Level** – Senior executives from the client and NTT DATA—including representatives from NASPO, if required, as well as the contract manager that liaises between NTT DATA and NASPO—form the strategic level of this model. These executives are also included in resolving escalated issues, if any, and in building a synergistic relationship.

Exhibit 35. Governance Model



*Typically, in engagements, we work in with clients in a three-tiered governance model, with interaction on the operational, program, and strategic levels.*

With that said, we understand that each statement of work issued by a purchasing entity will come with its own governance requirements, and we will operate within them.

### 6.4.1.3 SLA Management

Our customer service processes include other elements. For example, for more information on our incident escalation process, see Section 6.3 (Working with Purchasing Entities).

Also, as we indicated, for more information on our approach to service level management, see Section 6.10 (Service Level Agreements).

### 6.4.2 Compliance with Customer Service Requirements

8.4.2 Offeror must describe its ability to comply with the following customer service requirements:



- a. You must have one lead representative for each entity that executes a Participating Addendum. Contact information shall be kept current.
- b. Customer Service Representative(s) must be available by phone or email at a minimum, from 7AM to 6PM on Monday through Sunday for the applicable time zones.
- c. Customer Service Representative will respond to inquiries within one business day.
- d. You must provide design services for the applicable categories.
- e. You must provide Installation Services for the applicable categories.

NTT DATA will comply with these customer service requirements by following these practices and procedures:

- NTT DATA will assign one lead representative for each entity that executes a participating addendum. We will keep contact information current.
- NTT DATA customer service representatives will be available 24x7 by phone or by email.
- NTT DATA customer service representatives will respond to inquiries within one business day. We expect to formulate SLAs with purchasing entities that will significantly reduce required response times.
- NTT DATA can provide design services for your applicable categories. We are a full service IT services provider. The services we offer include design and consulting services for technologies ranging from infrastructure to enterprise package software, application development, and application maintenance.
- NTT DATA can provide installation services for your applicable categories. The purchasing entities you represent can also perform many self service functions, such as creation and destruction of server images, allocation of storage, and report generation through our self-service portal.

## 6.5 Security of Information (RFP §8.5)

### 6.5.1 Data Protection Measures

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

At NTT DATA, we take our role in protecting customer data seriously and we have several mechanisms and processes in place to do so. Several of these mechanisms and processes are described in more detail elsewhere in this document. For example:

- **Storage Architecture** – The NTT DATA storage services architecture is designed for high availability with redundant switching and host bus adaptors, and it uses enterprise class storage arrays from EMC and other vendors. Data can be encrypted at rest and data for different clients is logically segregated. See Section 6.1 (Technical Requirements) for more information.
- **Backup** – If requested by a purchasing entity, we can use Avamar software with Data Domain de-duplicating storage for backups. Backups are mirrored from our production site in Virginia to our DR site in Sacramento. See our response to Question 8.8.2 in Section 6.8 (Service or Data Recovery) for more information.

- **Replication** – In addition to backup—and if requested by a purchasing entity to lower a recovery time objective (RTO) or a recovery point objective (RPO)—we can replicate customer data asynchronously from production to DR sites. See our response to Question 8.8.2, in Section 6.8 (Service or Data Recovery) for more information.
- **Data Disposal** – When a purchasing entity exits our cloud, we will wipe all data from its portion of the storage pool so that it can be repurposed. We do not destroy drives, as they are reused. If there is a specific certification or process that a client requires, we can accommodate it so long as it does not require the destruction of drives.

## 6.5.2 Compliance with Data Privacy and Security Laws

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

We certify that NTT DATA will comply with all applicable laws related to data privacy and security, which will be defined in the relevant participating addendum or SLA.

## 6.5.3 Access of Purchasing Entity User Accounts and Data

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.

We certify that NTT DATA will not access a purchasing entity's user accounts or data except in the course of data center operations or in response to service or technical issues as required by the express terms of the master agreement, the applicable participating addendum, or the applicable SLA.

## 6.6 Privacy and Security (RFP §8.6)

### 6.6.1 Compliance with NIST and Other Standards

8.6.1 Offeror must describe commitment to your commitment 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.

At NTT DATA, we base our security policies on NIST and Center for Internet Security (CIS) guidelines. Specific guidelines regarding data privacy, protections, user access, server hardening, and encryption are based on NIST SP-SP 800 series documents. Adherence to such guidelines is audited to promote future compliance.

### 6.6.2 Security Certifications

8.6.2 Offeror must list all government or standards organization security certifications you currently hold that apply specifically to the hosted environment described in your firm's RFP response, 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.

NTT DATA has built an enviable reputation with a track record as a prime cyber security vendor for the federal government, state agencies, and local governments. This work includes defending defense-in-depth enterprise security postures, driving all aspects of certification and

accreditation activities, implementing and executing security functional and assurance testing, conducting vulnerability assessments, and recommending strategies to mitigate risk. We are trusted partners to a range of security-conscious federal agencies, including the:

- Federal Bureau of Investigation (FBI)
- U.S. Navy
- Securities and Exchange Commission
- Department of Homeland Security

We have security expertise who understand the security needs of many different industries, information security standards, and directives. We also have certified IT security experts on our staff who have helped define standards such as the NIST 800 series, Federal Information Security Management Act (FISMA)-related standards, Department of Defense directives, National Security Agency standards, ISO 27001, and others.

NTT DATA is compliant with a range of different government regulations, industry standards, industry processes, best practices, and guidelines, including:

- The Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), the Freedom of Information and Protection of Privacy Act (FIPPA), the Personal Health Information Protection Act (PHIPA), the Personal Information Protection and Electronic Documents Act (PIPEDA), and Sarbanes–Oxley Act (SOX).
- International Organization for Standardization (ISO) 17799 (27001:2005, 27002), 7498-2 ISO 20000
- NIST Special Publications i.e. FIPS (For example, 800, 180, 140-x) Certification
- Corporate Security GO–ITS security standards
- CSE, SANS, and CERT guidelines

Also, our Service Operations Center is ISO-27001 certified.

Exhibit 36 offers other examples of security certifications.

## Exhibit 36. Security Certifications



SSAE 16 - Type 2 SOC 1  
Annual SOC audit and report  
on financial controls



Type 2 SOC 2  
Annual audit and report on security  
and availability controls



PCI DSS 3.0  
Payment Card Industry Data  
Security Standard



FISMA - Moderate  
Federal Information Security  
Management Act



HIPAA  
Health Insurance Portability  
and Accountability Act



Energy Star Rating  
Energy efficiency



LEED Certification  
Leadership in Energy and  
Environmental Design



Safe Harbor  
Customer data privacy

*This exhibit summarizes some of the security certifications held by our company.*

### 6.6.3 Security of Data and Applications

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.

#### General Features of Physical Security

The data centers we are offering in this proposal include a broad range of physical security features designed to keep data secure.

The entire perimeter of the building, including the roof, is monitored by on-site security guards 24x7 using high-resolution, pan-tilt-zoom cameras. The parking lots adjacent to the building are controlled and monitored 24x7. The pathways and roadways leading to the main entrance, and to the shipping entrance, are also monitored 24x7. Data center exterior walls are concrete, 9-inches thick. The only exterior glass is located in the security lobby, which is protected by concrete and steel bollards outside of the building, as well as a raised sidewalk. The glass is also located outside of the mantrap area. Biometric iris scan required for entry into data center.

Access to the building lobby requires a card key. Once inside, the lobby is staffed 24x7 by armed in-house security staff seated behind bullet proof glass. Entrance to the first layer of the data center (which includes conference rooms, restrooms, and break rooms) requires dual-factor authentication with a biometric iris scanner and a card key.

Access to the deeper data center layers—including inner hallways with doors to the data center rooms and the actual data center rooms—is protected by multi-factor authentication points that include a combination of PIN-code access keypads, card key readers, and biometric iris

scanners. Every access point is monitored, and weight-sensitive portals control multi-person entries. Also, the system monitors and logs the entry and exit of each visitor to the facility and to customer cages. This means that the security staff has constant knowledge of the whereabouts and activities of all individuals within the data center facility.

The data center's cages have a final level of security. Based on customer requirements, a card key reader, a PIN-code access keypad, a biometric iris scanner, or any combination of the three can be installed on the cage door. Additionally, each customer has the option of having a camera security system independent of the building security cameras installed in their cage.

Other data center security features include:

- Digital, pan-tilt-zoom cameras that monitor all data center secure areas, parking lots, entrances, and the roof. These cameras are monitored by a 24x7 security team.
- 12-foot security fencing, a security-operated shipping and receiving area, and 175 steel and concrete bollards surrounding the facility
- A building-within-a-building design that provides physical protection for IT assets on the data floor

If a Procurement Entity contracts for colocation space, authorized Procurement Entity personnel will receive unescorted access to the specific co-location space that houses Procurement Entity-owned hardware. Procedures the data center will follow are detailed below.

### **Physical Access Control**

If a Procurement Entity contracts for colocation space, authorized Procurement Entity personnel will receive unescorted access to the specific co-location space that houses Procurement Entity-owned hardware. Procedures the data center will follow are detailed below (procedures are identical for NTT DATA support personnel to access the cage containing the VPC equipment).

At the first visit to the data center, Procurement Entity personnel with written authorization to have physical access to the co-location space will be asked to present photo identification, such as a driver's license or a passport. The in-house security staff will then set up the biometric and pin-code access and give the authorized contact a security card key badge.

The badges issued to Procurement Entity personnel can be used on the building entrance and on the IEHP cage. All visitors will be required to wear a visitor badge at all times.

IEHP personnel will have access to the common area of the facility, including a restroom and a galley. They will also have access to the data center loading dock, to a storage room that can be used to house IEHP's assets, and to a community staging area for pre-provisioning tasks.

To authorize new or different employees as eligible to visit the data center and IEHP's cage, IEHP will provide written notice to NTT DATA through a designated point of contact.

In some cases, IEHP may have a manufacturing or other third-party representative scheduled to be onsite. In this scenario, prior written notice from the Procurement Entity will be required before any third party will be allowed inside the facility, the cage, or other colocation space.

All equipment must be brought into the facility through the shipping and receiving area.

Note that other customers in the building will not have access to the Procurement Entity's cage, unless they are IEHP-authorized contacts.

### **Physical and Environmental Safety Measures**

All employees and co-location customers are required to adhere to NTT DATA's physical and electronic access control policy to ensure that only authorized users are provided access to

information based on business requirements. We have implemented a range of security controls to monitor and manage these requirements. Among them:

- We have segregated restricted areas from general public areas. We control access to restricted areas using an electronic access control system. We provide access only to authorized users based on their business needs and prior approvals.
- Our badge readers include an anti-pass back feature to better monitor user movement
- We provide authorized employees with individual access cards to access restricted areas
- Our security staff monitors entry to restricted areas and the movement of authorized employees and materials on a 24x7 basis.
- We allow visitors, contractors, and vendors' access to restricted areas based on business requirements and upon approval by the appropriate manager. Such visitors, contractors, and vendors are escorted by authorized NTT DATA employees.
- As part of our practice of monitoring physical access, individual facility team reviews physical access records to restricted areas and reports violation to the respective account head for further action.
- Our users are not authorized to carry personal devices such as personal laptops or storage devices in restricted areas. Only authorized NTT DATA devices (aside from mobile phones) are allowed inside our facilities. In certain cases, to protect client security, we will restrict employees from carrying mobile phones inside a client production area.
- All NTT DATA facilities include building safety measures such as fire extinguishers, smoke detectors, water sprinklers, emergency exits, and public announcement systems.

### Logical Security Measures

Client data within private clouds are protected from electronic intrusion by firewalls, access control measures and other standard security practices.

Client data within the NTT DATA virtual private (community) cloud are protected from electronic intrusion by firewalls, access control measures and other standard security practices. In addition, clients within the virtual private cloud are separated from one another by virtual firewalls, VLANs and SAN logical unit separation so that clients within the cloud have no means of intruding into the electronic space occupied by one another.

### 6.6.4 Data Confidentiality Standards and Practices

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

Access to the NTT DATA cloud environment is granted strictly to users requiring such access. Access to specific client data is restricted to administrators only and is governed on least-privilege basis. The list of users and administrators is audited on a quarterly basis. Strict policy on user access is enforced.

Users accessing the cloud environment connect via virtual desktops, granting them required access. Access from mobile devices is not permitted.



### 6.6.5 Third Party Attestations, Credentials, and Certifications

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.

NTT DATA holds SOC 1 and SOC 2 certifications. Other certifications include PCI and FISMA. Our Service Operations Center is ISO 27001-certified. For more details, please see our response to Question 8.6.2, in Section 6.6.2 (Security Certifications), including Exhibit 36.

### 6.6.6 NTT DATA's Logging Process

8.6.6 Offeror must provide and describe your 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.

All networking devices and infrastructure servers are configured to send real-time logs via syslog to a centralized logging location. Windows servers are set up for WMI information on application, security and system logs. Linux servers are setup as per application and system requirements based on various syslog facilities. As the customer has administrative access to virtual servers, they have great flexibility as to the event types logged. We can discuss special requirements during the contract process.

As mentioned in our report on our CSA Cloud Controls Matrix, named "NTT DATA's Report on Exhibit 2 to Attachment B – CSA\_CCM\_v3.0.1 09-16-2014", we conduct reviews of many frameworks and policies annually (or when we are notified of significant changes) to make sure we remain compliant. We review:

- Security certifications such as SOC-1 and 2 and ISO 27001
- Nonconformities of established policies, standard, procedures and compliance obligations
- Our overall control framework
- Compliance with baseline security requirements
- Formal risk assessments to determine the likelihood and impact of all identified risks using qualitative and quantitative methods.
- Network and virtual instance configurations

We take appropriate steps to address issues that are uncovered during the review process.

### 6.6.7 Restriction of Visibility of Cloud-Hosted Data and Documents

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

The NTT DATA cloud environment is created with full isolation, preventing data access across clients. In addition, user access such as VPN and client data access is governed by Active Directory group membership, whereby only users authorized to view client data are able to do so.

### 6.6.8 Notification of Security Incidents

8.6.8 Offeror must describe your notification process in the event of a security incident, including relating to timing, incident levels. You 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.

Please see our response to Section 6.3 (Working with Purchasing Entities) for a discussion of the notification process for a security incident. NTT DATA always works with our clients to refine the notification process so that it is customized to each client's requirements.

### **6.6.9 Isolation of Hosted Servers**

8.6.9 Offeror must describe any security controls, both physical and virtual Zones of Control Architectures (ZOCA), used to isolate hosted servers.

NTT DATA's cloud environment is built with strict physical and virtual VLAN segregation. Access across client environments is denied. Each client security zone is protected by a firewall restricting internal and external access. All network access has to be permitted via an explicit network access list. All traffic that is not explicitly permitted is denied.

In addition, servers requiring external access are placed in an isolated DMZ segment, with restricted access to other systems.

### **6.6.10 Security Technical Reference Architectures**

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)

Please see the diagram we included as a separate PDF attachment, named "8.6.10 NTT DATA\_Cloud\_security\_V2.3.pdf".

### **6.6.11 Security Procedures for Employees with Access to Sensitive Data**

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.

Operational security is a significant factor in securing information and such security is founded on a motivated and well evaluated workforce

NTT DATA hires only qualified college graduates for our service offerings. Our selection process starts with the Resource Request that contains a detailed job description, which is reviewed and approved by management. The job description provides details about the position requirements as well as the required profile in terms of "essential" and "desired" competencies, education, work-experience, and other factors necessary to recruit qualified candidates.

NTT DATA has a rigorous multi-step selection process aimed at providing "the right fit" person to the process. Our dedicated recruiting team works closely with our delivery managers to validate that all the requirements for the position are understood. Only then can the sourcing and identification of a candidate pool occur. Once a candidate pool has been identified, the recruitment team delivers appropriate written and oral tests to gauge such things as communication skills, business aptitude, as well as specific business process competency.

Top candidates are then taken through a series of personal interviews customized to the position description. A first level interview is conducted by Human Resources personnel, a semi-structured format aimed at evaluating proficiency levels on identified competencies such as problem solving skills. Communication skills are also assessed in this interview. A second level interview is then conducted by the business manager. When specific skill sets such as voice capabilities are required, candidates are assessed for specific communication attributes including factors such as accents, fluency, vocabulary, clarity, intonation, and pitch.



Post selection, candidates are subject to various verification tests to validate the integrity of the profile as well as the required background checks and verifications required by our clients. All statements made in the resume regarding education and professional qualifications are subject to check with review of original copies of such certificates required at the time of joining. Other factors such as a valid separation note from the previous employer are also reviewed. A formal employee agreement is signed upon hiring.

For all managerial positions (supervisors and above), a supervisory reference check is mandatory before extending a letter of intent. A detailed feedback is taken from at least two references in a prescribed format.

Access to each colocation room is controlled by a combination of card key and pin-code password. Biometric iris scanning is used to control access to the cage. Access logs can be pulled in real time from the NTT DATA web portal.

Logical access to all servers is recorded including username and source IP. These records are retained for a year.

#### **6.6.12 Confidentiality of Data at Rest and in Transit**

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.

At NTT DATA, we use a wide variety of encryption technologies from various vendors, including Cisco for network transmissions (data in motion), EMC AES 256-level encryption for data storage at rest, and Avamar and Data Domain for backup encryption (data at rest).

We have also enabled AES 256- level encryption for backups. Our Service Operations Center is ISO 27001 certified.

#### **6.6.13 Notification and Mitigation of a Data Breach**

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.

##### **Overview**

NTT DATA complies with all applicable laws regarding the safeguarding of client data. We will maintain PCI data and perform notification in accordance with the requirements of any applicable contract we might have with any purchasing entity. NTT DATA will work with the purchasing entity to identify the data involved in a breach and will help the purchasing entity with whatever information NTT DATA possesses to identify the persons affected, their identities and the confidential information and data disclosed.

##### **Response to Security Incidents**

NTT DATA has a documented response program with policies and procedures to address privacy incidents, unauthorized disclosure, access or breach of client confidential information. We follow our internal Intrusion reporting procedures that outline steps taken to isolate and block the potential breach or intrusion.

The threat detection database is updated daily with the latest threat signatures, so the newest threats are detected. All received alerts are logged and the IPS also captures all the detected packets which can be used for further investigation into traffic patterns.

The IPS is configured to alert based on the severity of detected threats. Once the alert is received, initial triage is performed, and depending on the severity of the threat, the customer is

notified. The client CIO on file and the escalation team will be notified of all high priority security events within four hours after the incident occurs.

All lower priority events will be assessed and notification will be sent out to the client CIO on file and escalation team within 1 business day of the incident.

Our security breach response is the process and action we take in response to a security incident to protect ourselves, our customers and partners if/when a security incident occurs - this includes:

- Receiving, reviewing and responding to a security breaches
- Working with the customer to understand the incident
- Preparing and planning for handling the incident
- Setting of clear priorities
- Executing a response to the incident
- Finding and correcting the root cause of the incident
- Determining of the implications of past incidents
- Recording and preserving the analysis of past incidents and learned lessons
- Reviewing and appropriately updating the policy at least once every 6 months or as a change in policy/ procedure/ technology occurs.

Incidents of any major category - which would include a major facility incident, major network incident, security incident, Data Breach or client specific incident - are classified as a "Priority 0" and addressed by representatives from each department including department heads, directors, and executive management. This core team is empowered to execute on every aspect of remediation and coordinates all activity through an open bridge line allowing fully and clear communication among all parties.

The specific makeup of the core team is determined during discussion between NTT DATA and the purchasing entity during the transition period and would at least the following participants:

- The **client manager**, who manages the business relationship between NTT DATA and the purchasing entity.
- The **delivery manager**, who manages the day-to-day delivery of services to the purchasing entity.
- **Individual SMEs** who possess domain-specific knowledge, notably the **security manager**.

In addition, **executive sponsors** may become involved as required by unfolding events.

For more details of our escalation process, see our response to Question 8.4, in Section 6.4 (Customer Service).

## 6.7 Migration and Redeployment Plan (RFP §8.7)

### 6.7.1 Closing a Service

8.7.1 Offeror must describe how it manage the end of life activities of closing down a service to a Purchasing Entity and safely deprovisioning it before you are 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 and how portable the data is during migration.

There are no particular technical constraints on moving data, metadata and usage data from our environment to a successor's and therefore data is fully portable. Should a purchasing entity choose, all data, can be encrypted at rest or in motion.

- Windows and Linux server images stored in our VMWare environment can be returned in a format suitable for VMWare-based systems. Alternatively, we support Open Virtualization Format (OVF), a standard in the industry supported by most Cloud Service Provider's and can export files in that format if needed.
- Usage and metadata can be exported in .xls or other appropriate formats and
- A purchasing entity will have direct administrative level access to their data and can copy it to a selected destination. Alternatively, data can be returned in backup format. The virtual private cloud can be thought of as the virtual equivalent of physical colocation.

Service shutdown would be treated as any other service request subject to governance of the service request and change management processes. We would plan and manage the data and application migration through our Service Operations Center.

## 6.7.2 Orderly Returns of Data

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.

A purchasing entity will have administrative access to its server images and data and can retrieve any data by simply copying it over the wire to a destination of their choosing. In that case, no SLA is necessary. Alternatively, a purchasing entity can request that NTT DATA perform the copy to a destination of the purchasing entity's choosing. Of course, if desired, NTT DATA can discuss an SLA covering data return with the purchasing entity.

## 6.8 Service or Data Recovery (RFP §8.8)

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

- a. Extended downtime.
- b. Suffers an unrecoverable loss of data.
- c. Experiences a business failure.
- d. Ability to recover and restore data within 4 business hours in the event of a severe outage.
- e. Describe your Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

### Extended Downtime

Once extended downtime is incurred, the NTT DATA Crisis Management team is convened and they monitor the situation. This team consults with technical SMEs, facilities managers, vendors and other support organizations. If the team determines that service will be restored within a reasonable amount of time, the various support organizations will continue to work to resolve the issue. If the team determines that downtime will be excessive, it will activate the NTT DATA disaster recovery plan and will switch operations over to the DR site for recovery or execute

other mitigation strategies. Once the issue(s) at the production site are corrected, production reverts back to Ashburn in an orderly manner.

### **Unrecoverable Losses of Data**

If an unrecoverable loss of data is experienced by a client, NTT DATA has the following options to recover that data.

- Restore data from the production site DataDomain system using our Avamar backup software. This can be done on a file by file basis by service request. If current file are compromised, older data can be recovered
- Restore data from the DR site by copying from replicated storage (data available only if Warm and Hot recovery have been selected for the data store in question).
- If the production DataDomain system has been compromised, data can be recovered from the Data Domain system located at the backup site which contains a replicated copy of the production device.

### **Business Failures**

If an overall system failure is encountered, see the high level description of NTT DATA's response to extended downtime above.

### **Ability to Recover and Restore Data Within 4 Business Hours**

NTT DATA provides many recovery options. A complete list of options follows, several of which support 4 hour recovery:

- No DR: Best effort recovery after servers with higher DR options are recovered
- Disaster Recovery from Backups (Cold DR):
  - All Production Instances will be recreated from backup data at a separate DR site.
  - Upon declaration of a disaster, the DR cloud instances will be created at the DR site using technology resource specified by the client.
  - RTO and RPO 48–72 hours.
- Recover from Replicated Data (Warm DR):
  - All Production Instances will have data asynchronously replicated to the DR site.
  - The production cloud instances will be recreated from replicated virtual machine images at the DR site upon declaration of disaster.
  - RTO will be 4 hours, and RPO will be less than 15 minutes.
- Hot DR:
  - All Production Instances will be installed and running at the DR site.
  - Data from the primary site is asynchronously replicated to the DR site.
  - The production cloud instances at the DR site will be activated through network switching on declaration of disaster.
  - RTO will be 15 minutes to 1 hour as required, and RPO will be less than 5 minutes.

## Recovery Point Objectives and Recovery Time Objectives

As we described in our listing of DR options above, NTT DATA can configure the rates of data replication and methods of application restoration, including RTOs and RPOs, to comply with your recovery requirements on a server by server basis.

### 6.8.1 Backup and Restore Services

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

- a. Method of data backups
- b. Method of server image backups
- c. Digital location of backup storage (secondary storage, tape, etc.)
- d. Alternate data center strategies for primary data centers within the continental United States.

#### Method of Data Backups

NTT DATA uses EMC Avamar and Data Domain deduplication backup software and systems to provide fast, efficient, data backups for its virtualized environments. All backup data is stored at redundant NTT datacenter sites and the data can be quickly recovered in just one step. Avamar provides AES 256- level encryption.

Backup data is encrypted during transit across our WAN and at rest for added security. Avamar Data Store uses grid architecture that eliminates single points of failure; system and data integrity are verified daily to ensure recoverability.

As a part of NTT DATA's backup solution, all backed up data standard retention is 31 days, or as directed by each customer for each platform. We are able to offer longer retention periods if specifically required by our clients.

Backup testing is performed every 30 days with a sampling of tenant data per customer. Backups are continuously monitored and if any of the backup jobs fail, they are immediately kicked off again in order to ensure proper completion.

#### Method of Server Image Backups

NTT DATA's backup solution provides fast, single-step recovery of individual files or complete VM images to the original VM, an existing VM or a new VM.

#### Digital Location of Backup Storage

Backups are stored in our Data Domain system located at our production site in Ashburn, VA. We maintained a mirrored, replicated copy in a second Data Domain system located in our DR facility in Sacramento, CA.

#### Alternate Data Centers

Our primary data center is located in Ashburn, Virginia; our secondary (DR) data center in Sacramento, California. Backup storage is located in both sites. The production backup store is mirrored in the secondary site.

If a purchasing entity chooses, we can lower recovery time and recovery point capability by replicating data from the production site to the DR site as described above in our response to Question 8.8.1.

## 6.9 Data Protection (RFP §8.9)

### 6.9.1 Encryption and Other Options for Protecting Sensitive Data

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.

NTT DATA uses a wide variety of encryption technologies from various vendors, including Cisco for network transmissions (data in motion), EMC AES 256-level encryption for data storage at rest and Avamar and Data Domain for backup encryption (data at rest). We have enabled AES 256- level encryption for backups.

### 6.9.2 Agreements to Protect Data

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.

On behalf of NTT DATA, we certify that, after an appropriate review, we are willing to sign a business associate agreement (BAA) or any other agreement that may be necessary to protect a purchasing entity's data.

### 6.9.3 Use of Data for Defined Purposes

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.

We certify that NTT DATA shall only use data for the purposes defined in the master agreement, a participating addendum, or a related SLA. We will not use government data or government-related data for any other purpose, such as for data mining. NTT DATA and our subcontractors (should we ever employ subcontractors) will not resell nor otherwise redistribute information gained from access to the data received through this contract vehicle.

## 6.10 Service Level Agreements (RFP §8.10)

### 6.10.1 Negotiability of Sample SLA

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.

#### Overview

NTT DATA's performance is measured in different ways by different customers. During the definition of a statement of work, NTT DATA and the purchasing entity will mutually agree on a SLA and key performance indicators (KPIs) that will comprise the data categories within the monthly reports that will be submitted for performance review purposes. Typical KPIs are described in the attached sample contract, named "5.5.4 NTT DATA Sample Cloud Hosting Contract.pdf".



SLAs are established during NTT DATA's well-defined transition process as part of the activities we perform to assume responsibility for the operation of a purchasing entity's environment. The transition process is briefly described in the following overview. More detail on the transition process is available in Appendix 1 (Overview of Transition Process). We can supply still more detail about the transition process upon request.

### Overview of Transition Approach

NTT DATA differentiates itself from competitors by treating transitions as a specialized activity requiring specialized skills. It is our practice to assign a dedicated and experienced transition manager from NTT DATA's Transition Services Group (TSG). TSG is a group of highly experienced IT managers who have managed about 70 transitions over the last several years, with a total contract value of more than \$1.6 billion. Over the course of these transitions, NTT DATA has not incurred a single financial penalty for missing a transition milestone, which immediately translates into reduced risk for a purchasing entity. Having a dedicated team ensures that NTT DATA is able to apply best practices and lessons learned to every transition effort and allows the engagement manager to focus on managing service delivery and establishing a long-term partnership with our clients.

The following Exhibit 37 depicts the high-level approach NTT DATA would take for transitioning the services for a purchasing entity, including phases, major activities, and deliverables.

Exhibit 37. High-Level Transition Approach

Phase	Transition In					Service Delivery and Improvement
	Transition Planning	Knowledge Acquisition	Process and Staff Integration	Engagement Governance	Project Management	
Activity	<ul style="list-style-type: none"> <li>» Complete due diligence</li> <li>» Ramp-up staff</li> <li>» Prepare for knowledge transfer</li> <li>» Establish network, hardware &amp; application access</li> <li>» Set-up office, logistics onsite &amp; offshore</li> <li>» Develop transition plan and Knowledge Acquisition Process (KAP) syllabus</li> </ul>	<ul style="list-style-type: none"> <li>» 4 Learning phases to acquire knowledge driven by detailed KAP syllabus</li> <li>» Deliverables at end of each phase</li> <li>» Learn how apps and infrastructure support Purchasing Entity business</li> <li>» Resolve incidents and problems, and perform productive work</li> </ul>	<ul style="list-style-type: none"> <li>» Acclimate to Purchasing Entity environment</li> <li>» Train staff on NTT DATA and Purchasing Entity environments</li> <li>» Define delivery procedures, handoffs, and templates</li> <li>» Implement work tracking tool for all in scope services</li> <li>» Develop in-flight project assessment</li> </ul>	<ul style="list-style-type: none"> <li>» Develop communication plan</li> <li>» Agree on service levels</li> <li>» Assess metrics tool to determine changes needed to support new model</li> <li>» Baseline and report service levels</li> </ul>	<ul style="list-style-type: none"> <li>» Structured management of the transition project</li> <li>» Issue management</li> <li>» Risk management</li> <li>» Status reporting</li> <li>» Status meetings</li> <li>» Delivery acceptance</li> <li>» Change management</li> </ul>	<ul style="list-style-type: none"> <li>» SLA achievement</li> <li>» Regular client Communication</li> <li>» Cross-training</li> <li>» Productivity improvement</li> <li>» Risk management</li> <li>» Relationship management</li> <li>» Issue resolution</li> </ul>
	<ul style="list-style-type: none"> <li>» Detailed transition plan and risk plan</li> <li>» Agreed-on entry and exit criteria for each transition phase - KAP syllabus</li> </ul>	<ul style="list-style-type: none"> <li>» Reverse presentation</li> <li>» Application documents and run books</li> <li>» Transfer of ownership plan</li> </ul>	<ul style="list-style-type: none"> <li>» Procedure manuals</li> <li>» Staff training plan</li> </ul>	<ul style="list-style-type: none"> <li>» Communication plan</li> <li>» SLA reports</li> <li>» client environment document (CED)</li> </ul>	<ul style="list-style-type: none"> <li>» Status reports</li> <li>» Risk plans</li> <li>» Issue logs</li> </ul>	<ul style="list-style-type: none"> <li>» Knowledge management system</li> <li>» Governance reporting</li> <li>» Support and maintenance services</li> </ul>

UtahCloud1620

*This exhibit summarizes our approach to transitions at a high level.*

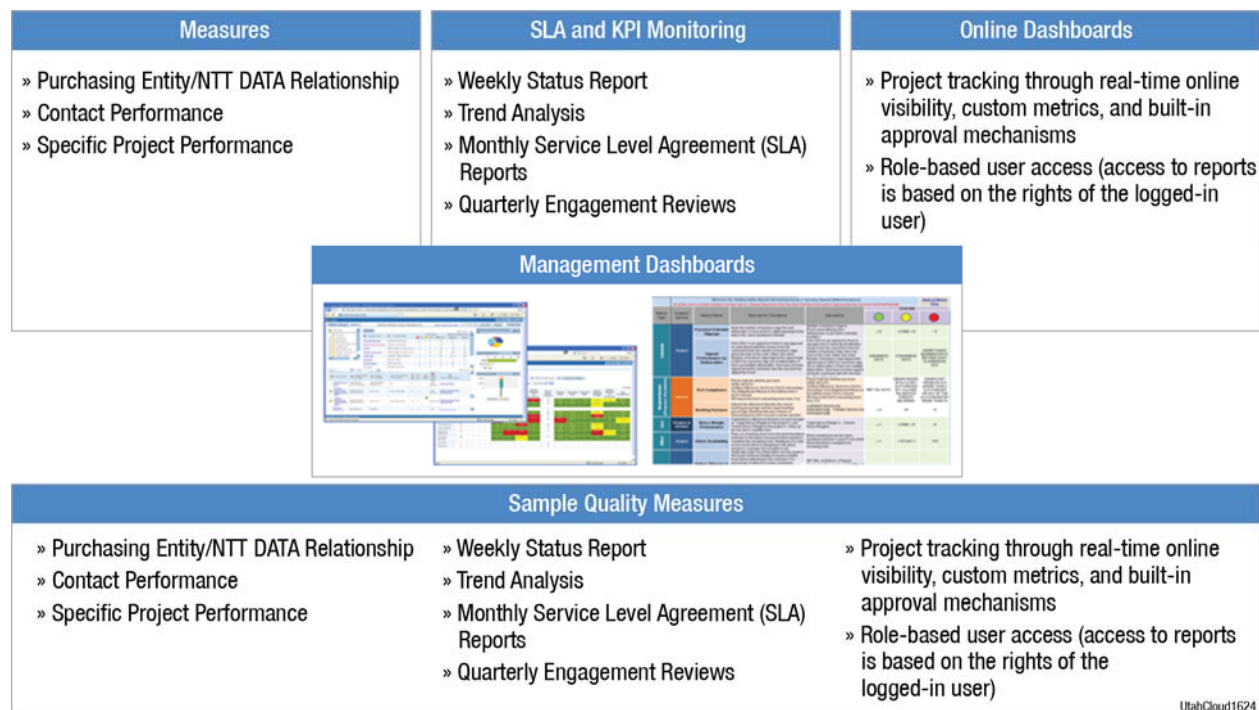


## Service Level Requirements Management Approach

NTT DATA's overall methodology includes various management and operational reports to track the transition itself and the support as we move forward. We plan to utilize the reports to support our overall service plans for purchasing entities.

Exhibit 38 shows the SLAs and metrics we use to measure the project performance.

Exhibit 38. SLAs and Metrics



*This exhibit summarizes some examples of service level measures and metrics.*

## Define and Meet Service Levels

NTT DATA will focus on process integration that will define a unified process for service delivery during transition. As part of our process integration set of activities within transition, we will prepare any processes, tools, reports, or similar necessary components to enable accurate data capture, analysis, and reporting.

The following exhibit depicts NTT DATA's typical service level targets:

Exhibit 39. Service Level Targets

	Acknowledge Time	Performance Min./Target	Status Updates	Resolution Time	Performance Min./Target
Severity 1	15 minutes	96% – 98%	Hourly	1 hours	92% – 98%
Severity 2	15 minutes	96% – 98%	Hourly	4 hours	92% – 98%
Severity 3	8 hours	96% – 98%	Weekly*	2 days	92% – 98%
Severity 4	1 business day	96% – 98%	Weekly*	5 days	75% – 80%

*This table summarizes some typical service level targets. \*These intervals typically are negotiated at less than weekly when services are first established.*

NTT DATA will review the service level targeted by purchasing entities within their RFPs and anticipates complete compliance with the identified response and resolution time targets and associated achievement percentages subject to final, detailed description during SLA development. NTT DATA commits to meet service levels from day one of the steady state phase including the 99.99 percent availability target for production applications

NTT DATA recognizes that managing based on facts makes organizations more proactive in the identification and resolution of problems, helps project future performance, and enables better, timelier, and informed decision-making.

### Developing and Analyzing Metrics

NTT DATA has a well-defined testing metrics model, which is developed on the GQM method. The GQM method is a common approach to identify an appropriate set of metrics for reporting.

This is a top-down method in which business goals are formulated. These goals include questions that constitute the basis for the metrics.

The collected metrics will provide the answers to those questions, and indicate, among other things, whether the goal is being achieved. The following Exhibit 40 depicts the GQM methodology.

In consultation with the purchasing entity, a focused set of metrics will be selected and achievable target values for each measure will be set. NTT DATA will analyze and trend the metrics to measure progress towards goals and identify opportunities for improvement.

When any of the thresholds have been crossed, further investigation will be conducted to determine root cause and correct the problem. The trending of metrics will allow measures to be compared to past performance, action thresholds, or target levels so that appropriate action can be taken to improve the measurement.

We would recommend following the GQM process to fully explore those goals and their related questions and metrics. However, based on our current knowledge of typical Public Sector Entities, the sampling of metrics described below would be among those that we would consider to be valuable to them and would be candidates for implementation.

It should be noted that these metrics reflect activity or impact across the services. However, the information necessary to generate the metrics can be collected through tools and would be available to the Metrics Manager and those working with them.

The following table summarizes key cost metrics.

Exhibit 40. Goal-Question-Metric Method



*We follow a four step process for developing metrics.*

Exhibit 41. Key Cost Metrics

Metrics Name	Description	Frequency
Effort Variance	Variance in actual effort with respect to planned effort	Month end, phase end

Metrics Name	Description	Frequency
Effort Saved due to Automation	Automated test execution effort with respect to manual test effort	Phase end
Resource Utilization	Captures resource usage and idle time to plan for future period and optimized resource utilization	Weekly, monthly

With regard to cost metrics, we can also work with purchasing entities to define other cost-related metrics, but those will require data collection activities that go beyond the information that is readily captured in a test management tool set. Those metrics could include rework cost per defect by application area or by severity, average rework cost by capture area, rework cost as a percentage of development cost and other similar information.

The selected metrics will be added to the metrics management dashboard to help a purchasing entity and NTT DATA review them strategically against the overall objectives, including:

- Cost savings (initial and continuous)
- Improved productivity and cost effectiveness
- Quality improvement

At this point, a selected group of metrics can then be added to the dashboard on a “snap shot” basis to provide a summary for each development phase by application area or other meaningful grouping.

### Leading Indicator Metrics

NTT DATA recognizes that managing by leading indicators makes organizations more proactive, helps project future performance, and enables better, timelier decisions. NTT DATA will work with appropriate purchasing entity counterparts and use tools such as Pareto analysis and Trend analysis to analyze the metrics and evaluate developing trends to measure progress toward goals and identify opportunities for improvement.

The following table outlines a set of metrics that would assist a purchasing entity and NTT DATA in managing by leading indicators.

Exhibit 42. Leading Indicators

Leading Indicator	Summary of Leading Indicator	Metrics	Target/Goal
Productivity	Productivity has a direct link to cost. A trend in improved productivity will indicate a reduction in cost and declining productivity will indicate higher costs. This indicator will also be helpful in improving effort estimation accuracy for future projects.	Test Execution Productivity = Total # of test cases executed/Total test cases design effort (hr.) Test Design Productivity = Total # of test cases designed/Total test case design effort (hr.)	The higher the better. A trend showing and increase in the #/hr.
Schedule Slippage	Schedule slippage will directly indicate whether the delivery will be on time or not, and the extent of delay. It will also improve schedule	Schedule Variance – % deviation from planned schedule = [(Actual End Date – Estimated End Date)/(Estimated End Date –	Closer to 0%

Leading Indicator	Summary of Leading Indicator	Metrics	Target/Goal
	estimation accuracy.	Estimated Start date)] X 100 Phases will be Test Planning, Test Design and Prepare, and Test Execution	
Effort Slippage	Effort slippage indicates whether a project is executed within the budgeted effort. This metric will be used to improve effort estimation accuracy by providing feedback on the estimation model for future releases.	Effort Variance – % deviation from planned effort = [(Actual Effort – Planned Effort)/Planned Effort] * 100 Phases will be Test Planning, Test Design and Prepare, and Test Execution	Closer to 0%
Support Adequacy	Development Support Adequacy indicates whether there is enough support from the development team to fix the defects raised. Insufficient support will result in schedule slippage. In addition, sufficient testing may not be possible due to late defect fixes and will have a bearing on the quality of the system that moves to production.	Defect Status – Number of Defects Closed vs. Number of Defects reported = (# Defects Closed/# of Defects Reported) x 100	Closer to 100%
Resource Utilization	Resource utilization will indicate the amount of work coming to the Augmented Test Pool with respect to the resource level in the Augmented Test Pool. This will allow for future resource planning of the augmented test pool. This will also indicate if the augmented test pool is being used effectively, and indicate its cost effectiveness.	Resource Utilization – Percentage of effort that is utilized for test projects within the Augmented Test Pool = [Total # of hours spent by all resources in a month/Planned billable hours of all resources in a month] x 100	Closer to 100%

### Metrics in Place for Various Engagement Types

NTT DATA implements quality measures for a project such as effort variance, schedule variance, defect slippage, defect density, productivity index, and SLA-related metrics for engagements to arrive at mandating the performance of the engagement. Further, we constantly (weekly/monthly/mile stone based) track these metrics through tools such as defect management system, integrated project tracking system and dashboards to monitor the quality of the engagement.

For the data center services, NTT DATA defines SLAs taking into account estimates of current and desired service levels, and specifies a range of services and expected performance levels.

The SLA is reviewed periodically over the term of the engagement to accommodate updates resulting from changes in environment, client expectations, and work volume/profile.

Some sample metrics that are used to build SLAs are listed in the following table.

Exhibit 43. Sample SLA Metrics

Metric	Content	Frequency	Level	Calculation
Availability	Availability is a function of the total service time, the mean time between failure (MTBF), and the mean time to repair (MTTR)	Monthly	Per Category	$\left[ \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}} \right] \times 100$
Mean Time Between Failures	MTBF is the aggregate time of all time periods between failures, divided by the number of failures (-1)	Monthly	Per Category	$\frac{\text{Sum (Time stamp of new failure - Time stamp of old failure)}}{(\text{Total number of failures} - 1)}$
Mean Time To Repair	MTTR is the aggregate of all the time required to resolve issues, divided by the number of items repaired	Monthly	Aggregate	$\frac{\text{Sum (Time stamp of the resolution of a ticket minus the time stamp of the start of the ticket)}}{\text{Total number of tickets}}$
Number of Incidents Occurrences	Measurement of the incident-based workload	Daily	Per Category	Total number of incidents logged in the incident management application for a given period
Incident Resolution Effort	Optimize resource utilization and determine where investments in automation make sense	Monthly	Per Category	Total work effort to resolve the all incidents/Total number of incidents
Top N Failure Causes (N typically equals 5 to 10)	Optimize resource utilization and determine where investments in automation make sense	Monthly	Per Cause Type	Total work effort to resolve all the incidents/Total number of incidents
Top N Affected Items	Optimize resource utilization and determine where investments in automation make sense	Monthly	Per Item Type	Total work effort to resolve all the incidents/Total number of incidents
Number of Knowledge Assets Created	Reduce MTTR	Monthly	Per Category	Number of knowledge records in either the vendor or MS knowledge

Metric	Content	Frequency	Level	Calculation
				management application
Total Number of Calls to Service Desk	Make more informed resourcing decisions	Daily	Per Category	Calculated from Automatic Call Distribution (ACD) statistics
Average Call Duration (minutes)	Make more informed resourcing decisions	Daily	Per Category	Calculated from ACD statistics
Time to Respond to Outage Tickets	Reduce MTTR	Monthly	Incident	Time to respond – Time of initial notification
Time to Respond to Normal Problems and Requests (non-outage)	Reduce MTTR	Monthly	Incident	Time to respond – Time of initial notification
Time-to-Close/Escalate Outage Tickets	Reduce MTTR	Monthly	Incident	Time to close/escalate – Time of initial notification
Time-to-Close/Escalate Normal Problem and Request Tickets (which do not require Change Management or work window) or Dev./QA incidents	Reduce MTTR	Monthly	Incident	Time to close/escalate – Time of initial notification
% of Reopened Request/Incident Tickets	Customer Satisfaction	Monthly	Aggregate	Tickets reopened/Total Tickets
Root Cause Analysis	Problem Management	Monthly	Aggregate	Number of root causes provided within 24 hours/Number of root causes requested

*This table contains sample SLA metrics.*

A distinguishing feature of the data centers in which our production and DR sites are located is a service level that includes 100 percent uptime for power and cooling service. This SLA, which may be unique in the industry, sets our data center apart, and is a function of its patented 2N+2 design.



#### Exhibit 44. Typical Facility-Level SLAs

Service Type	Availability/Response Guarantee	Time Frame for Service Credit Applicability	Resolution
Power	99.99%	15 minutes after power failure	Power restored
Network	99.99999%	15 minutes	Network recovered
HVAC	99.99%	15 minutes	HVAC restored
Service Management	100% response time	24 hours from request	Request fulfilled

*These are typical facility-level SLAs.*

We will work with individual purchasing entities to establish an SLA and KPIs appropriate to their hosted and managed environment.

### 6.10.2 Sample SLA

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.

NTT DATA has provided a sample contract, named "5.5.4 NTT DATA Sample cloud Hosting Contract", that lists typical terms, conditions, and service levels as part of our response package. This document will serve as a starting point for negotiations. With that said, arriving at an actual contract along with an accompanying SLA will require negotiation and a signed agreement with a purchasing entity.

## 6.11 Data Disposal (RFP §8.11)

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

When a Purchasing Entity exits our cloud, we wipe all data from their part of the storage pool so that it can be repurposed. Drives are not destroyed as they will be re-used. A customer typically receives confirmation of the execution of this task via a service request close ticket, but if there is a specific certification or process that a client requires, it can be accommodated so long as it does not require destruction of drives.

## 6.12 Performance Measures and Reporting (RFP §8.12)

### 6.12.1 Ability to Guarantee Reliability and Uptime

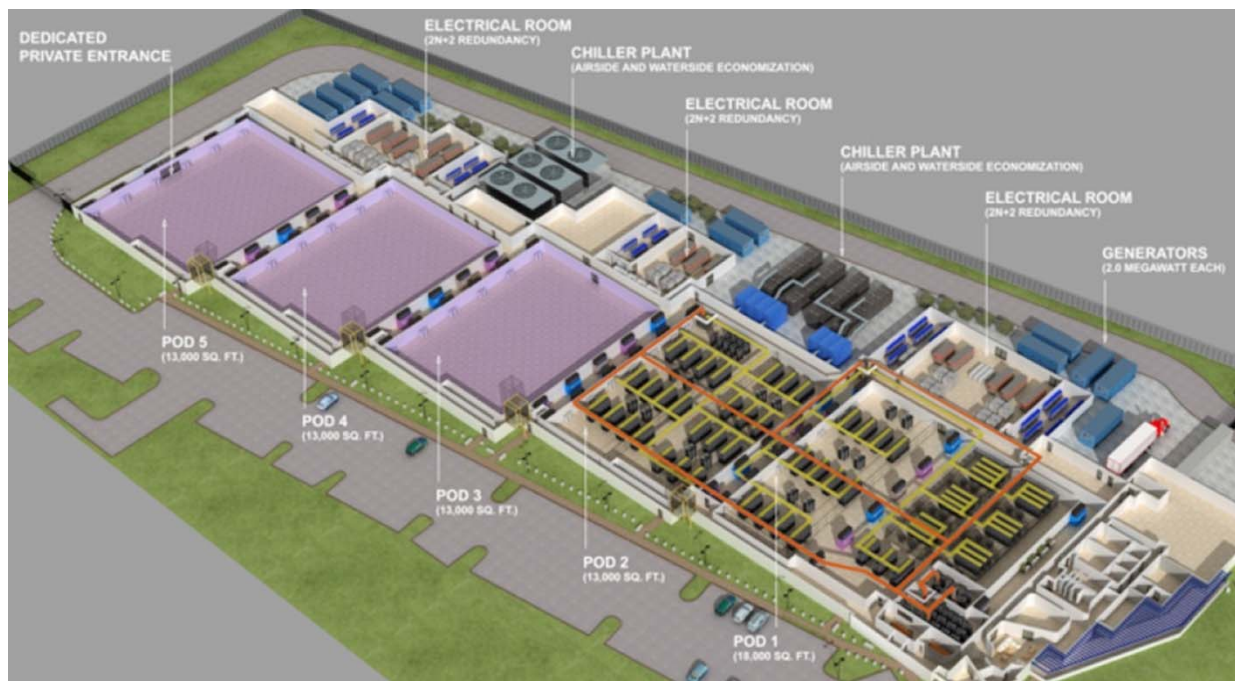
8.12.1 Describe your ability to guarantee reliability and uptime greater than 99.9%. Additional points will be awarded for 99.99% or greater availability.

A distinguishing feature of the data centers in which our production and DR sites are located is a service level that includes 100 percent uptime for power and cooling service. This SLA, which may be unique in the industry, sets our datacenter apart, and is a function of its patented 2N+2 design.



As we have indicated, the data center used by our production instance is located in Ashburn, Virginia. This is a world-class data center that includes many state-of-the-art-features, including redundant systems and modular architecture. Exhibit 45 below, provides a floor plan of the Ashburn data center. The Sacramento site where our DR instance is located is similar in design and implementation

Exhibit 45. NTT DATA Center Floor Plan



*This data center, located in Ashburn, Virginia, includes a patented “2N+2” design. This allows us to commit to 100 percent uptime for power and cooling.*

Overall availability is based on the capability of the physical infrastructure as well as that of the server and storage equipment within the facility. Our cloud is based on the VMWare hypervisor and VCenter administration so, in the event of failure of an individual physical system, workloads can be seamlessly migrated from one physical device to another. We use enterprise class EMC storage equipment; data is backed up locally and replicated to our DR site in Sacramento, CA. Finally, the site is monitored continuously and we conduct proactive Capacity Management to identify bottlenecks and overflows and address them before they affect the site.

As mentioned in the attached sample contract (named “5.5.4 NTT DATA’s Sample Cloud Hosting Contract.pdf”), our typical availability SLA for the entire IaaS offering is 99.93 percent, inclusive of planned downtime.

### 6.12.2 Standard Uptime Service and Related Criteria

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

Please see our response to Question 8.10, in Section 6.10 (Service Level Agreements).

### 6.12.3 Obtaining Support

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.

A participating entity can contact us for support in several different ways:

- By telephone
- By email
- By web-based ticket entry using BMC Remedy

Our Service Operations Center provides 24x7, as we described in Section 6.3 (Working with Purchasing Entities).

### 6.12.4 Failure to Meet Incident Response Times and Incident Fix Times

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

At NTT DATA, we take very seriously our responsibility to provide available infrastructure to our clients. In our agreements with clients, failure to meet SLAs is often penalized through service credits or other penalties, but these penalties vary according to the portfolio of services we are providing. Thus, specific remedies will be determined between NTT DATA and a purchasing entity during the transition and stabilization periods.

### 6.12.5 Procedures for Planned Downtime

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

NTT DATA conducts routine maintenance according to a pre-determined schedule that is available well in advance of downtime. NTT DATA conducts Change Approval Board (CAB) meetings weekly and notifies clients of scheduled downtime as part of the minutes of those meetings.

### 6.12.6 Consequences If Disaster Recovery Metrics Are Not Met

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

As we have indicated, at NTT DATA, we take very seriously our responsibility to provide available infrastructure to our clients. Failure to meet SLAs is often penalized by service credits or other penalties, but those penalties vary with the portfolio of services being provided. Thus, specific remedies will be determined between NTT DATA and a purchasing entity during the transition and stabilization periods.

### 6.12.7 Sample of Performance Reports

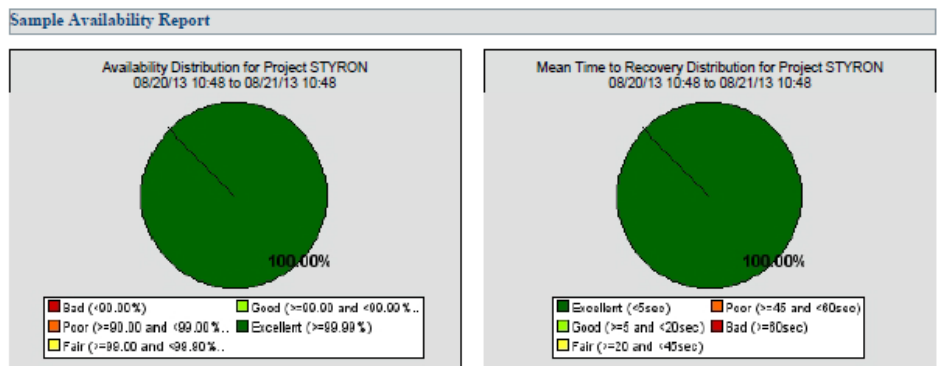
8.12.7 Provide a sample of performance reports and specify if they are available over the Web and if they are real-time statistics or batch statistics.

A variety of real-time performance reports are available through our web portal. Exhibit 46 contains sample screen shots from such reports.

Exhibit 46. Sample Availability Reports

Sample Availability\_Report Page 1 of 1

Sample Availability Report



Index	Application Transaction	Measurement Duration	Down Time	MTTR	Availability(%)
1	NASADMWSTYAD01 NASADMWSTYAD01	23 hr 59 min	0 sec	0 sec	100.0
2	NASADMWSTYAD02 NASADMWSTYAD02	23 hr 59 min	0 sec	0 sec	100.0
3	NASADMWSTYDBS01 10.2.0.50	23 hr 59 min	0 sec	0 sec	100.0
4	NASADMWSTYDS01 10.2.0.200	23 hr 59 min	0 sec	0 sec	100.0
5	NASADMWSTYIP01 10.2.0.203	23 hr 59 min	0 sec	0 sec	100.0
6	NASADMWSTYTS01 NASADMWSTYTS01	23 hr 59 min	0 sec	0 sec	100.0
7	NASADMWSTYWBS01 10.2.0.51	23 hr 59 min	0 sec	0 sec	100.0
8	NASADMWSTYWDB01 10.2.0.100	23 hr 59 min	0 sec	0 sec	100.0
9	NASDNFLBMCAP01 10.0.206.8	23 hr 59 min	0 sec	0 sec	100.0
10	PSIPRODAD10 10.33.32.59	23 hr 59 min	0 sec	0 sec	100.0
11	PSIPRODAD11 10.33.32.60	23 hr 59 min	0 sec	0 sec	100.0



*This exhibit shows some examples of our availability reports.*

## 6.12.8 Ability to Print Historical, Statistical, and Usage Reports Locally

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

As usage reports are available through a web interface, they can be printed locally to the machine used to make the report request.

## 6.12.9 Support for On-Demand Deployment

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

We certify that NTT DATA's on-demand deployment is supported 24x365.

## 6.12.10 Scale-Up and Scale-Down

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

We certify that NTT DATA's scale-up and scale-down is available 24x365, and that new instances can be added in 1 hour or less. Please see our extensive responses to Question 8.14 and Question 8.17 (in Section 6.14 and Section 6.17, respectively) for a discussion of our service provisioning process.

## 6.13 Cloud Security Alliance Questionnaires (RFP §8.13)

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

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

As we indicated in our response to Question 5.5.3 in Section 3.3.3 (Completed Copy of CSA Star Self-Assessment Form), we have completed and submitted the CSA STAR Registry self-assessment.

NTT DATA has not applied for Level 2 CSA STAR Registry Certification, but we can discuss the possibility of obtaining such certification during contract negotiations. Also, NTT DATA has not obtained a Level 2 CSA STAR Registry Attestation, but this is something we can also discuss during contract negotiations.

NTT DATA has completed and submitted both the CSA STAR Registry Self-Assessment named ("NTT DATA's Report on Exhibit 1 to Attachment B - CAIQ version v 3.0.1-09-16-2014") and a report on our compliance with the Cloud Controls Matrix named ("NTT DATA's Report on Exhibit 2 to Attachment B – CSA\_CCM\_v3.0.1 09-16-2014"). Specifically, we have provided these documents as attachments to this proposal and uploaded them separately on Bidsync as part of our submission.

## 6.14 Service Provisioning (RFP §8.14)

### 6.14.1 Emergency or Rush Implementation Requests

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

To fully understand our process for emergency changes or rush implementations, it is necessary to understand our complete change management process, which we apply to all changes to the configuration of our overall cloud and individual client environments. Emergency changes and rush implementation are available, if necessary, and described below as a sub process, but are discouraged because rushing such modifications can result in avoidable errors.

With change being a constant in any IT organization, a comprehensive change management process is critical. Adopting this capability enables better management of change in the environment with the goal of minimizing the adverse impact of change. Leveraging existing ISO 20000 certified and ITIL-based change management processes allows the NTT DATA Team to meet industry proven practices, enables a shared services environment, and ensures that all changes are:

- Assessed in a controlled manner
- Approved/rejected in a controlled manner
- Implemented and reviewed in a controlled manner

NTT DATA's change management process manages the risk associated with performing changes to a purchasing entity's Infrastructure, allowing for consistent service to be delivered



while facilitating changes. Change Management provides a method for implementing approved changes efficiently, cost-effectively, and with minimum risk to IT services and its underlying infrastructure. A consistent and reliable approach accomplishes this, because most incidents and problems can be attributed to change.

Our process provides visibility of upcoming changes, improves communication, shares technical experience, and helps minimize disruption to the environment. Our change management solution builds in technological integration with other processes.

NTT DATA's Change Management process consists of eight activities (Sub-processes):

- **Change Initiation and Recording:** This sub-process controls the initiation and recording of Application or Infrastructure-related changes.
- **Change Assessment and Authorization:** This sub-process is responsible for reviewing and prioritizing a change. Scoping, impact analysis and planning activities are performed at this stage.
- **Change Scheduling:** This sub-process is responsible for scheduling a change once it has been built and tested. This sub-process involves the review and approval of the change request from a final review authority such as a Service Owner, Change Manager, or the Change Advisory Board.
- **Change Planning and Implementation:** This sub-process is responsible for final planning and the implementation and validation of a change in the production IT environment.
- **Post Implementation Review:** This sub-process is responsible for determining the potential root causes of failed changes, determining lessons learned, and executing remedial action plans.
- **Emergency Change:** This sub-process is responsible for managing Emergency changes. Emergency Change requests go through an expedited approval and implementation process. A formal RFC is drafted after implementation and reviewed to determine any required follow-up actions.

Other Change Management Activities:

- **Change Management Reporting:** This sub-process is responsible for collecting and defining the reporting requirements for the Change Management process.
- **Manage and Improve the Change Management Process:** This sub-process is responsible for managing and improving the Change Management Process. This involves defining policies for Change Management practices and regularly reviewing and auditing those practices. The Process Owner has final responsibility, although other process members will perform part of the activities and tasks.

Exhibit 47. Change Management Roles and Responsibilities

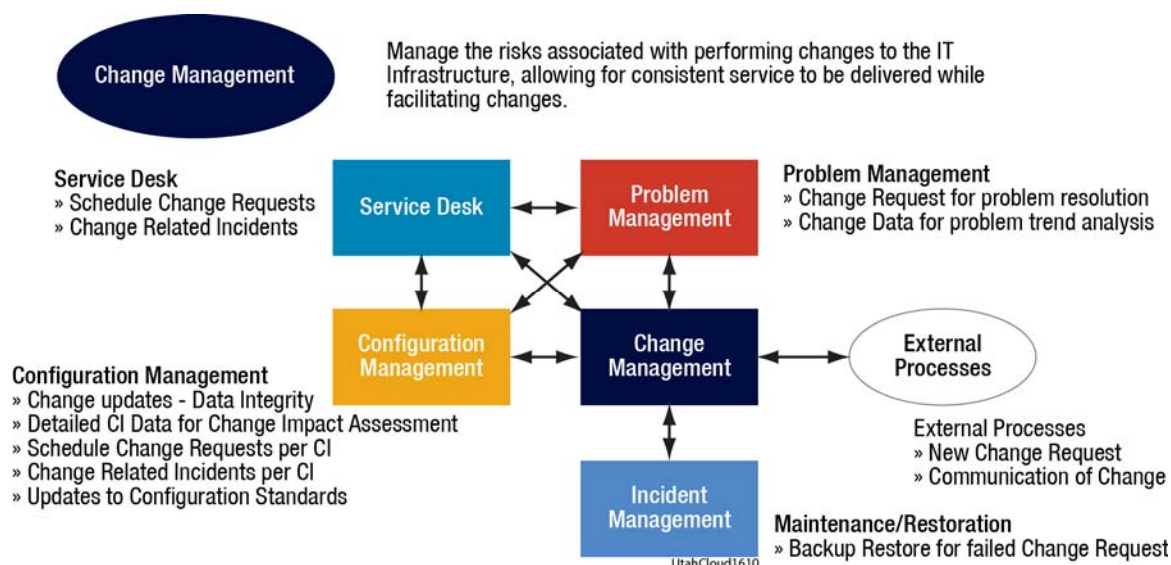
Roles	Responsibilities
Change Management Process Owner	<ul style="list-style-type: none"><li>• Recognized in the whole organization as the spokesperson for Change Management</li><li>• Communicates and markets the process, initiates Process Improvements and sets goals</li><li>• Leads development/improvement efforts of the Change Management process on a regular basis</li><li>• Approves alteration of the Change Management process and supporting procedures</li></ul>

Roles	Responsibilities
	<ul style="list-style-type: none"> <li>Enforces and plans for audits of the Change Management process</li> <li>Accountable for defining change management reporting requirements and frequency</li> <li>Accountable for the overall effectiveness and efficiency of the process</li> </ul>
Change Initiator	<ul style="list-style-type: none"> <li>Initiates a Change by opening a Change Request or contacting a Local Process Expert or the Service Desk</li> <li>Involved in reviewing comments upon rejected changes to decide next steps</li> </ul>
Change Manager	<ul style="list-style-type: none"> <li>Operational leader of the Change Management process</li> <li>Coordinates all of the activities of the Change Management process</li> <li>Validates completeness of change request documentation on ad hoc basis</li> <li>Resolves scheduling conflicts for Changes where CAB involvement is not required</li> <li>For Emergency Changes, coordinates approval and implementation with Change Implementers and Change Approvers</li> <li>Reviews change request and associated documents for scheduling on ad hoc basis</li> <li>Chairs the Change Advisory Board</li> <li>Publishes Schedule of Changes</li> <li>Participates in any Emergency CAB</li> <li>Validates completeness of Change Request documentation</li> <li>Reviews emergency change records and closes them</li> <li>Is responsible for defining Change Management reporting requirements and frequency</li> <li>Is responsible for providing metrics, measurements, and reports of the entire process</li> <li>Coordinates the regular review and improvement of the Change Management process</li> <li>Plans and Coordinates Process Training</li> </ul>
Service Desk	<ul style="list-style-type: none"> <li>Provides guidance to end users upon requests of types not clear or not known</li> <li>Evaluates incoming requests and determines if they are Change Requests</li> <li>Records change details provided by Local Process Experts</li> <li>Ensures complete and accurate Requests for Change from end users</li> <li>Determines Request type and category</li> <li>Routes the Change Request to the appropriate group/coordinator</li> <li>Assigns emergency change requests</li> <li>Reviews and assigns pre-approved change requests</li> </ul>
Change Implementer	<ul style="list-style-type: none"> <li>Plans for detailed implementation tasks like scoping, impact assessment, and planning</li> <li>Determines if a Change Request meets Project criteria and classifies Changes as major or minor</li> <li>Schedules change implementation</li> <li>Generates work orders for the testing and implementation of the Change according to the plans and monitors the execution for success or failure</li> <li>Initiates back-out procedures when necessary</li> <li>Documents the results of the change and involves Incident or Problem Management if problems are encountered</li> <li>Executes follow up action plan for any changes recommended by</li> </ul>



Roles	Responsibilities
	CAB/Change Manager/Change approvers <ul style="list-style-type: none"> <li>• Closes Change record</li> <li>• Notifies Change Initiators upon Change completion (tool-enabled, potentially automated)</li> </ul>
Change Advisory Board (CAB)	<ul style="list-style-type: none"> <li>• Reviews Change Requests for associated documentation</li> <li>• Validates completeness of change request documentation</li> <li>• Validates change schedules</li> <li>• Maintains and publishes Schedule of Changes</li> <li>• Provides ad hoc communications to relevant stakeholders if needed</li> <li>• Convenes post-implementation reviews</li> <li>• Reviews potential root causes for failed changes</li> <li>• Determines lessons learned on failed or backed out changes</li> <li>• Verifies change implementation date and checks for any conflicts</li> <li>• Arranges arbitration meetings when necessary</li> </ul>
Emergency CAB	<ul style="list-style-type: none"> <li>• Involved with Emergency Changes</li> <li>• Approves Emergency Changes</li> <li>• Reviews Emergency Changes after implementation to determine if further action is required</li> </ul>
Service Owner	<ul style="list-style-type: none"> <li>• Reviews and prioritizes change</li> <li>• Authorizes infrastructure or break/fix application change requests (depending on service) and notifies appropriate people accordingly</li> <li>• Validates schedules</li> <li>• Resolves scheduling conflicts with help of Change Manager as necessary</li> <li>• Reviews RFCs and associated documents for scheduling changes</li> <li>• Approves Emergency Changes</li> </ul>
Application Coordinator/ Infrastructure Coordinators	<ul style="list-style-type: none"> <li>• Reviews RFCs for completeness and correctness of details</li> <li>• Reviews RFCs with other functional Coordinators as necessary and performs overall impact analysis on Production Environment</li> <li>• Performs initial level of effort estimates for a Change</li> <li>• Updates RFCs as required</li> </ul>
Business Process Engineer	<ul style="list-style-type: none"> <li>• Involved with the review and approval of application changes</li> <li>• Reviews and prioritizes change</li> <li>• Takes the initial decision for approving change requests and notifies appropriate people accordingly</li> </ul>

## Exhibit 48. Change Management Process Flow



*This exhibit summarizes the flow associated with our change management process.*

### 6.14.2 Lead Time for Provisioning Solutions

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

NTT DATA's standard lead time for the provision of non-emergency, simple changes to servers and storage is 5 business days from request to implementation.

More complex changes that require major modifications may require detailed planning and design and therefore may require longer implementation times. In such cases, NTT DATA will start working with the purchasing entity in question to determine project plans and implementation times within 5 or fewer business days.

## 6.15 Back Up and Disaster Plan (RFP §8.15)

### 6.15.1 Applying Legal Retention Periods and Disposition Policies

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

Retention periods can be set as part of our backup and archive process. Non-standard retention periods are available but may be subject to special rates, depending on the particular retention schedule.

At the end of a retention period, data will be discarded and the associated storage returned to the storage pool. For more details on our data disposal process, please see our response to Question 8.11, in Section 6.11 (Data Disposal).

### 6.15.2 Disaster Recovery Risks and Potential Mitigation Strategies

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

NTT DATA has a disaster recovery plan in place to cover all aspects of its business and operational support systems. The details of this plan are confidential, as they relate specifically to NTT DATA's business and operations. Even so, at a high level, NTT DATA's business continuity strategy is to implement measures that take into account the recovery of technological systems needed to sustain the business of NTT DATA, but that also focus on personnel safety and the ability to continue critical business processes during and following an extended disruption.

While developing our DR plan, NTT DATA conducted an "all hazards" investigation into potential failure scenarios. These include:

- Natural hazards such as storm, flood and fire. Our data centers are designed to the highest fault tolerance and engineering strength
- Technology failures, such as:
  - Power or cooling failure. Most data center providers offer N+1 redundancy. Our data center's patented 2N+2 electrical infrastructure redundancy is unmatched. It includes two completely separate power paths to the customer rack (2N). Also, all of the critical components in those two independent power paths have (at least) two extras for backup (N+2). This design gives a new definition for availability: the ability to perform maintenance, have a simultaneous equipment fault and a simultaneous utility outage, and still maintain power and connectivity to the mission critical applications.
  - System failure. Our VMWare cloud can use Vmotion to instantly migrate workloads off failing physical host servers. Our EMC technology can migrate data from failing physical drives to others within the storage pool. All network paths are redundant so that connectivity can be failed over if needed. If all else fails within the production data center, we can switch to our DR site, located far enough away so that it would not be affected by a regional failure.
- Human-caused failures. Human-caused failure range from deliberate sabotage and terrorism to errors of omission by system operators. Mitigation strategies include:
  - Outstanding physical security featuring defense in depth with multiple authentication, authorization and access control
  - Logical security measures at firewalls and with electronic intrusion detectors allow intrusions to be prevented, detected and managed as required.
  - Operator error is reduced through strict adherence to ITIL-based change and incident management processes for which operators are trained. In addition, all data is backed up in both the production and DR sites and can be recovered as required.

Customer-specific disaster recovery capabilities are driven by the customer's business continuity plan, which should have a list of discrete requirements that can be designed into a set of work instructions created for each customer that hosts with NTT DATA's managed hosting service. These work instructions specify quick redirection and recovery of the specific services supplied to the customer by NTT DATA.

Once these work instructions are developed by NTT DATA during the customer's transition project, they can be shared with the customer for inclusion into the customer's overall disaster recovery plan. NTT DATA does not foresee that a participating entity's business continuity plan will be greatly affected. Details of the DR plan, such as network reconfigurations and restart instructions, will change as a result of a new technical environment.

### 6.15.3 Infrastructure for Data Centers

8.15.3 Describe the infrastructure that supports multiple data centers within the United States, each of which supports redundancy, failover capability, and the ability to run large scale applications independently in case one data center is lost.

#### NTT DATA's Cloud Hosting Environment

We understand that client systems need to be available for sustaining both internal and external business operations without disruption or delay; this high availability requirement necessitates a resilient infrastructure that can withstand individual component failures and a DR approach for disaster situations. We recognize the need to provide a DR approach that addresses relevant technology components and platforms to prevent a single point of failure and implement a tape backup/restore for the client applications that meets the business requirements. Our approach will be structured to maintain consistency and integrity of the client applications and data.

The DR activities will include data backup restore tests, as well as testing of the fault tolerant aspects of the infrastructure. We will record the results of the tests, including failures and lessons learned and submit the same to the client.

#### Features of NTT DATA's Virtual Private Cloud Hosting Services

NTT DATA, together with our affiliates in the NTT Group, is

- A VCE solution provider accredited in all five global regions
- The only provider of IBM pSeries consumption-based LPARs
- An SAP-certified provider of cloud services
- An SAP-certified provider of hosting services
- AN SAP-certified provider of SAP HANA operations services

#### Features of NTT DATA's DR Hosting Model

Features of NTT DATA's DR hosting model include:

- **Dedicated Customer DR Technology:** NTT DATA will allocate and configure the necessary technology to support our customers in the event that their own technology becomes unavailable. This technology allows customers to duplicate the production environment for those systems selected for this treatment and achieve fully independent operation and equivalent performance for any application present in the production site.
- **Customizable RTO and RPO:** Depending on the requirements of the application(s) and the customer, NTT DATA can configure the rates of data replication and methods of application restoration to comply with client's outage window
- **Service Monitoring:** NTT DATA will monitor all equipment and processes involved in replicating and supporting your applications in case of failure; a customer declaration of an outage will immediately commence the restoration process using the most recent data available
- **Accessible Technology:** Pre-established network links will allow users to be re-directed to the DR site for application access
- **NTT DATA's multiple data center US strategy:** NTT DATA's virtual private cloud is located in Ashburn, Virginia, (production instance) and Sacramento, California (DR instance). Connectivity between the two sites is maintained over triply redundant communications links managed by multiple carriers, shown in Exhibit 49.



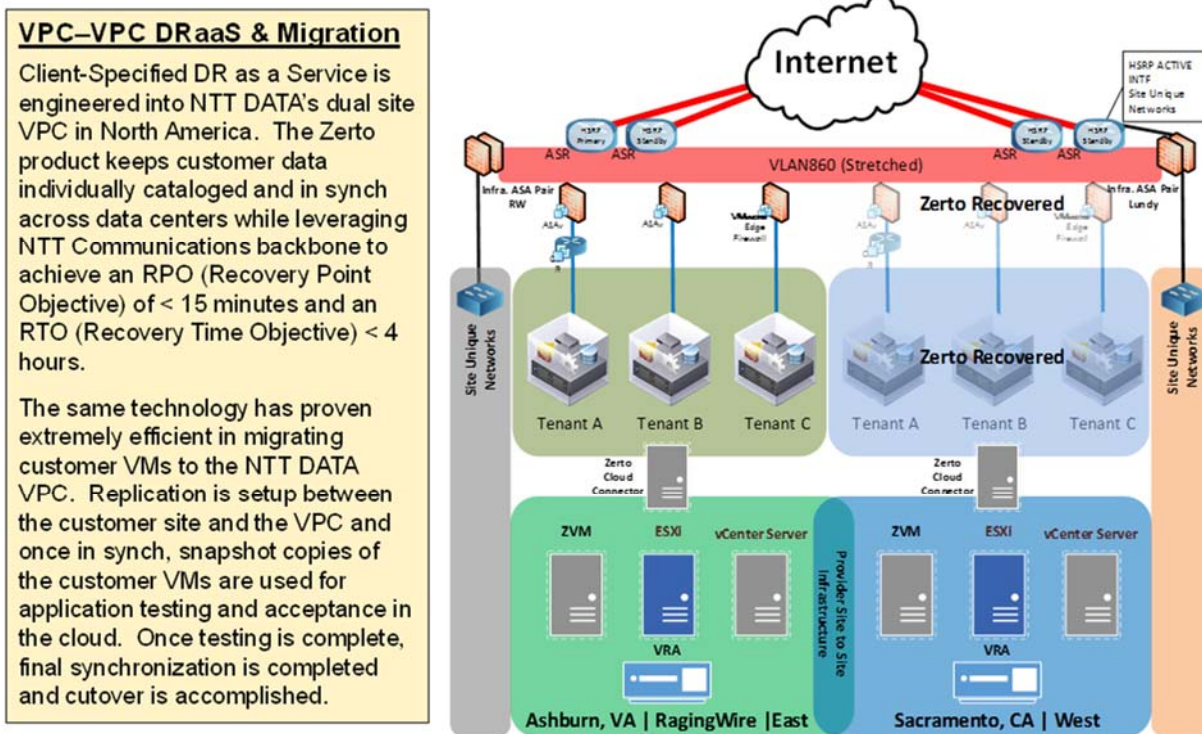
Exhibit 49. NTT DATA's Data Center Topology



*This exhibit summarizes our triply-redundant data center topology.*

NTT DATA uses Zerto technology to manage DR failover, which is designed so that clients can fail over their environments separately from other cloud tenants should the need arise. Infrastructure within the Sacramento DR site is fully capable of assuming the processing load should production instances be failed over.

Exhibit 50. NTT DATA VPC Architecture



*This exhibit summarizes our VPC architecture.*

## 6.16 Solution Administration (RFP §8.16)

### 6.16.1 Managing Identity and User Accounts

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

In our solutions, a purchasing entity will have full freedom with unfettered administrator access to server instances. Identity management systems can be established in the cloud or on client premises, as desired.

### 6.16.2 Anti-Virus Protection for Data Stores

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

The NTT DATA storage pool is SAN -based. As such, it does not have the level of vulnerability of NAS-based storage. Any A/V solution for SAN involves significant performance degradation, and therefore we have not deployed one. As mentioned elsewhere, NTT DATA provides anti-virus protection for physical or virtual server instances using Trend Micro and provides many other logical security controls. In addition, encryption is offered at the OS level and any client wishing to encrypt their servers can utilize encryption to protect their data from exposure.

### 6.16.3 Migration of Data to a Successor Cloud Provider

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

NTT DATA recognizes that a purchasing entity may, for a variety of reasons, wish to transition out from NTT DATA services to another provider. We have developed a process for transition out that we have described at a high level in Appendix 1 (Overview of Transition Process).

There are no particular technical constraints on moving data, metadata and usage data from our environment to a successor's.

- Open Windows and Linux server images stored in our VMWare environment can be exported as "OVF" files,
- Usage and metadata can be exported in .xls or other appropriate formats and
- A purchasing entity has direct administrative level access to its data and can copy it to a selected destination. Alternatively, data can be returned in backup format. The virtual private cloud can be thought of as the virtual equivalent of physical colocation.

Should the time come, NTT DATA is prepared to discuss transition assistance requirements with the purchasing entity in more detail and craft a solution that supports those needs.

### 6.16.4 Distributed Administration

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

A purchasing entity can have administrator access to server instances (but not the underlying hypervisor and other cloud infrastructure). Different participating entities can establish administration processes among each other in the cloud or on client premises as desired.

### 6.16.5 Applying Administrative Policies of Participating Entities

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

A purchasing entity can have administrator access to server instances (but not the underlying hypervisor and other cloud infrastructure). A participating entity also can establish systems in the cloud or on client premises, as desired, for full administrative freedom.

## 6.17 Hosting and Provisioning (RFP §8.17)

### 6.17.1 Cloud Hosting Provisioning Processes

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

For more information on our server deployment process see the user's manual for our cloud portal which we have submitted as an attachment to this technical proposal. (The name of the attachment is "8.17.1 Create a vApp with VMs v 1.2".)

### 6.17.2 Tool Sets

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.)
2. Creating and storing server images for future multiple deployments
3. Securing additional storage space
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).

As part of our standard offerings:

- Clients may use VMWare VCenter, as available in our cloud portal and as documented in the attached file (named "3.6.3 Create a vApp with VMs v 1.2"), to deploy new servers.
- Clients may work with NTT DATA to create and store server images for future multiple deployments using our web portal.
- Clients can secure additional storage space for specific servers through our web portal. (We recommend that large allocations be coordinate with NTT DATA via our change management process.)

Also, specific BMC Monitoring tools we and our clients use include:

- BPPM – This is a centralized event management console that performs all the management and analysis of the events from the monitoring agents. It also performs suppression, correlation, base-lining, notification, auto-action, and alert message enrichment.
- Monitoring (Patrol) Agents – This monitors from 100 to 300 or more metrics, including the operating system, applications, databases, and middleware.
- TMART – This is a synthetic transaction monitoring product. It monitors transaction performance, site availability, and security monitoring.
- Capacity Optimizer – This tool provides capacity and performance monitoring on IT resources. It also provides modeling and forecasting (what if scenarios) of resources.
- Nagios – This is a network and infrastructure monitoring and alerting tool. It monitors network devices such as switches, routers, hubs, network services, and other resources.



- EUEM (End User Experience Management) – This tool monitors and detects “end-user” transaction performance issues across the technology domain, including infrastructure, cloud, networks, and applications.
- BMC Remedy 9 ITSM – This is an IT service management (ITSM) tool that includes all ITIL-compliant service modules, such as incident management, problem management, change management, service level management, asset management, release management, and contract management. It also includes a supported Atrium CMDB (Common Management Database).
- Analytics – This is a centralized reporting tool that provides management or operational type reports from the different toolsets.
- ITSM Portal – This is a centralized portal for management and operations personnel to view the status of the environment, including ticketing, alerts, and performance data.

NTT DATA’s clients also have access to the Cloud Cruiser product for tracking usage statistics. Please see the overview presentation, named “6.5.1 Cloud Cruiser Overview.pdf”, that we submitted in addition to this technical proposal. Cloud Cruiser presents usage statistics to cloud consumers in an easy to understand dashboard format. Consumers can break down usage by device, within departments, and even at the individual level.

## **6.18 Trial and Testing Periods (Pre- and Post-Purchase) (RFP \$8.18)**

### **6.18.1 Testing and Training Periods**

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

NTT DATA provides training during the transition period, as we will describe in our answer to Question 8.18.3 and in Appendix 1 (Overview of Transition Process). Training can be conducted at other times, but, in our experience, the operation of our environment is easy for skilled IT practitioners to understand.

Proof of concept testing as part of the evaluation process is available. As NTT DATA’s virtual private cloud is based on a pool of servers and storage, it is straightforward to provide a POC environment for evaluation by either NASPO or a purchasing entity. We would be happy to discuss further requirements and details when appropriate.

Testing is available at any time during the project on a service request basis. The client is responsible for consumables and setup fees.

### **6.18.2 Environments for Testing and Proof of Concept**

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.
--

As NTT DATA’s virtual private cloud is based on a pool of servers and storage, it is straightforward to provide a proof of concept environment for evaluation by either NASPO or a purchasing entity. We would be happy to discuss further requirements and details when appropriate.

### **6.18.3 Training and Support**

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

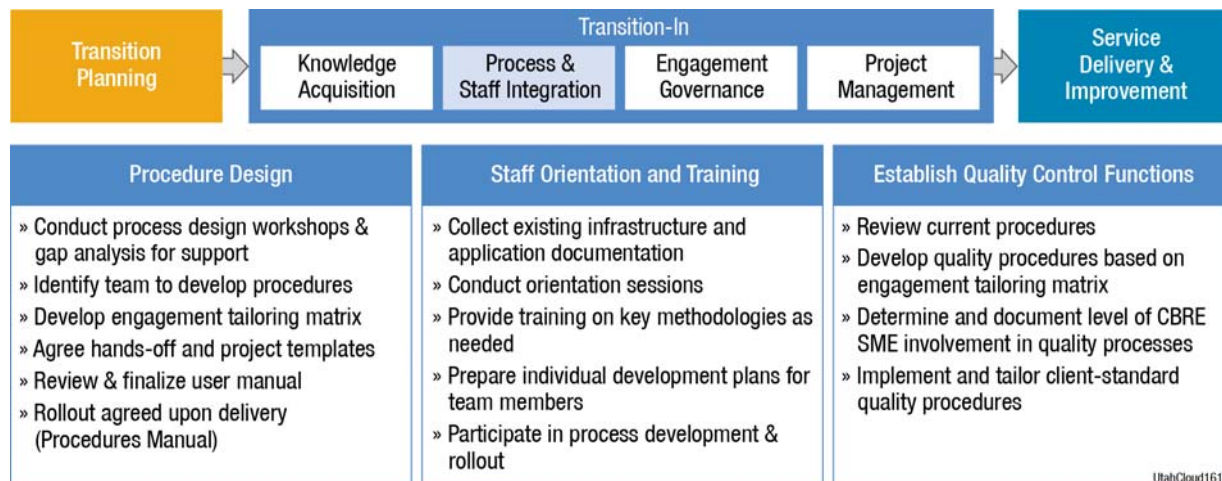
## Introduction

Training and integration of client personnel is conducted at no additional cost as part of our transition process, which we will describe in this rest of this section.

## Process and Staff Integration

Process and staff integration includes procedure design, staff orientation and training, and quality control functions. Exhibit 51 shows the activities and primary tasks that we perform for each of these aspects of process and staff integration.

Exhibit 51. Process and Staff Integration Activities and Tasks



*In our approach to process and staff integration, we address procedure design, staff orientation and training, and quality control functions.*

Building on data gathered during transition planning, NTT DATA will review the purchasing entity IT environment, business processes, system tools, and framework component inventories through structured meetings and data gathering activities. At the same time, NTT DATA will enable key NTT DATA and purchasing entity personnel to receive training in NTT DATA's project management disciplines and methodologies (if deemed appropriate) to confirm that NTT DATA's best practices are well understood and successfully integrated. The following is a 'starter list' of management processes which will be co-developed and approved as an outline for the final process and procedure documentation for each type of service:

- Application Support and Infrastructure Services
- Environments Staging – Procedures to Access
- Support Manual/Procedures
- Full Lifecycle of work tickets
- Change Management Procedures
- Escalation Procedures
- Deliverable Acceptance
- Testing process
- SLA Reporting
- Comprehensive Communication Plan

- Release Management Process & Procedures
- Process Flow of each Incident and Problem Type
- Business Process Services
- Standard Operating Procedures
- Sample process inputs and outputs

NTT DATA will work with purchasing entity resources to develop customized, repeatable processes for the engagement. NTT DATA and purchasing entity will also establish processes for collecting, reviewing, and responding to the metrics that will indicate the team's performance to service levels and areas of improvement. These processes are initiated during transition-in and used throughout the life of the engagement.

Please refer to the full description of our transition process in Appendix 1 (Overview of Transition Process).

In addition to training, NTT DATA, through its Service Operations Center, provides extensive support integrated with our overall RIM services throughout the project lifetime. On call assistance is available to help clients to perform tasks such as entering tickets and service requests into our Remedy ticketing system as well as for provisioning and server management tasks that the client can perform through the Cloud Portal.

## 6.19 Integration and Customization (RFP §8.19)

### 6.19.1 Integration of Services to Other Complementary Applications

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

The control and reporting interfaces for our services are based on web technology, making integration relatively straightforward with complementary applications such as client ticketing, event monitoring, and metering.

Purchasing entities should note that we use the BMC Enterprise Tool Suite as our incident reporting and monitoring software. We have extensive experience ebonding BMC tools with other ticketing technologies so that tickets can be passed back and forth between our system and the systems of our clients. This includes opening or closing tickets in either system.

Our metering software, Cloud Cruiser, also has web-based interfaces so that information can be exchanged between our cloud and whatever accounting systems are being operated by the client.

As a full-service IT provider with skills across the technology stack, we are qualified to discuss more complex interfacing requirement beyond REST or other web technologies and would be happy to do so if desired.

### 6.19.2 Customization and Personalization of Services

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

#### Introduction

NTT DATA's services can be customized in many ways to meet the specific needs of purchasing entities. Customizations can be selected applied to pricing, compute and storage

services, DR and data protection, and levels of remote infrastructure management (RIM). In most cases, these customizations are available on a server by server level (with associated storage) in order to provide maximum flexibility.

### Pricing

NTT DATA offers two methods of subscription to our cloud (IaaS) services:

- **Allocation Method** – In this method, a dedicated cloud technology is allocated to a particular purchasing entity application, to a project team, or along similar principles. In this method, the purchasing entity would maintain a steady monthly payment with expansion (or contraction) available on demand but tightly controlled through the change management process between NTT DATA and the client. This method requires clients to perform regular maintenance, especially of storage, to keep available workspace within allocated limits. The allocation method is used to permanently reserve computing and storage resources.
- **Pay-as-you Go Method** – In this method, the purchasing entity would be charged only for the computing and services consumed (as measured by GHz, RAM, SAN storage, and backups, for example). So, when all or part of the environment is idle, this method primarily incurs just storage costs for servers and virtual machine “templates” that remain idle. In this subscription model, resource use has a tendency to grow unchecked unless clients use disciplined software development life cycle processes.

With either method, a purchasing entity would receive detailed billing by project or by cost center

### Provisioning

Clients can provision compute and storage services or NTT DATA can do so.

**Compute Services.** Virtual machines are available from two server pools or a server by server basis. Specifically, we can provide:

- **VMWare-based systems.** Windows and Linux templates can be created with varying number of CPUs (cores) and associated compute power and local RAM storage
- **AIX-based systems.** AIX, Linux and iSeries LPAR's are available in our Power 7 environment. This is a rarely available cloud offering.

Physical machines are also available, if required, for special computing needs. This provides our clients flexibility when legacy technologies unready for the cloud must be part of an overall solution.

**Storage.** Two classes of storage are available:

- **Optimized Storage.** Our standard offering, optimized storage features automatic migration of data to improve access speed. Data can be moved into fast or slow cache or stored on physical disks of different performance characteristics.
- **Economy Storage.** Economy storage is used for rarely written/rarely accessed data that must be kept online.

### Data Protection and DR

When it comes to backups, NTT DATA can tailor backup frequency, the extent of each backup, and retention periods for each server.

As for disaster recovery, we offer customizable RTO and RPO. Depending on the requirements of our clients' cloud-hosted application(s), NTT DATA can configure the rates of data replication and the methods of application restoration to meet the variable SLA recovery times of a server

tier recovery model on a server-by-server basis in the most cost-effective manner, in the unlikely event of a failure of our facility in Virginia.

Other data recovery options include:

- **Disaster Recovery from Backups (No DR).** With this option:
  - All production instances will be recreated from backup data at a separate DR site.
  - Upon declaration of a disaster, the DR cloud instances will be created at the DR site using available technology equal to the needs of the production environment.
  - RTO will be best effort as required and RPO will be at most 24 hours. All other SLA-based DR recovery described below takes priority.
- **Disaster Recovery from Backups (Cold DR).** With this option:
  - All production instances will be recreated from backup data at a separate DR site.
  - Upon declaration of a disaster, the DR cloud instances will be created at the DR site using available technology equal to the needs of the production environment.
  - RTO will be 24 to 72 hours, as required, and RPO will be at most 24 hours. The cold DR service includes a reservation fee in order to make certain that we have allocated resources at the DR site to recover data and meet the client's SLA.
- **Warm DR utilizing Zerto Technology.** With this option:
  - All production instances will have data asynchronously replicated to the DR site.
  - The production cloud instances will be automatically recreated from replicated virtual machine images at the DR site upon the declaration of a disaster.
  - RTO will be 4 hours to 8 hours, as required, and RPO will be less than 15 minutes.

**Custom Hot DR.** NTT DATA offers various methods of architecting active site configurations that will automatically redirect service to the other site in the case of either site failing. With this option:

- Global load balancing and backbone site connectivity streamlines the failover and data synchronization processes.
- RTO and RPO will depend on the particular architectures and methods of synchronization.

### Levels of RIM Service Available

As different systems within a purchasing entity's environment may require different levels of support, NTT DATA's RIM services are available in three levels on a server by server basis, depending on how much technology in a system must be monitored, managed, or administered. Pricing is different by level; customers can decide the solution that makes the most sense to them.

NTT DATA offers three levels of RIM support—bronze, silver, and gold—for equipment. The equipment we support with RIM can be located in one of our data centers, in a client data center, or in the NTT DATA virtual private cloud environment. This provides a cost-effective way of providing support, depending on the criticality of the equipment in question:

- **Bronze Support** includes 24x7 monitoring of devices with notification of alerts. Bronze support is suitable for network and other connectivity devices and non-critical servers such those in development environments.



- **Silver Support** includes device monitoring as well as ITIL-managed service support covering the operating system. Silver support is suitable for test and non-mission critical production servers.
- **Gold Support** includes device and operating system monitoring as well as ITIL-managed service support covering applications for mission critical production servers. Gold support is suitable for mission-critical production servers.

All gold, silver and bronze services include 24x7 service desk support, reachable by telephone, email, or over the web.

Exhibit 52 offers more detail on the services included in each service tier.

Exhibit 52. RIM Service Levels

Level of Service		Bronze	Silver	Gold
Client Support	24x7 Monitoring			
	24x7 Notification			
Incident Reporting	Phone Call			
	E-mail			
	Web Access			
Availability	Node Up/Down			
	Interface Up/Down			
	OS Processes			
	Application Processes			
	OS File Systems			
	Application File Systems			
	OS Log Files			
	Application Log Files			
Performance	OS Processes			
	Application Processes			
	OS File Systems			
	Application File Systems			
	CPU			
	Memory			
	Interface			
	Application Transactions (up to 3 Avail. Trans.)			
Security	Failed Logins			
	Login Violations			
Log File Criteria	3 OS Log Files and up to 3 Criteria			
	Up to 2 App Log Files and up to 3 Criteria			
Integration	Script Integration (up to 3 Scripts)			
Custom	Application Script (1 Script)			
SNMP	SNMP Traps (up to 10 Traps)			
Reporting	Canned			
	Ad-hoc (up to 3 reports)			
	Custom (up to 1 report)			

**Near/Off Shore**

- Service Desk
- ITSM Tools
- Remote Infrastructure Management

**Service Desk**

- » Single Point of Contact
- » 24x7x365 Client Support
- » L1/L2 Support
- » Service Request
- » Self Service
- » Incident Management
- » Multi-shore Model
- » Multi-channel Services
- » Knowledge Management Services

**Remote Infrastructure Management**

- » 24x7x365 Operations Support
- » Auto Ticketing
- » Auto Notification and Escalation
- » Proactive Monitoring and Alerting
- » Self Healing
- » Root Cause Analysis
- » Trouble Shooting and Resolution
- » Problem Management
- » Network and Security Configuration
- » System Configuration and Maintenance
- » Storage Configuration and Maintenance
- » System/Data Backup and Restore
- » Configuration Management Systems
- » User Administration
- » Security Auditing
- » Task Automation
- » Canned/Adhoc Reporting

UtahCloud1611

By offering services tiered into bronze, silver and gold levels, our clients can match the services they need to their specific technical and financial requirements.

## 6.20 Marketing Plan (RFP §8.20)

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

## Overview

NTT DATA works with a variety of state agencies, some of them participants in NASPO. Our growth and work in these agencies is the result of a combination of key wins and smart investments in an experienced and talented sales and management team as well as a dedicated, professional support operations team. NTT DATA will leverage these teams to promote support for this contract

Specifically, our plan is to establish a marketing campaign to promote the contract to participating agencies, much the same way we would if rolling out a new solution or service of our own creation. To establish and run a marketing campaign, we will:

- Identify prospects
- Establish a marketing communication plan
- Produce campaign materials
- Execute the marketing communication plan
- Measure results

We will review each of these steps in the rest of this section. Put simply, NTT DATA is a global company with the experience, resources, and processes to ensure a successful campaign for cloud services.

## Identifying Prospects

If contact information for potential targets is not already available from NASPO, we will capture that information from internal existing contact details and other publically available sources and store it in a campaign folder in NTT DATA's customer relationship management system. By establishing a campaign, we enable a variety of features that we can use for connecting with prospects, who will likely be participating agency decision makers.

## Establishing a Marketing Communication Plan

After identifying prospects for this contract, NTT DATA will determine how best to communicate the right message to them. At this time, we anticipate two key approaches for promoting this contract.

First, NTT DATA will create an outreach communication using email or outbound telephone calls to alert prospects to the availability of the contract. In these communications, we will educate prospects on the importance of cloud services in government agencies and share ongoing results of the program. For example, once quarterly cost savings reports are available, we would be able to share summary data after removing any sensitive information. By sharing information about the program, our goal would be to gain interest and acceptance from prospects that simply do not know much about it.

In addition, NTT DATA will prepare a brochure with content that is similar to our outreach communications and provide this brochure to our sales teams. These sales teams will contact prospects directly to discuss the contents of the brochure and seek to gain commitment for participation.

Depending on how these efforts pan out, NTT DATA could deploy other strategies as well. For example, we could produce an informational website or webinars to supplement these other promotional efforts. We would make a decision on whether or not to invest in these additional marketing channels once the initial campaign efforts are executed and measured.



### **Producing Campaign Materials**

Once we have established a marketing communication plan, NTT DATA will make use of our marketing operations team to produce the required materials. This team includes graphic artists and technical writers with a history of producing quality materials.

### **Executing a Marketing Communication Plan**

Once our marketing operations team has produced the materials we need for the marketing campaign, we will distribute them. At this point, we will begin to execute and measure the campaign.

### **Measuring Results**

On a quarterly basis, NTT DATA will review the results of the campaign and plan activities for the following quarter, improving our efforts as part of an iterative process.

## **6.21 Related Value-Added Services To Cloud Solutions (RFP §8.21)**

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.

### **Introduction**

NTT DATA is a full service provider of IT services that range from Application development, maintenance and outsourcing through configuration and installation of enterprise packages such as SAP and Oracle through Cloud services. NTT DATA's portfolio of Cloud Services have been developed and structured with the intent of helping our customers:

- Drive fast results
- Optimize the complete environment
- Provide flexibility to embrace growth

Our value-added services provide support before during and after migration into our cloud environment.

### **Cloud Advisory Services**

Assessment and transformational services are focused on helping our clients define or refine their cloud computing vision, architecture, and roadmap. NTT DATA cloud service professionals are experts in cloud computing, providing neutral-party advice and using our rich heritage to plan the transition of your IT environment.

With our cloud advisory services, NTT DATA partners with clients to strategize and architect their cloud transformation, using our deep cloud expertise and vertical industry knowledge. Following our Enterprise Transformation Framework<sup>SM</sup>, we assure that our clients understand the full impact of adopting the cloud, including process, organization, capability, technology, governance, and strategy and culture. Our services enable clients to plan for the transition of infrastructure, applications, and business services to the cloud. We provide vendor-agnostic assessment and transformational services focused on helping our clients define or refine their cloud computing vision, architecture, and roadmap. We align business goals and objectives to the right cloud strategy and providers. The Cloud Advisory Services portfolio consists of two offerings: Cloud Defogger<sup>SM</sup> and Cloud Direct<sup>SM</sup>.

**Cloud Defogger.** Cloud DeFogger offers two types of short client engagements:

- **Cloud Discovery Workshop** – A customizable 1-day executive session provides a clear, high-level view of cloud benefits for the delivery of services to the business, leveraging market data pertinent to the client's industry vertical and size. This workshop answers the question "Why should I consider the cloud?"
- **Cloud Clarity Workshop** – A 2–3 week consulting engagement assesses key elements or requirements of a client's enterprise services portfolio and impact to moving those services to the cloud, assessing their current cloud service characteristics and/or selecting the appropriate cloud solution.

**Cloud Direct.** Cloud Direct encompasses two detailed client engagements:

- **Cloud Business Services Assessment** – A 6–10 week assessment that provides a comprehensive view into all aspects of cloud migration. Includes a detailed review of client's business application and infrastructure environments and a readiness assessment across key areas: strategy, operations, architecture, security, resources, and cost/benefit analysis. This assessment answers the question "What do I put in to the cloud?"
- **Cloud Strategy Roadmap** – A 4–8 week strategy development engagement that substantiates the return on investment (ROI) impact of cloud migration and delivers a customized roadmap that prescribes the technology, process, partners, and organization model required for a successful cloud transition and outlines the cloud migration journey. This engagement answers the question "When and how do I execute my cloud strategy?"

### **Cloud Infrastructure Services**

NTT DATA provides turnkey integrated operational management and support for public, private and hybrid cloud environments that reduces complexity and cost with a single point of accountability and drives consistent service levels with proactive service delivery and continuous improvement.

With cloud infrastructure services, NTT DATA offers comprehensive cloud infrastructure services for all client workloads and requirements. We perform infrastructure consulting, migration, ongoing management and hosting services for both cloud and non-cloud workloads. The cloud infrastructure services portfolio consists of the following offerings:

- **Infrastructure Consulting Services** – Helps in cutting data center costs, typically the most expensive area of the client's infrastructure, while assuring business continuity by rationalizing, consolidating, and pruning servers, applications, and on-premise data centers. Services include data center rationalization, virtualization, planning and implementation, infrastructure assessment, and disaster recovery and business continuity services.
- **Cloud Infrastructure Migration Services** – We help clients migrate from a traditional on-premise infrastructure to a public, private, and/or hybrid cloud environment to access new business processes quickly and cost-effectively.
- **Cloud Infrastructure Installation Services** – We help clients to install the physical and virtual assets they need to operate within our cloud environment. Installation effort and cost depend on the number of assets deployed.
- **Cloud Infrastructure Management Services** – Our 24x7 remote cloud infrastructure management services are delivered through an NTT DATA-owned, secure, global business systems operating framework. Services include monitoring and management of cloud infrastructure (network, security, server, database, storage, messaging, and unified communication infrastructure). All supported by our cloud Service Operations Center, which

reduces the cost and complexity of service management with a single point of accountability. Our cloud Service Operations Center follows IT Infrastructure Library (ITIL, 2011 edition) best practices and provides horizontal level 1 support, functional level 2+ support, and full-service infrastructure support.

- **A Service Operations Center** – Our Service Operations Center is an integrated IT service management offering that reduces complexity and cost with a single point of accountability for consistent service levels and predictive outcomes.

## 6.22 Supporting Infrastructure (RFP §8.22)

### 6.22.1 Infrastructure Requirements

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

Assuming that a purchasing entity already has commonly available WAN equipment, they will only have to acquire redundant connectivity to our production site in Ashburn, Virginia, with failover to our DR facility in Sacramento in the event of loss of Ashburn. This connectivity can be implemented in several ways:

- **NTT DATA-provided VPN.** This includes small setup fees and monthly charges.
- **A purchasing entity-purchased direct connection.** This requires setup and monthly charges for cross connect and cabling.
- **A purchasing entity-purchased MPLS connection.** This requires setup and monthly charges for cross connect and cabling.

There is also a charge for client Internet traffic into and out of the cloud.

If colocation is required in addition to cloud services, additional infrastructure may be necessary and will be specified during the design phase. Installation and recurring costs will be paid by the purchasing entity.

Costs for these services are detailed in our cost proposal.

### 6.22.2 Installation of New Infrastructure

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

Building out cloud infrastructure requires installation and recurring costs, which we have detailed in our accompanying cost proposal. There is no charge for self-service setup of virtual resources (servers and storage).

## 6.23 Alignment of Cloud Computing Reference Architecture (RFP §8.23)

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

### Overview

The architecture of NTT DATA's cloud offering compares closely to the NIST Cloud Computing Reference Architecture. That close comparison is evident in NTT DATA's answers, above, to

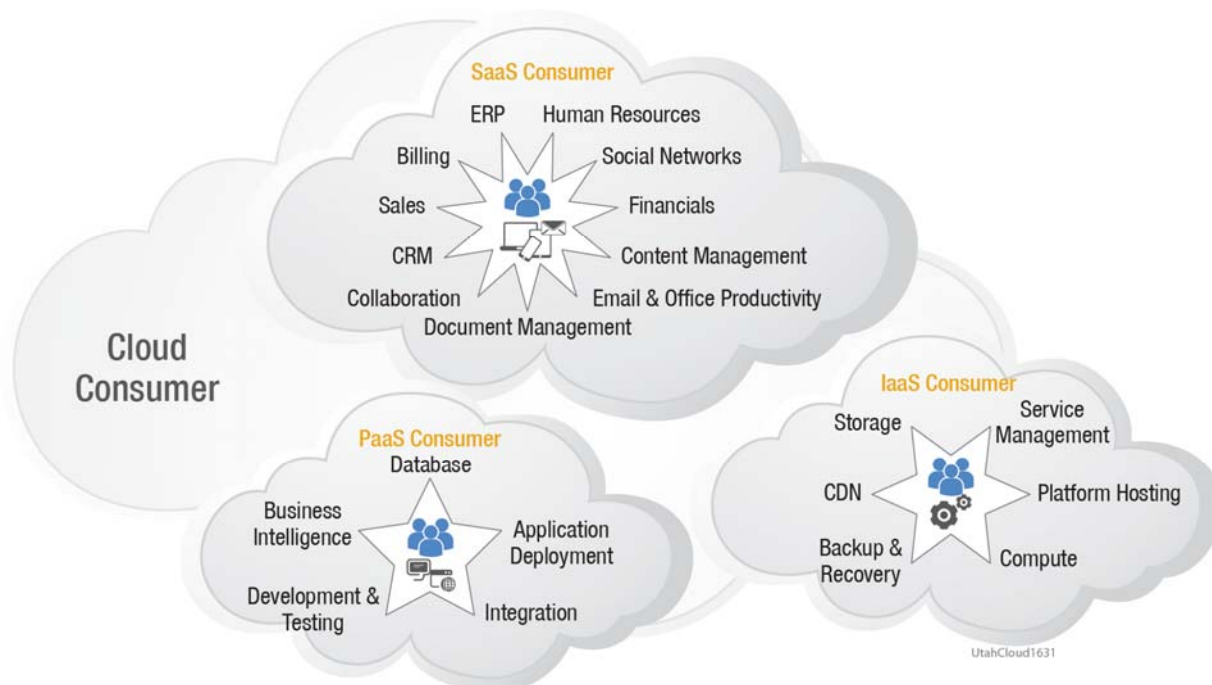
the questions contained in the RFP. We can further clarify this by examining several figures in the NIST reference architecture document, including:

- **IaaS domain**, particularly in reference to Exhibit 53, which contains examples of services available to a cloud consumer
- **Services Provided**, particularly in reference to Exhibit 54, concerning cloud services management

### IaaS Domain

The NIST Reference Architecture illustrates the three service models.

Exhibit 53. NIST Reference Architecture



*This exhibit summarizes some of the typical services available to cloud consumers, according to the NIST Reference Architecture.*

NTT DATA provides the following listed IaaS Cloud services. Further details of these services are included in our response to previous questions in the RFP, particularly in our response at the beginning of Section 6 (Technical Response) as well as our response to Question 8.19.2, in Section 6.19 (Integration and Customization).

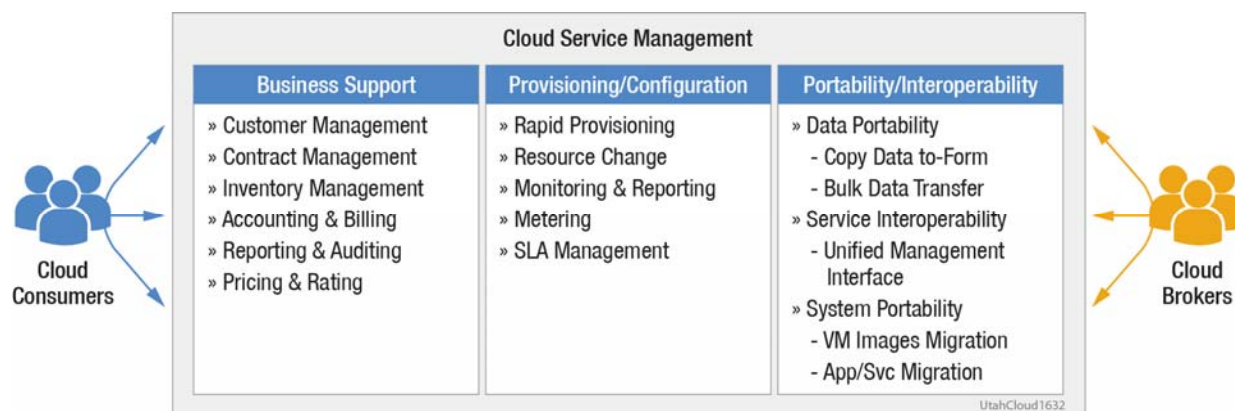
- **Compute.** NTT DATA provides Windows, Linux, AIX and iSeries compute resources drawn from our pools hosted on V+C+E and Power 7 systems.
- **Storage.** NTT DATA provides a pool of storage compute resources drawn from our pool hosted on our SAN containing EMC Enterprise storage frames
- **Backup & Recovery.** We provide Backup & Recovery services through our Avamar/Data Domain infrastructure with automatic replication of backups to our DR site. We also provide Zerto-based disaster recovery from replicated data. See also our responses to 8.8.1 and 8.8.2 in Section 6.8 (Service or Data recovery).

- **Services Management.** NTT DATA provides Service Management capability through our BMC toolset that allows clients to monitor and manage infrastructure performance and capacity. We offer such service in three levels – bronze, silver and gold depending on the level in the technology stack of management required.
- **Platform Services.** Services for managing platforms running within our VPC are available for infrastructure directly through our Service Operations Center. For other platforms, NTT DATA has over 50 years of experience managing a wide variety of technologies and can provide platform management services for from large scale systems such as packaged platforms like SAP, PeopleSoft and Oracle EBS to unique software applications.
- **Content Delivery.** NTT DATA assumes content delivery services will be available through the Cloud Carrier. We recommend that our clients contact bandwidth service providers for connectivity to our site and for CDN services.

### Services Provided

The NIST Reference Architecture provides a high level illustration of cloud service management. This includes all of the cloud services-related management functions that are necessary for the management and operation of those services required by or proposed to cloud consumers.

Exhibit 54. Cloud Service Management



*This exhibit summarizes the forms of cloud service management in the NIST Reference Architecture.*

For example:

- **Business Support** – At NTT DATA, we provide business support through our contract manager, our contracts administrator, and the administrative tools that support them.
- **Provisioning and Configuration.** At NTT DATA:
  - We provide tools to our clients to enable rapid self-provisioning of services. For more details, see the information we provided in Section 6.14 (Service Provisioning) and 6.17 (Hosting and Provisioning). We also follow the robust ITIL-based change management process that we described in our answer to Question 8.14.1 in Section 6.14 (Service Provisioning). This process helps see to it that resource changes are minimally disruptive.

- We provide tools for monitoring system performance and reporting results, as we described in our response to Question 8.17.2, in Section 6.17 (Hosting and Provisioning).
- Our Cloud Cruiser provides metering services at the department level or even at an individual level. For more information, see our response to Question 6.5.1 and the file we submitted separately, named "6.5.1 Cloud Cruiser Overview.pdf".
- We manage SLAs using the BMC tool suite, as we described in Section 6.10 (Service Level Agreements).
- **Portability and Interoperability.** At NTT DATA:
  - Clients have administrative rights to data files and they can copy data to or from the environment whenever desired.
  - NTT DATA's BMC toolset provides the ability to support unified management Interfaces through eboning features that allow sharing of tickets and performance information between management systems. For more information about service interoperability, see our response to Question 8.19.1 in Section 6.19 (Integration and Customization).
  - System images can be transferred directly to other clouds based on the VMWare architecture. Alternatively, images can be exported (or imported) using the industry standard OVF format. For more information, see our response to Question 8.7.1 in Section 6.7 (Migration and Redeployment).

## 7. Confidential, Protected or Proprietary Information

---

REDACTED.



## **8. Exceptions and/or Additions to the Standard Terms and Conditions**

---

We have provided a redlined version of Attachment A of your RFP to the Bidsync site as a separate attachment which is part of our submission. The name of this file is "NASPO Attachment A - Master Agreement Terms and Conditions – Marked by NTT DATA".

We have also provided a redlined version of Exhibit 3, which supplements RFP Attachment A. The name of this file is "NASPO Exhibit 3 to Attachment A - Infrastructure-as-a-Service – Marked by NTT DATA".

## **9. Cost Proposal**

---

As per the instructions in your RFP, we have submitted our cost proposal separately.

## Appendix 1 Overview of Transition Process

### Overview of Transition Approach

NTT DATA differentiates itself from competitors by treating transitions as a specialized activity requiring specialized skills. It is our practice to assign a dedicated and experienced transition manager from NTT DATA's Transition Services Group (TSG). TSG is a group of highly experienced IT managers who have managed ~70 transitions over the last several years, with a total contract value of more than \$1.6B. Over the course of these transitions, NTT DATA has not incurred a single financial penalty for missing a transition milestone, which immediately translates into reduced risk for a purchasing entity. Having a dedicated team ensures that NTT DATA is able to apply best practices and lessons learned to every transition effort and allows the engagement manager to focus on managing service delivery and establishing a long-term partnership with our clients.

The following Exhibit depicts the high-level approach NTT DATA would take for transitioning the services for a purchasing entity, including phases, major activities and deliverables.

Exhibit 55. High-level Transition Approach

Phase	Transition Planning	Transition In				Service Delivery and Improvement
		Knowledge Acquisition	Process and Staff Integration	Engagement Governance	Project Management	
Activity	<ul style="list-style-type: none"> <li>» Complete due diligence</li> <li>» Conduct stakeholder impact assessment</li> <li>» Ramp-up staff</li> <li>» Prepare for knowledge transfer</li> <li>» Establish network and infrastructure access</li> <li>» Logistics setup</li> <li>» Develop transition plan and KAP syllabus</li> </ul>	<ul style="list-style-type: none"> <li>» 4 Learning phases to acquire knowledge</li> <li>» Deliverables at end of each phase</li> <li>» Configure monitoring</li> <li>» Resolve tickets and perform productive work</li> </ul>	<ul style="list-style-type: none"> <li>» Acclimate to clients environment</li> <li>» Train staff on NTT DATA and client processes</li> <li>» Delivery procedures, handoffs, and templates</li> <li>» Implement work tracking tool for all in scope services</li> </ul>	<ul style="list-style-type: none"> <li>» Develop communication plan</li> <li>» Agree on service levels</li> <li>» Assess metrics tool to determine changes needed to support new model</li> <li>» Develop in-flight project assessment</li> <li>» Baseline and report service levels</li> </ul>	<ul style="list-style-type: none"> <li>» Structured management of the transition project</li> <li>» Issue management</li> <li>» Risk management</li> <li>» Status reporting</li> <li>» Status meetings</li> <li>» Delivery acceptance</li> </ul>	<ul style="list-style-type: none"> <li>» SLA achievement</li> <li>» Communication</li> <li>» Cross-training</li> <li>» Productivity improvement</li> <li>» Risk management</li> <li>» Relationship management</li> <li>» Future account planning</li> </ul>
	<ul style="list-style-type: none"> <li>» Detailed transition plan and risk plan</li> <li>» Agreed-on entry and exit criteria for each transition phase</li> </ul>	<ul style="list-style-type: none"> <li>» KAP population</li> <li>» Transfer of ownership plan</li> <li>» Readiness checklist</li> </ul>	<ul style="list-style-type: none"> <li>» Documented service delivery procedures (user manual)</li> <li>» Staff training plan</li> </ul>	<ul style="list-style-type: none"> <li>» Communication plan</li> <li>» SLA reports</li> <li>» Penvironment document</li> </ul>	<ul style="list-style-type: none"> <li>» Status reports</li> <li>» Risk plans</li> <li>» Issue logs</li> </ul>	<ul style="list-style-type: none"> <li>» Knowledge management system</li> <li>» Governance dashboard</li> <li>» Support and maintenance services</li> </ul>

UtahCloud1612

*NTT DATA's Transition-In Focuses on Knowledge Acquisition, Process and Staff Integration, Governance and Project Management*

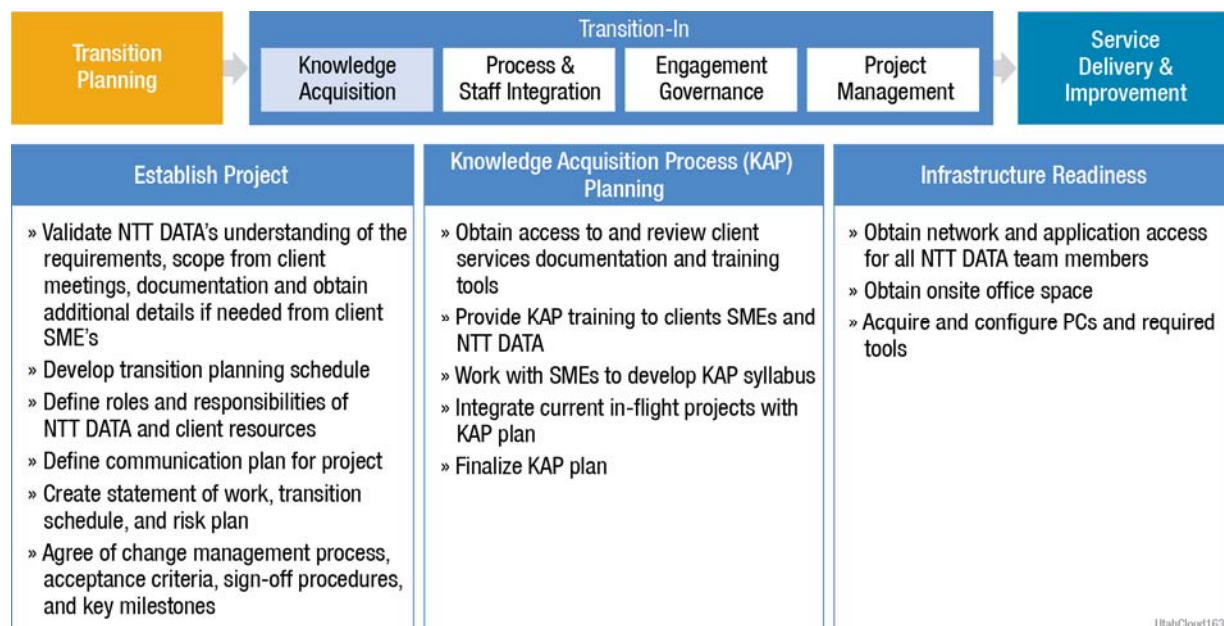
The key phases of NTT DATA's transition framework are detailed in the following sections.

### Transition Planning

Transition planning prior to any start of engagement or service to confirm that NTT DATA and the purchasing entity teams are adequately prepared to begin transition-in.

The primary activities and tasks of transition planning are shown in Exhibit 62.

Exhibit 56. Transition Planning Activities and Tasks



*This exhibit summarizes the planning activities and tasks associated with our approach to transition.*

An experienced NTT DATA Transition Manager will lead the transition planning phase, with assistance from the Delivery Managers and oversight from the Contract Manager.

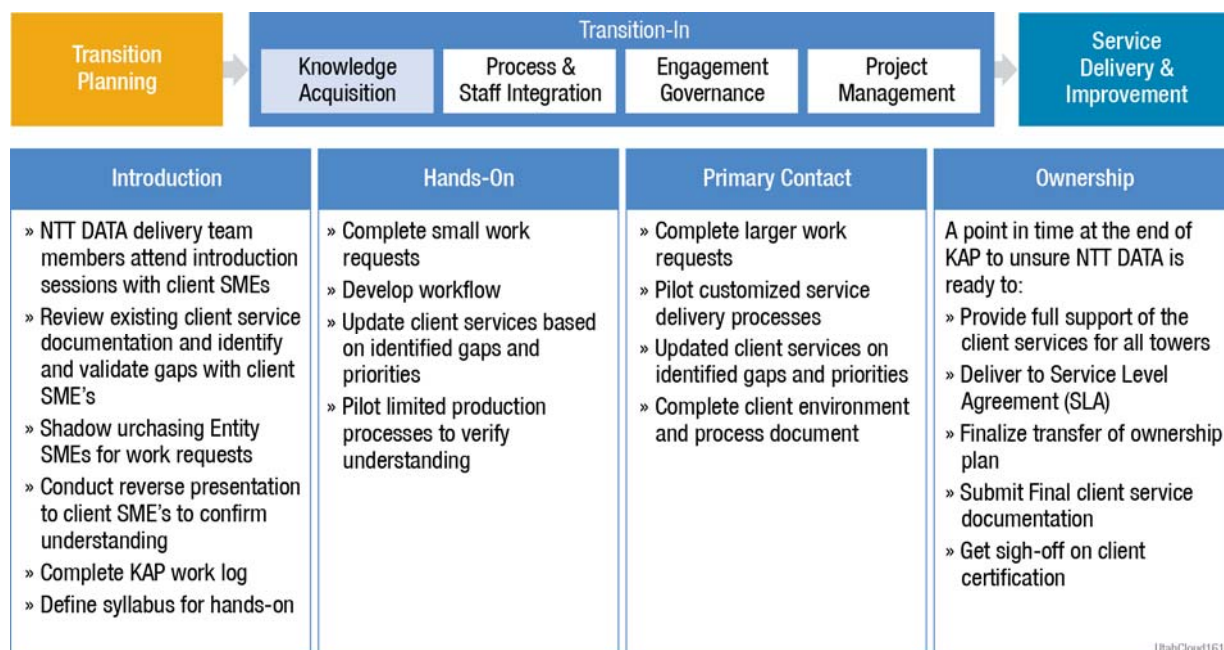
NTT DATA believes that the best way to transition services is to engage resources that will have an ownership interest in the long-term success of the engagement. As a result, NTT DATA strives to assign resources to the transition team who will have ultimate delivery responsibility, therefore building in an incentive to learn well and to establish a working relationship with the onsite client team. This practice has proved successful with our clients and has generated deep respect for individuals on both sides and allowed for quicker issue resolution when such need arises.

The NTT DATA transition manager will review current data and NTT DATA's proposal, meet with key contacts recommended by a purchasing entity, review purchasing entity existing support services and environments, and develop the transition-in project plan and knowledge acquisition process (KAP) plan. Another key activity is the establishment of connectivity between the purchasing entity and NTT DATA, and, if necessary, arranging for office space at the purchasing entity for key personnel.

### Knowledge Transfer

Exhibit 63 shows four stages of the KAP and representative tasks executed during each of these stages.

## Exhibit 57. Knowledge Acquisition Activities and Tasks



*This exhibit summarizes the activities and tasks associated with our knowledge acquisition process.*

The state of the documentation, complexity, and the size and stability of the technical components will determine the KAP approach and drive the priority of transition-in activities. These characteristics, along with SME availability and effective resource loading, will be used to determine the sequence and schedule of the application knowledge transfer.

KAP follows a documented and proven set of learning practices. NTT DATA resources will work closely with purchasing entity SMEs to gain business and technical knowledge, as well as observe and participate in the provision of support and enhancements. Critical activities in the KAP phase include:

- Decomposition of the support services into components such as logical groupings of systems, subsystems, programs, modules, or functions
- Review and validation of business processes and application environment
- Assigning NTT DATA team members to the framework components
- Rigorous on-the-job training activities to gain experience required to successfully maintain the applications

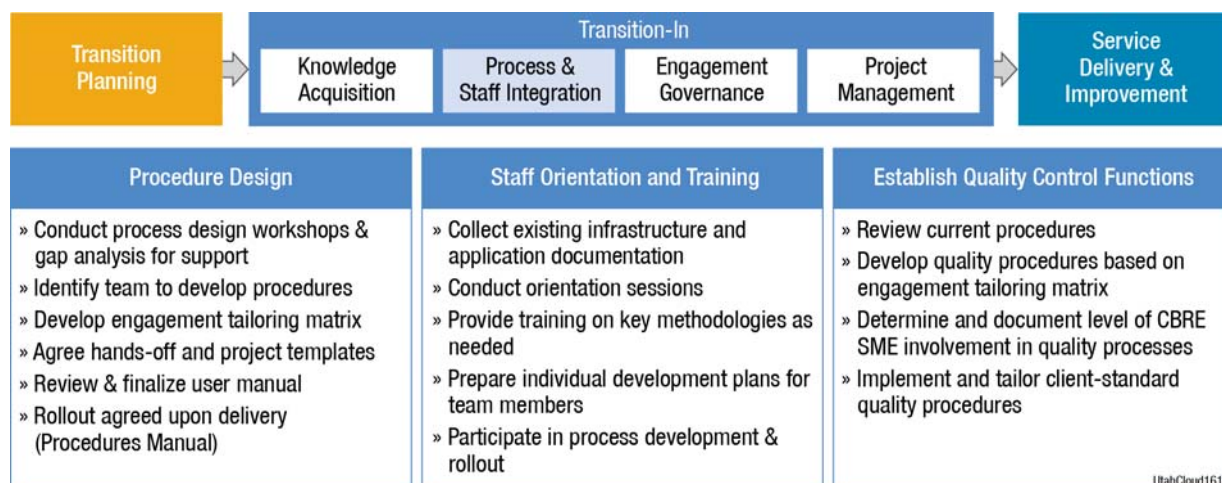
### Process and Staff Integration

Process and staff Integration includes procedure design, staff orientation and training, and quality control functions.

The following Exhibit depicts the activities and primary tasks performed for each.



Exhibit 58. Process and Staff Integration Activities and Tasks



*This exhibit shows the activities and tasks associated with NTT DATA's approach to process and staff integration.*

Building on data gathered during transition planning, NTT DATA will review the purchasing entity IT environment, business processes, system tools, and framework component inventories through structured meetings and data gathering activities. At the same time, NTT DATA will enable key NTT DATA and purchasing entity personnel to receive training in NTT DATA's project management disciplines and methodologies (if deemed appropriate) to confirm that NTT DATA's best practices are well understood and successfully integrated. The following is a 'starter list' of management processes which will be co-developed and approved as an outline for the final process and procedure documentation for each type of service:

- Application Support and Infrastructure Services
- Environments Staging – Procedures to Access
- Support Manual/Procedures
- Full Lifecycle of work tickets
- Change Management Procedures
- Escalation Procedures
- Deliverable Acceptance
- Testing process
- SLA Reporting
- Comprehensive Communication Plan
- Release Management Process & Procedures
- Process Flow of each Incident and Problem Type
- Business Process Services
- Standard Operating Procedures
- Sample process inputs and outputs

NTT DATA will work with purchasing entity resources to develop customized, repeatable processes for the engagement. NTT DATA and purchasing entity will also establish processes for collecting, reviewing, and responding to the metrics that will indicate the team's performance to service levels and areas of improvement. These processes are initiated during transition-in and used throughout the life of the engagement.

### Engagement Governance

At the overall engagement level, a master services agreement (MSA) between NTT DATA and purchasing entity will be the overarching contractual document. Upon award of this engagement, the to-be-developed project plan shall articulate additional governance elements specific to the specific requirements of this engagement. This section describes selected aspects of NTT DATA's governance approach. NTT DATA's engagement governance includes service level implementation, in-flight project integration, and organizational change management and governance. The following Exhibit depicts the activities and primary tasks performed for each.

Exhibit 59. Engagement Governance Activities and Tasks



*This exhibit summarizes NTT DATA's approach to engagement governance.*

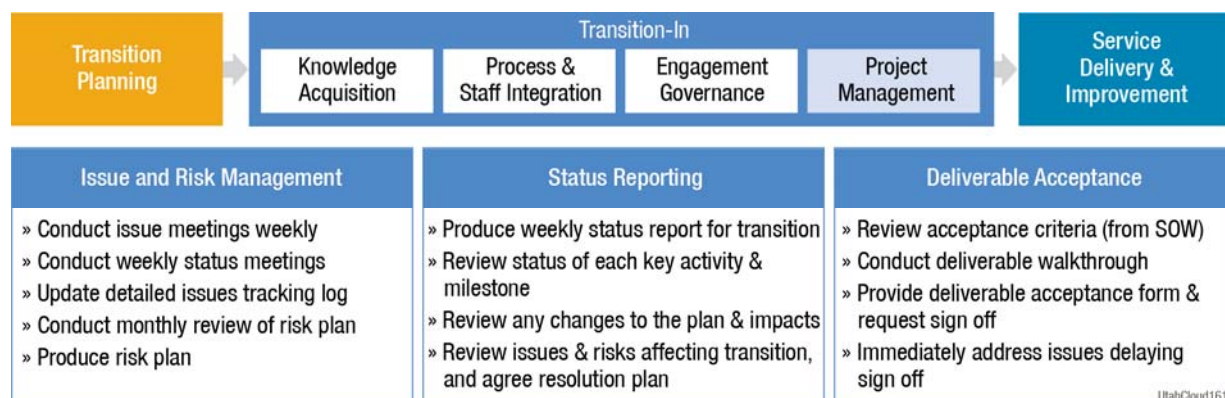
### Project Management Life Cycle Management (PMLC)

The PMLC aspect of transition-in includes issue and risk management, status reporting, and deliverable acceptance activities performed during the transition-in phase.

The following Exhibit depicts the activities and primary tasks performed for each.



## Exhibit 60. Project Management Life Cycle Activities and Tasks



*This exhibit summarizes the activities and tasks associated with NTT DATA's standard project management lifecycle.*

NTT DATA will apply its PMLC principles to the transition-in project, and manage the effort as for all NTT DATA projects. The application of these principles increases the success rate by minimizing differences in expectations and providing a basis for ongoing management of projects. The following Exhibit summarizes NTT DATA's project management details.

## Exhibit 61. Project Management Details

<b>Issue and Risk Management</b>	NTT DATA will actively identify, address, and resolve any issues that may impact the success of the transition-in project. Issue meetings with the transition team will be conducted daily during the early part of transition-in, and then reduced as the project progresses. In cases where issues need to be escalated, NTT DATA will do so immediately and track the issue through to completion. The same level of rigor will be applied to any risks that NTT DATA identifies during transition planning and throughout the duration of the transition-in project.
<b>Status Reporting</b>	NTT DATA will provide the purchasing entity with a weekly report detailing the status of the transition-in project. In addition, we will hold weekly status meetings with the appropriate purchasing entity management to confirm a clear understanding of how the project is progressing, changes in the purchasing entity environment are well understood, and any major issues and risks are jointly discussed at the management level.
<b>Deliverable Acceptance</b>	NTT DATA will actively work with the purchasing entity to jointly define the acceptance criteria for each transition-in deliverable, as well as the overall transition-in project. These acceptance criteria will be documented within the final transition-in statement of work, and re-visited during deliverable walkthroughs. This ensures there are no surprises over the course of the project, and the purchasing entity is completely satisfied with the deliverables and activities that occur during transition-in. In cases of delayed deliverable sign-off, NTT DATA will work with the purchasing entity to understand what is causing the delay, and address their concerns promptly.

## Transition-In Critical Success Factors

The following table summarizes the critical success factors during purchasing entity transition.

## Exhibit 62. Transition-In Critical Success Factors

<b>Continued Use of Infrastructure</b>	<ul style="list-style-type: none"> <li>• Provide capabilities for the NTT DATA team to be productive right away</li> <li>• Identify NTT DATA and current purchasing entity infrastructure resources to trouble shoot and resolve issues</li> <li>• Use the transition planning period to document access requirements for each resource supporting the transition project</li> </ul>
<b>Dedicated NTT DATA Transition Management Resources</b>	<ul style="list-style-type: none"> <li>• Clear role definition for client staff</li> <li>• Review and acceptance of project deliverables</li> <li>• Sponsorship of new delivery processes across business units</li> <li>• Project planning, tracking, and oversight</li> <li>• Issue escalation and resolution</li> <li>• Risk identification and management</li> </ul>
<b>SME Availability During KAP</b>	<ul style="list-style-type: none"> <li>• Joint prioritization of ongoing operations vs. transition activities</li> <li>• Identification of valuable activities to enable knowledge transition</li> <li>• Active participation in KAP activities</li> </ul>
<b>Effective and Frequent Communications</b>	<ul style="list-style-type: none"> <li>• Important for business stakeholders</li> <li>• Status meetings and quick issue resolution</li> <li>• Risk identification and management</li> </ul>
<b>Governance Model</b>	<ul style="list-style-type: none"> <li>• Clearly define how the purchasing entity and NTT DATA want this relationship to work</li> </ul>

## Transition Out Plan

NTT DATA's transition-out approach facilitates the planned transfer of knowledge and responsibilities to the target team while ensuring minimal disruption to business operations. A transition-out phase would include the following high-level knowledge transfer and project closure activity sets:

## Exhibit 63. Transition Out Plan

Phase	Objective
Verify scope and objectives	<ul style="list-style-type: none"> <li>• Timeframes, risks, and mitigation</li> <li>• Develop transition-out plan in accordance with the purchasing entity's objectives</li> </ul>
Assess infrastructure readiness	<ul style="list-style-type: none"> <li>• Undo any connectivity in place</li> <li>• Return hardware, software tools, and licenses</li> </ul>
Knowledge acquisition planning and execution	<ul style="list-style-type: none"> <li>• Ramp down resources</li> <li>• Determine the knowledge acquisition strategy (onsite, travel, electronic)</li> <li>• Prepare both purchasing entity and NTT DATA teams, and set expectations regarding roles and responsibilities</li> <li>• Integrate with existing service delivery requirements</li> </ul>
Provide engagement assets	<ul style="list-style-type: none"> <li>• Provide knowledge acquisition plan syllabus and work logs</li> <li>• Provide application documents, client environment document, procedures manual, and quality control processes</li> <li>• Provide project assets</li> </ul>

## Appendix 2 Details of Migration Methodology

---

A high level description of our Migration Methodology can be found in our response to Question 8.3.7. NTT DATA has extensive experience in migrating systems as part of service transition and the description below provides further details of the steps of the process.

### Phase 1: Plan

#### Overview

In this first phase, we will establish project objectives and document your current data center environment, identify your requirements and validate opportunities for data center migration.

**Establish Project Objectives.** This step will help us refine and communicate the objectives, scope, and logistics of this project to all stakeholders. We will:

- Identify project stake holders
- Develop a project charter, a project plan, an interviewee list, and an invitation to the kick-off meeting for the project stakeholders.
- Prepare and finalize an approach to interviews and questionnaires
- Organize project logistics such as office space and telephone extensions
- Identify roles and responsibilities and dates for interviews and any workshops
- Schedule a project kick-off meeting with key project stakeholders to launch this project. Attendees should include purchasing entity staff, key IT representatives, and other individuals, and anyone else who can provide information or contribute to the discussions.
- Identify business goals and validate priorities

**Document the Current Data Center Environment.** In this step, we will develop an understanding of your current state and your goals for migrating into the proposed data center and environment. We will assess the state of your current environment, and gain a better understanding of your application priorities, your logical and physical groupings, and your availability requirements. This current state assessment will cover the entire technology stack, including facilities, networks, server platforms, and the application landscape. It will include IT service management processes as well as your organization and governance structure.

As part of this step we will:

- Interview purchasing entity personnel and also use tools such as pre-populated spreadsheets, Access databases and automated discovery tools such as BMC Atrium to gather, store and analyze data about the environment
- Review an inventory of all hardware, software, utilities and applications, and evaluate all current purchasing entity equipment at any existing data center sites.
- Collect and report on best practices concerning performance and utilization
- Document a physical assessment of servers, storage, and back-up equipment.
- Document wide area network (WAN) and site-to-site connectivity as well as network dependencies of Internet and intranet communications
- Capture and generate software configuration details for the installed systems through hands-on access to each system

- Identify and make recommendations on potential and viable cost savings that can be realized through the salvage of any infrastructure equipment
- Identify initial application cluster groupings

### **Identify Requirements and Validate Opportunities for Data Center Migration**

#### **Hosting and Co-location Data Center Requirements**

The information collected in this activity focuses primarily on the underlying business needs not being met by the current data center infrastructure and facility. It assesses the concerns and constraints of those who use, administer, and manage the data center infrastructure.

Finally, this activity involves obtaining an overview of existing investments and assets in the current data center environment at the enterprise level. The tasks to be performed by the team are:

- Determine operational needs, agree on key metrics based on business needs and industry best practices
- Create application inventory and map to servers and governing organizations
- Prepare utilization outline including performance and capacity
- Evaluate current server environment, such as, shared storage and common application workloads

#### **Identify Future Hosting and/or Co-location Data Center Environment**

This activity involves working with the purchasing entity to develop a “collaboration statement of transformational direction” that addresses the stated strategic goals, given the specific business and technical challenges it faces. Developing the future data center environment requires addressing the business directions of the purchasing entity as stated with recommendations across the infrastructure dimensions (infrastructure architecture, data center facilities, data center operations, the data center service organization).

The tasks to be performed by the team are:

- Determine operational needs for servers, applications, storage, back-up, restore and network throughput
- Determine migration and retirement options and identify, validate and prioritize storage and consolidation opportunities based upon the potential return on investment and the importance to your operations.
- Recommend any new servers, storage, back-up and restore equipment
- Recommend any new routers and new end points
- Recommend new operational and/or disaster recovery (DR) strategies
- Conduct validation workshops: The team will conduct workshop sessions with individuals from purchasing entity IT, and business to stress test the future state environment. This process will help validate the Future State and obtain buy-in from stakeholders

#### **Develop Hosting or Co-location Services Migration Strategy**

Developing a purchasing entity migration strategy involves identifying the best set of recommendations from among a set of viable alternatives. It involves synthesizing recommendations to:

- Provide best methods/leading practices for migration planning and provide a critical path/project phase schedule
- Develop wide area network (WAN) schedule and plan to coordinate the WAN connection changes
- Develop migration roadmap from cluster groupings of similar apps with sequencing and timing criteria
- Develop Migration/Virtualization Roadmap
- Develop operational risk plan for the migration strategy
- Recommend preferred methods and realistic expectations regarding lead time required from date of “cage ready” prior to completing the last phase of the migration

### Phase 1: Deliverables

The below Exhibit summarizes the deliverables we will produce as part of this planning phase.

Exhibit 64. Planning Phase Deliverables

<b>Establish Project Objectives</b>	<p>In this step, we will deliver:</p> <ul style="list-style-type: none"> <li>• A project charter</li> <li>• A work plan and schedule</li> <li>• A document that describes roles and responsibilities</li> </ul>
<b>Document Current Data Center Environments</b>	<p>We will produce a current data center environment report. This report will provide an overview of the purchasing entity's current data center environments. Depending on final project requirements, the report may include a discussion of:</p> <ul style="list-style-type: none"> <li>• Detailed migration and requirements for application priority and availability</li> <li>• Application-to-server, network, storage and database mapping</li> <li>• Applications interdependency</li> <li>• Applications usage</li> <li>• Current network deployment</li> <li>• Network assessment and gaps</li> <li>• Server inventory list</li> <li>• A security assessment</li> </ul>
<b>Identify Requirements and Validate Opportunities for Data Center Migration</b>	<p>We will develop a migration strategy that includes the following deliverables:</p> <ul style="list-style-type: none"> <li>• An analysis of requirements</li> <li>• A consolidation strategy and a guiding principles report that includes specific application groupings and sequencing</li> <li>• An application inventory mapped to servers and grouped by functionality (cluster groupings).</li> <li>• A consolidation architecture report, including a consolidation roadmap.</li> <li>• A mitigation analysis, including a virtualization roadmap</li> </ul>

### Phase 2: Design

#### Complete Detailed Design

Engineer Final Design – This design activity uses input from the current state assessment, future-state analysis, and hosting /co-location data center strategy and migration planning activities to help develop a detailed design for hosting /co-location and managed services. NTT DATA's best and leading practices are integrated into this design to help the purchasing entity

improve operations and reduce management costs by customizing architecture to meet your specific requirements. The activities to be performed by the team in this step are:

- Create detailed server and storage /backup/network target architecture
- Map applications to newly designed server farms
- Prepare comprehensive risk management plans
- Determine migration and retirement options of non-strategic assets

Work with existing and new vendors accordingly to develop target architectures

- Develop final design
- Prepare migration, contingency, operational infrastructure plans

### **Review of the New Co-location Facility Physical Design**

Next, if colocation is required, NTT DATA will assess the physical design of the purchasing entity's proposed hosting/co-location facility space. This assessment analyzes the floor plan and cabling system. After these factors are analyzed, the facility assessment will provide floor plan recommendations that can improve the layout of the new purchasing entity space and offer greater accessibility to higher-density infrastructure, and recommendations to help simplify power and network cabling.

Specifically, we will help you:

- Decide on the placement of equipment within racks and the rack placement within the co-location facility.
- Perform infrastructure mapping, tracking, and labeling of data paths from servers to switches and identify the proper lengths of the cables needed
- Develop a cable management and cable tray configuration based on a rack layout that meets our own standards

### **Deliverables**

As part of this design phase, we will create a Migration Design which includes the following components:

- Detailed hosting or co-location data center infrastructure design
- Technical architecture definition
- High-level migration plan with risk/fallback strategy
- Disaster recovery facility assessment
- Floor plan recommendation report
- Cabling assessment and recommendations
- Power and cooling recommendations

### **Phase 3: Build**

#### **New Hosting or Co-location Data Center Implementation**

The build phase includes the implementation of the purchasing entity's hosting or co-location data center design. This phase is carried out in an iterative manner to help assure achievement of continuous realizable benefits throughout the hosting or co-location data center services project. The activities to be performed by the team in this step are:



- Update/maintain implementation plan (provide critical path/project phase schedule: purchasing entity staff will be available to work with NTT DATA onsite during after-hours and weekends, especially during the actual migration)
- Coordinate Wide Area Network (WAN) changes with purchasing entity staff
- Assist with managing the movement and installation of data center Internet/intranet communications equipment. (This includes conferring with purchasing entity data communications staff on data center site-to-site connectivity, network dependencies, network design, and implementation services)
- Begin setup of the environment at both the primary and secondary DR data center.
- Begin testing.

### **Deliverables**

#### **New Hosting/Co-location Data Center Implementation**

The build phase provides the following deliverables:

- Updated detailed design
- Updated migration plan with risk/fallback strategy

#### **Phase 4: Deploy**

##### **Final Production Cut-over**

The Deploy phase includes assistance with the final production cut-over to the new purchasing entity hosting or co-location data center. The activities to be performed by the team in this step are:

- Support short user acceptance testing or system functionality verification before the production cut over
- Complete testing and move to the go live stage
- Monitor and validate the production cut-over of servers
- Update documentation
- Disaster recovery testing

### **Deliverables**

#### **Final Production Acceptance**

The co-location data center deployment activity provides the following deliverables:

- Environment accepted
- Sign-off document

#### **Phase 5: Operations**

##### **Operational Support Services**

NTT DATA's Service Operation Center provides IT Infrastructure Library (ITIL)-based management and support services across all computer platforms. Armed with market leading monitoring and management tools, our team of experts proactively supports and optimizes the management of your IT assets and transactions under the ITIL best practices framework and enforced by an SLA, enabling the purchasing entity to:

- Get the cost-saving benefits of the cloud plus best-practice IT management
- Simplify and consolidate management across cloud and non-cloud systems
- Ensure consistent performance and uptime 24x7
- Comprehensive IT service management

Whether you migrate some or all of your IT operations, NTT DATA gives the purchasing entity an opportunity to consolidate IT service management across all investments, from SaaS solutions to traditional applications, and from infrastructure to networks. We take a holistic, proactive approach to service management to ensure the highest levels of IT performance and service quality.

With NTT DATA's proactive approach to IT service management, we can detect and solve a large percentage of all incidents before they affect users or business operations. Other benefits include:

- A single point of accountability managing all service desk functions and infrastructure support
- Seamless management of traditional applications and infrastructure for improved visibility, consistent support, and better business performance
- Process improvement and tool innovation that streamline issue resolution
- A global, extended team providing 24x7 coverage

## Appendix 3 D&B Report



Printed By: Tamarai Selvan  
Date Printed: February 10, 2016

Live Report : NTT DATA, INC.

D-U-N-S® Number: 07-170-7764

Trade Names: (SUBSIDIARY OF NTT DATA INTERNATIONAL L.L.C., NEW YORK, NY)

Endorsement/Billing Reference: Tamarai.selvan@nttdata.com

D&B Address		Added to Portfolio: 12/30/2014	
<b>Address</b>	5601 Granite Pkwy Ste 1000 Plano, TX, US - 75024	<b>Location Type</b>	Headquarters (Subsidiary)
<b>Phone</b>	800 745-3263	<b>Web</b>	www.nttdata.com/americas
<b>Fax</b>		<b>Last View Date:</b>	01/26/2016
		<b>Endorsement :</b>	Tamarai.selvan@nttdata.com

### Company Summary

Currency: Shown in USD unless otherwise indicated

#### Score Bar

<b>PAYDEX®</b>		<b>77</b>	Paying 5 days past due
<b>Commercial Credit Score Percentile</b>		<b>77</b>	Low to Moderate Risk of severe payment delinquency.
<b>Financial Stress Score National Percentile</b>		<b>32</b>	Moderate to High Risk of severe financial stress.
<b>D&amp;B Viability Rating</b>	<div> <div>4</div> <div>5</div> <div>B</div> <div>Z</div> </div>		View More Details
<b>Bankruptcy Found</b>	<b>No</b>		
<b>D&amp;B Rating</b>	<b>--</b>		Unavailable.

#### Detailed Trade Risk Insight™

Days Beyond Terms Past 3 Months

**6**  
Days

Dollar-weighted average of **41** payment experiences reported from **26** Companies

##### Recent Derogatory Events

	Dec-15	Jan-16	Feb-16
Placed for Collection	-	-	-
Bad Debt Written Off	-	-	-




#### News & Alerts

Alert Type	Date	Actions
------------	------	---------

#### D&B Viability Rating

<b>4</b>	<b>Viability Score: 4</b>
<b>5</b>	<b>Portfolio Comparison: 5</b>
<b>B</b>	<b>Data Depth Indicator: B</b>
<b>Z</b>	<b>Company Profile: Z</b> Subsidiary

#### D&B Company Overview

 Financial Stress Score Class	02/07/2016	<a href="#">View</a>
Litigation	01/28/2016	<a href="#">View</a>
 Financial Stress Score Class	01/26/2016	<a href="#">View</a>
 Commercial Credit Score Class	01/17/2016	<a href="#">View</a>

In the last 30 days, 4 alerts were generated for this company.

This is a headquarters (subsidiary) location

Branch(es) or Division(s) exist Y	
Chief Executive	JOHN W MCCAIN, CEO-PRES
Year Started	1967
Management Control	1986
Employees	200 (199 Here)
SIC	7373 , 7372
Line of business	Computer systems design, prepackaged software svc, computer related svcs
NAICS	541512
History Status	CLEAR

#### FirstRain Company News




**SAP® SuccessFactors® Performance & Goals**  
2016-02-08T11:36:15 EST 11:36 AM-

Powered by FirstRain

#### Public Filings

The following data includes both open and closed filings found in D&B's database on this company.

Record Type	Number of Records	Most Recent Filing Date
Bankruptcies	0	-
Judgments	0	-
Liens	1	02/06/15
Suits	0	-
UCCs	1	11/10/14

The public record items contained herein may have been paid, terminated, vacated or released prior to today's date.

## Corporate Linkage

### Global Ultimate

Company	City , Country	D-U-N-S® NUMBER
NIPPON TELEGRAPH AND TELEPHONE CORPORATION	CHIYODA-KU , JAPAN	69-062-6718

### Parent

Company	City , State	D-U-N-S® NUMBER
NTT DATA INTERNATIONAL L.L.C.	NEW YORK , New York	80-436-5083

2

#### Subsidiaries (Domestic)

Company	City , State	D-U-N-S® NUMBER
KEANE CONSULTING, INC.	BOSTON , Massachusetts	02-129-3535
DATASKILLS, INC.	BOSTON , Massachusetts	03-285-1961
NTT DATA FEDERAL SERVICES, INC.	VIENNA , Virginia	06-678-1865


#### Subsidiaries (International)

Company	City , Country	D-U-N-S® NUMBER
NTT DATA Canada, Inc.	CAMLACHIE , CANADA	24-168-2640
NTT DATA VICTORIAN TICKETING SYSTEM PTY LTD	MELBOURNE , AUSTRALIA	75-365-0832
KEANE AUSTRALIA PTY LTD	MELBOURNE , AUSTRALIA	75-365-0899

#### Branches (Domestic)

Company	City , State	D-U-N-S® NUMBER
NTT DATA, INC.	JACKSONVILLE , Florida	06-481-6000
NTT DATA, INC.	SAN JUAN , SAN JUAN	10-188-0958
NTT DATA, INC.	JACKSONVILLE , Florida	11-637-9475
NTT DATA, INC.	ALBANY , New York	19-368-8504
NTT DATA, INC.	MC LEAN , Virginia	61-165-1043
NTT DATA, INC.	DALLAS , Texas	62-035-0116
NTT DATA, INC.	INDIANAPOLIS , Indiana	62-035-0405
NTT DATA, INC.	MARINA DEL REY , California	82-479-7062
NTT DATA, INC.	REDMOND , Washington	86-753-1068
NTT DATA, INC.	SYRACUSE , New York	92-855-6778
NTT DATA, INC.	BLOOMINGTON , Illinois	80-844-7028
NTT DATA, INC.	FRANKFORT , Kentucky	00-644-6552
NTT DATA, INC.	HAUPPAUGE , New York	01-081-1509
NTT DATA, INC.	PRINCETON JUNCTION , New Jersey	00-471-1389
NTT DATA, INC.	SYRACUSE , New York	07-179-9986
NTT DATA, INC.	PRINCETON , New Jersey	07-847-7712
NTT DATA, INC.	CHICAGO , Illinois	07-845-2451
NTT DATA, INC.	BOSTON , Massachusetts	07-925-6311
NTT DATA, INC.	BALA CYNWYD , Pennsylvania	01-122-4497
NTT DATA, INC.	LOUISVILLE , Kentucky	05-502-0219

#### Predictive Scores

Currency: Shown in USD unless otherwise indicated 

#### D&B Viability Rating Summary

The D&B Viability Rating uses D&B's proprietary analytics to compare the most predictive business risk indicators and deliver a highly reliable assessment of the probability that a company will go out of business, become dormant/inactive, or file for bankruptcy/insolvency within the next 12 months. The D&B Viability Rating is made up of 4 components:

<b>4</b>	<b>Viability Score</b>	Lowest Risk:1	Highest Risk:9
<b>Compared to All US Businesses within the D&amp;B Database:</b> <ul style="list-style-type: none"> <li>Level of Risk: <b>Low Risk</b></li> <li>Businesses ranked 4 have a probability of becoming no longer viable: <b>5 %</b></li> <li>Percentage of businesses ranked 4: <b>14 %</b></li> <li>Across all US businesses, the average probability of becoming no longer viable: <b>14 %</b></li> </ul>			
<b>5</b>	<b>Portfolio Comparison</b>	Lowest Risk:1	Highest Risk:9
<b>Compared to All US Businesses within the same MODEL SEGMENT:</b> <ul style="list-style-type: none"> <li>Model Segment : <b>Established Trade Payments</b></li> <li>Level of Risk: <b>Moderate Risk</b></li> <li>Businesses ranked 5 within this model segment have a probability of becoming no longer viable: <b>5 %</b></li> <li>Percentage of businesses ranked 5 with this model segment: <b>11 %</b></li> <li>Within this model segment, the average probability of becoming no longer viable: <b>5 %</b></li> </ul>			
<b>B</b>	<b>Data Depth Indicator</b>	Predictive Data:A	Descriptive Data:G
<b>Data Depth Indicator:</b> <ul style="list-style-type: none"> <li>✓ Rich Firmographics</li> <li>✓ Extensive Commercial Trading Activity</li> <li>✓ Basic Financial Attributes</li> </ul> <p>Greater data depth can increase the precision of the D&amp;B Viability Rating assessment.</p>			
<b>Z</b>	<b>Company Profile</b>	<b>Subsidiary</b>	

#### Credit Capacity Summary

This credit rating was assigned because of D&B's assessment of the company's creditworthiness. For more information, see the

D&B Rating Key

D&B Rating : --

The blank rating symbol should not be interpreted as indicating that credit should be denied. It simply means that the information available to D&B does not permit us to classify the company within our rating key and that further enquiry should be made before reaching a decision. Some reasons for using a "-" symbol include: deficit net worth, bankruptcy proceedings, insufficient payment information, or incomplete history information.

Below is an overview of the company's rating history since 02-03-2012

Number of Employees Total: 200 (199 here)

4



D&B Rating	Date Applied
--	02-03-2012

Payment Activity:	(based on 142 experiences)
Average High Credit:	36,894
Highest Credit:	1,000,000
Total Highest Credit:	3,534,200

#### D&B Credit Limit Recommendation

Conservative credit Limit	80,000
Aggressive credit Limit:	200,000

Risk category for this business : **LOW**

The Credit Limit Recommendation (CLR) is intended to serve as a directional benchmark for all businesses within the same line of business or industry, and is not calculated based on any individual business. Thus, the CLR is intended to help guide the credit limit decision, and must be balanced in combination with other elements which reflect the individual company's size, financial strength, payment history, and credit worthiness, all of which can be derived from D&B reports.

Risk is assessed using D&Bs scoring methodology and is one factor used to create the recommended limits. See Help for details.

#### Financial Stress Class Summary

The Financial Stress Score predicts the likelihood of a firm ceasing business without paying all creditors in full, or reorganization or obtaining relief from creditors under state/federal law over the next 12 months. Scores were calculated using a statistically valid model derived from D&Bs extensive data files.

The Financial Stress Class of 4 for this company shows that firms with this class had a failure rate of 0.84% (84 per 10,000), which is 1.75 times higher than the average of businesses in D & B's database.

**Financial Stress Class : 4** (Lowest Risk:1; Highest Risk:5)

Moderately higher than average risk of severe financial stress, such as a bankruptcy or going out of business with unpaid debt, over the next 12 months.

Probability of Failure:

Risk of Severe Financial Stress for Businesses with this Class: **0.84 %** (84 per 10,000)  
 Financial Stress National Percentile : **32** (Highest Risk: 1; Lowest Risk: 100)  
 Financial Stress Score : **1446** (Highest Risk: 1,001; Lowest Risk: 1,875)  
 Average Risk of Severe Financial Stress for Businesses in D&B database: **0.48 %** ( 48 per 10,000)

The Financial Stress Class of this business is based on the following factors:

UCC Filings reported.  
 High number of inquiries to D & B over last 12 months.  
 Low proportion of satisfactory payment experiences to total payment experiences.  
 High proportion of slow payment experiences to total number of payment experiences.  
 High proportion of past due balances to total amount owing.

**Notes:**

The Financial Stress Class indicates that this firm shares some of the same business and financial characteristics of other companies with this classification. It does not mean the firm will necessarily experience financial stress.  
The Probability of Failure shows the percentage of firms in a given Class that discontinued operations over the past year with loss to creditors. The Probability of Failure - National Average represents the national failure rate and is provided for comparative purposes.  
The Financial Stress National Percentile reflects the relative ranking of a company among all scorable companies in D&Bs file.  
The Financial Stress Score offers a more precise measure of the level of risk than the Class and Percentile. It is especially helpful to customers using a scorecard approach to determining overall business performance.

Norms	National %
This Business	32
Region: WEST SOUTH CENTRAL	44
Industry: BUSINESS, LEGAL AND ENGINEERING SERVICES	52
Employee range: 100-499	75
Years in Business: 26+	77

This Business has a Financial Stress Percentile that shows:

- Higher risk than other companies in the same region.
- Higher risk than other companies in the same industry.
- Higher risk than other companies in the same employee size range.
- Higher risk than other companies with a comparable number of years in business.

**Credit Score Summary**

The Commercial Credit Score (CCS) predicts the likelihood of a business paying its bills in a severely delinquent manner (91 days or more past terms).

The Credit Score class of 2 for this company shows that 2.5% of firms with this class paid one or more bills severely delinquent, which is lower than the average of businesses in D & B's database.

**Credit Score Class : 2**  Lowest Risk:1;Highest Risk :5

**Incidence of Delinquent Payment**

Among Companies with this Classification: **2.50 %**  
Average compared to businesses in D&Bs database: **10.20 %**  
Credit Score Percentile : **77** (Highest Risk: 1; Lowest Risk: 100)  
Credit Score : **541** (Highest Risk: 101; Lowest Risk:670)

The Credit Score Class of this business is based on the following factors:

- Proportion of slow payments in recent months
- Higher risk industry based on delinquency rates for this industry
- Proportion of past due balances to total amount owing
- Evidence of open liens

**Notes:**

The Commercial Credit Score Risk Class indicates that this firm shares some of the same business and financial characteristics of other companies with this classification. It does not mean the firm will necessarily experience severe delinquency.  
The Incidence of Delinquent Payment is the percentage of companies with this classification that were reported 91 days past due or more by creditors. The calculation of this value is based on D&B's trade payment database.  
The Commercial Credit Score percentile reflects the relative ranking of a firm among all scorable companies in D&B's file.  
The Commercial Credit Score offers a more precise measure of the level of risk than the Risk Class and Percentile. It is especially helpful to customers using a scorecard approach to determining overall business performance.


Norms	National %
This Business	77

Region: WEST SOUTH CENTRAL	52
Industry: BUSINESS, LEGAL AND ENGINEERING SERVICES	43
Employee range: 100-499	89
Years in Business: 26+	85

This business has a Credit Score Percentile that shows:

- Lower risk than other companies in the same region.
- Lower risk than other companies in the same industry.
- Higher risk than other companies in the same employee size range.
- Higher risk than other companies with a comparable number of years in business.


## Trade Payments

Currency: Shown in USD unless otherwise indicated 

### D&B PAYDEX®

The D&B PAYDEX is a unique, weighted indicator of payment performance based on payment experiences as reported to D&B by trade references. Learn more about the D&B PAYDEX

Timeliness of historical payments for this company.

**Current PAYDEX is** **77** Equal to 5 days beyond terms ( Pays more promptly than the average for its industry of 6 days beyond terms )  
**Industry Median is** **76** Equal to 6 days beyond terms  
**Payment Trend currently is**  Unchanged, compared to payments three months ago

Indications of slowness can be the result of dispute over merchandise, skipped invoices etc. Accounts are sometimes placed for collection even though the existence or amount of the debt is disputed.

Total payment Experiences in D&Bs File (HQ)	142
Payments Within Terms (not weighted)	81 %
Trade Experiences with Slow or Negative Payments(%)	19.01%
Total Placed For Collection	0
High Credit Average	36,894
Largest High Credit	1,000,000
Highest Now Owing	200,000
Highest Past Due	15,000

**D&B PAYDEX® : 77**  (Lowest Risk:100; Highest Risk:1)

When weighted by amount, payments to suppliers average 5 days beyond terms

**3-Month D&B PAYDEX® : 76**  (Lowest Risk:100; Highest Risk:1)

Based on payments collected over last 3 months.

When weighted by amount, payments to suppliers average 6 days beyond terms

### D&B PAYDEX® Comparison

#### Current Year

PAYDEX® of this Business compared to the Primary Industry from each of the last four quarters. The Primary Industry is Computer systems design, prepackaged software svc, computer related svcs , based on SIC code 7373 .

Shows the trend in D&B PAYDEX scoring over the past 12 months.

	3/15	4/15	5/15	6/15	7/15	8/15	9/15	10/15	11/15	12/15	1/16	2/16
<b>This Business</b>	73	71	78	77	76	76	77	77	77	77	77	77
<b>Industry Quartiles</b>												
Upper	80	.	.	80	.	.	80	.	.	80	.	.
Median	77	.	.	77	.	.	76	.	.	76	.	.
Lower	70	.	.	69	.	.	69	.	.	69	.	.

Current PAYDEX for this Business is 77 , or equal to 5 days beyond terms  
The 12-month high is 78 , or equal to 3 DAYS BEYOND terms  
The 12-month low is 71 , or equal to 14 DAYS BEYOND terms

#### Previous Year

Shows PAYDEX of this Business compared to the Primary Industry from each of the last four quarters. The Primary Industry is Computer systems design, prepackaged software svc, computer related svcs , based on SIC code 7373 .

Previous Year	03/14 Q1'14	06/14 Q2'14	09/14 Q3'14	12/14 Q4'14
<b>This Business</b>	76	75	77	77
<b>Industry Quartiles</b>				
Upper	80	80	80	80
Median	77	77	77	76
Lower	70	69	69	69

Based on payments collected over the last 4 quarters.

Current PAYDEX for this Business is 77 , or equal to 5 days beyond terms  
The present industry median Score is 76 , or equal to 6 days beyond terms  
Industry upper quartile represents the performance of the payers in the 75th percentile  
Industry lower quartile represents the performance of the payers in the 25th percentile

#### Payment Habits

For all payment experiences within a given amount of credit extended, shows the percent that this Business paid within terms. Provides number of experiences to calculate the percentage, and the total credit value of the credit extended.

\$ Credit Extended	# Payment Experiences	Total Amount	% of Payments Within Terms
Over 100,000	8	2,500,000	98%
50,000-100,000	5	330,000	67%
15,000-49,999	18	520,000	73%
5,000-14,999	14	107,500	89%
1,000-4,999	20	38,000	84%
Under 1,000	30	9,500	83%

Based on payments collected over last 24 months.

All Payment experiences reflect how bills are paid in relation to the terms granted. In some instances, payment beyond terms can be the result of disputes over merchandise, skipped invoices etc.

## Payment Summary

There are 142 payment experience(s) in D&Bs file for the most recent 24 months, with 74 experience(s) reported during the last three month period.

The highest Now Owes on file is 200,000 . The highest Past Due on file is 15,000

Below is an overview of the companys currency-weighted payments, segmented by its suppliers primary industries:

	Total Rev'd (#)	Total Amts	Largest High Credit Within Terms (%)	Days Slow <31 31-60 61-90 90+ (%) (%) (%) (%)					
Top Industries									
Telephone communictns	19	344,050	200,000	97	3	0	0	0	0
Public finance	10	30,900	10,000	100	0	0	0	0	0
Short-trm busn credit	9	210,000	40,000	87	13	0	0	0	0
Whol computers/softwr	6	943,500	500,000	100	0	0	0	0	0
Whol office equipment	6	40,850	35,000	48	3	46	0	3	
Misc business service	6	13,350	10,000	100	0	0	0	0	0
Prepackaged software	4	155,000	65,000	55	45	0	0	0	0
Custom programming	3	1,041,000	1,000,000	96	0	2	2	0	
Mfg computers	3	150,000	100,000	67	0	33	0	0	
Detective/guard svcs	3	1,250	750	60	30	0	0	10	
State commercial bank	2	135,000	100,000	87	0	13	0	0	
Radiotelephone commun	2	15,500	15,000	52	0	48	0	0	
Trucking non-local	2	8,250	7,500	9	0	46	45	0	
Executive office	2	5,050	5,000	100	0	0	0	0	
Nonclassified	2	5,050	5,000	99	0	0	0	1	
Electric services	2	1,750	1,000	100	0	0	0	0	
Ret mail-order house	2	1,250	1,000	80	20	0	0	0	
Computer system desgn	1	200,000	200,000	100	0	0	0	0	
Whol electronic parts	1	90,000	90,000	50	50	0	0	0	
Mfg medical instrmnt	1	55,000	55,000	100	0	0	0	0	
Data processing svcs	1	40,000	40,000	50	0	50	0	0	
Mfg process controls	1	10,000	10,000	100	0	0	0	0	
Mfg relays/controls	1	5,000	5,000	100	0	0	0	0	
Newspaper-print/publ	1	1,000	1,000	100	0	0	0	0	
Information retrieval	1	1,000	1,000	50	0	0	50	0	
Misc equipment rental	1	500	500	100	0	0	0	0	
Mfg signs/ad spectlys	1	250	250	100	0	0	0	0	
Passenger car rental	1	250	250	50	50	0	0	0	
Mfg misc office eqpt	1	100	100	100	0	0	0	0	
Whol service paper	1	100	100	50	50	0	0	0	
Lithographic printing	1	50	50	100	0	0	0	0	
Whol electrical equip	1	0	0	0	0	0	0	0	
Other payment categories									
Cash experiences	40	4,050	750						
Payment record unknown	4	25,150	25,000						
Unfavorable comments	0	0	0						
Placed for collections	0	N/A	0						
Total in D&B's file	142	3,534,200	1,000,000						

Accounts are sometimes placed for collection even though the existence or amount of the debt is disputed.

Indications of slowness can be result of dispute over merchandise, skipped invoices etc.

**Detailed payment history for this company**

Date Reported (mm/yy)	Paying Record	High Credit	Now Owes	Past Due	Selling Terms	Last Sale Within (month)
01/16	Ppt	500,000	0	0		1 mo
	Ppt	200,000	0	0		4-5 mos
	Ppt	200,000	200,000	0	N30	1 mo
	Ppt	55,000	0	0		1 mo
	Ppt	40,000	0	0	N30	1 mo
	Ppt	30,000	20,000	0		1 mo
	Ppt	30,000	0	0		6-12 mos
	Ppt	20,000	0	0		2-3 mos
	Ppt	20,000	20,000	0		1 mo
	Ppt	15,000	0	0		2-3 mos
	Ppt	10,000	0	0		6-12 mos
	Ppt	5,000	0	0		6-12 mos
	Ppt	5,000	5,000	0		1 mo
	Ppt	2,500	0	0		1 mo
	Ppt	2,500	0	0		1 mo
	Ppt	1,000	1,000	500		1 mo
	Ppt	500	50		Lease Agreemnt	
	Ppt	100	0	0	N30	6-12 mos
	Ppt	0	0	0		1 mo
	Ppt-Slow 15	65,000	0	0		1 mo
	Ppt-Slow 15	100	0	0		6-12 mos
	Ppt-Slow 30	65,000	0	0		2-3 mos
	Ppt-Slow 30	40,000	35,000	0		1 mo
	Ppt-Slow 30	20,000	15,000	250		1 mo
	Ppt-Slow 30	2,500	0	0	N30	1 mo
	Slow 30	250	0	0	N30	6-12 mos
	Slow 210	50	50	50		
12/15	Ppt	200,000	65,000	0		1 mo
	Ppt	15,000	0	0		1 mo
	Ppt	10,000	5,000	0	N30	1 mo
	Ppt	7,500	5,000	0		1 mo
	Ppt	2,500	0	0		2-3 mos
	Ppt	2,500	0	0		2-3 mos
	Ppt	2,500	2,500	0		1 mo
	Ppt	2,500	2,500	0		1 mo
	Ppt	1,000	1,000	0		1 mo
	Ppt	1,000	0	0		6-12 mos
	Ppt	750	250	0		1 mo
	Ppt	500	250	0		1 mo
	Ppt	500	0	0		4-5 mos
	Ppt	250	100	0		1 mo
	Ppt	250	0	0		4-5 mos
	Ppt	100	100	0		1 mo
	Ppt	100	100	0	Lease Agreemnt	1 mo
	Ppt	0	0	0		1 mo
	Ppt-Slow 30	15,000	7,500	250		1 mo

10



	Ppt-Slow 30	10,000	2,500	0	1 mo
	Ppt-Slow 60	40,000	20,000	15,000	1 mo
	Ppt-Slow 60	2,500	0	0	2-3 mos
	Slow 30	1,000	0	0 N30	6-12 mos
	Slow 30-150+	2,500	0	0	2-3 mos
11/15	Ppt	1,000	0	0	6-12 mos
	Ppt	50			1 mo
	Ppt	50			1 mo
	Ppt	50			1 mo
	Ppt-Slow 90	1,000	500	500	6-12 mos
	(057)	50		Cash account	4-5 mos
	(058)	50		Cash account	1 mo
	(059)	50			1 mo
	(060)	50			1 mo
	(061)	50		Cash account	1 mo
10/15	Ppt	750	0	0	6-12 mos
09/15	Ppt	0	0	0 N30	6-12 mos
	(064) Cash own option	100		Cash account	1 mo
07/15	Ppt	5,000	0	0	6-12 mos
05/15	Ppt	50	0	0	6-12 mos
	Slow 60-90	7,500	0	0	6-12 mos
04/15	Ppt	2,500			1 mo
	Ppt	2,500			1 mo
	Ppt	750			1 mo
02/15	Ppt	50			1 mo
01/15	(072) Cash own option	50		Cash account	1 mo
12/14	Ppt	1,000	50	0	1 mo
11/14	Ppt	50			1 mo
09/14	Ppt	750	750	0	1 mo
	Ppt	500	500	0	1 mo
	Ppt	250	0	0	6-12 mos
08/14	Ppt	750	0	0	6-12 mos
07/14	Ppt	2,500	0	0	1 mo
06/14	Ppt	1,000	0	0	6-12 mos

Payments Detail Key: ■ 30 or more days beyond terms

Payment experiences reflect how bills are paid in relation to the terms granted. In some instances payment beyond terms can be the result of disputes over merchandise, skipped invoices, etc. Each experience shown is from a separate supplier. Updated trade experiences replace those previously reported.

## Public Filings

Currency: Shown in USD unless otherwise indicated 

### Summary

The following data includes both open and closed filings found in D&B's database on this company.

Record Type	# of Records	Most Recent Filing Date
Bankruptcy Proceedings	0	-

11

Judgments	0	-
Liens	1	02/06/15
Suits	0	-
UCCs	1	11/10/14

The following Public Filing data is for information purposes only and is not the official record. Certified copies can only be obtained from the official source.

#### Liens

A lien holder can file the same lien in more than one filing location. The appearance of multiple liens filed by the same lien holder against a debtor may be indicative of such an occurrence.

<b>Status</b>	Open
<b>BOOK/PAGE</b>	1551/0780
<b>Type</b>	State Tax
<b>Filed By</b>	STATE OF KENTUCKY
<b>Against</b>	NTT DATA INC, BOSTON, MA
<b>Where Filed</b>	JEFFERSON COUNTY DEEDS AND RECORDS, LOUISVILLE, KY
<b>Date Status Attained</b>	02/06/15
<b>Date Filed</b>	02/06/15
<b>Latest Info Received</b>	01/23/16

#### UCC Filings

<b>Collateral</b>	Equipment and proceeds - Computer equipment and proceeds
<b>Type</b>	Original
<b>Sec. Party</b>	DELL FINANCIAL SERVICES L.L.C., ROUND ROCK, TX
<b>Debtor</b>	NTT DATA LONG TERM CARE SOLUTIONS, INC., REDMOND, WA
<b>Filing No.</b>	201431453353
<b>Filed With</b>	SECRETARY OF STATE/UCC DIVISION, OLYMPIA, WA
<b>Date Filed</b>	2014-11-10
<b>Latest Info Received</b>	11/18/14

#### Government Activity

##### Activity summary


Borrower (Dir/Guar)	NO
Administrative Debt	NO
Contractor	YES
Grantee	NO
Party excluded from federal program(s)	NO

##### Possible candidate for socio-economic program consideration

Labour Surplus Area	N/A
Small Business	N/A
8(A) firm	N/A

The details provided in the Government Activity section are as reported to Dun & Bradstreet by the federal government and other sources.

## Special Events

Currency: Shown in USD unless otherwise indicated 

### Special Events

09/29/2015

In 2015 NTT Data International Services (DUNS 80-999-1912) merged with NTT Data, Inc. As a result, NTT Data, Inc will be a subsidiary of NTT Data International, LLC (DUNS 80-436-5083).

#### 06/09/2015 -ANNOUNCED MERGER/ACQUISITION :

According to published reports, Carlisle & Gallagher Consulting Group, DUNS 797119083, (Charlotte, NC) announced that it will be acquired by NTT Data Inc., DUNS 071707764, (Plano, TX). The combined company's new headquarters will move to Plano. Terms of the deal were not immediately available. The acquisition is subject to regulatory approvals and is expected to close next quarter.

## History & Operations

Currency: Shown in USD unless otherwise indicated 

### Company Overview

Company Name:	NTT DATA, INC.
Doing Business As :	(SUBSIDIARY OF NTT DATA INTERNATIONAL L.L.C., NEW YORK, NY)
Street Address:	5601 Granite Pkwy Ste 1000 Plano , TX 75024
Phone:	800 745-3263
URL:	<a href="http://www.nttdata.com/americas">http://www.nttdata.com/americas</a>
History	Is clear
Present management control	30 years

### History

The following information was reported: 09/29/2015

Officer(s):	JOHN W MCCAIN, CEO-PRES MARV MOUCHAWAR, EXEC V PRES MICHAEL THOMAS, EXEC V PRES-CSO DAVID CROXVILLE, CFO JOHN M DICK, SEC LAWRENCE D WHELAN, TREAS
-------------	---

DIRECTOR(S) :	THE OFFICER(S) and John W. McCain, Kazuhiro Nishihata, Koji Miyajima.
---------------	---

The Massachusetts Secretary of State's business registrations file showed that NTT Data, Inc. was registered as a corporation on March 6, 1967.

Business started 1967. Present control succeeded 1986. 100% of capital stock is owned by the parent company.

The common stock was previously traded on the New York Stock Exchange under the symbol "KEA ".

#### CONTROL CHANGE :

According to published reports on June 4, 2007, Caritor, Inc. announced the completion of its acquisition of Keane, Inc. for an all-cash purchase price of approximately \$854 million.

Under the terms of the merger agreement, holders of Keane's common stock will receive \$14.30 per share in cash. As a result of this transaction, Keane common stock is no longer traded on the New York Stock Exchange. The resulting private company now operates globally under the Keane name and is based in San Ramon, CA, with US Client Management located in Boston, MA.

#### RECENT EVENTS :

In 2015 NTT Data International Services (DUNS 80-999-1912) merged with NTT Data, Inc. As a result, NTT Data, Inc will be a subsidiary of NTT Data International, LLC (DUNS 80-436-5083).

On May 21, 2012, sources stated that Ntt Data Inc., Boston, MA, has merged with and into NTT Data Agilenet LLC, Palo Alto, CA, on March 31, 2012. With the merger, Ntt Data Inc. is the surviving entity. NTT Data Agilenet LLC ceased to operate as a legal entity. Terms of the deal were not disclosed. Further details are unavailable.

On April 18, 2012, sources stated that The Revere Group, Limited, Chicago, IL, merged with and into NTT Data, Inc., formerly Keane, Inc., Boston, MA,

13

last March 31, 2012. With the merger, The Revere Group, Limited has ceased to exist as a legal entity, and its location now operates as a location of NTT Data, Inc. NTT Data, Inc. is a subsidiary of NTT Data International Services, Inc., formerly Keane International, Inc.

On May 11, 2010, sources stated that Keane, Inc., Boston, MA, has acquired Cyberefficient Technologies, Inc., Lockhart, TX, on March 24, 2010. With this acquisition, Cyberefficient Technologies, Inc. changed its name to Keane Texas, Inc. and will operate as a wholly owned subsidiary of Keane, Inc. The employees and management were retained at this time. Further details are not disclosed.

On July 15, 2009, sources stated that Keane, Inc., Boston, MA, announced the completion of its purchase of portions of the state and local government business of Bearingpoint, Inc., Dallas, TX, on July 13, 2009. As part of the acquisition, Keane, Inc. will acquire the New York City Practice from Bearingpoint, Inc. which brings approximately 30 professionals spanning numerous contracts within various New York City governmental entities. With this transaction, portions of the state and local government business of Bearingpoint, Inc. will now be owned by Keane, Inc. Further details are unavailable.

(06/05) The company acquired Cresta Testing Inc (New York, NY), and merged the company into Keane, Inc. on December 9, 2005.

#### CONTROL CHANGE :

Tokyo, Japan / Boston, MA - January 03, 2011 - NTT DATA CORPORATION, the Japanese-based leading IT services company ( "NTT DATA ", TSE : 9613), and Keane, a US-based IT services firm, today announced that NTT DATA has completed the acquisition of Keane International, Inc. Following the acquisition, Keane International, Inc. and its subsidiaries, including Keane, Inc., will remain outstanding as separate legal entities.

"We are excited to officially be part of the NTT DATA family," stated John McCain, president and chief executive officer of Keane. "As we align with NTT DATA and their global group of companies, we expect to drive growth by expanding our market reach and bringing greater visibility to our core capabilities."

Also commenting on the acquisition completion, Bob Khanna, managing director of Citi Venture Capital International (CVCI) and outgoing Keane International Board member, said, "We are pleased for all Keane stakeholders and the positive market impact this acquisition will have. This transaction represents a key milestone in the successful history of Keane."

This transaction enables NTT DATA to provide fully integrated IT services in the U.S., in addition to the strong global SAP service capabilities it has built to date. NTT DATA plans to further strengthen its support of the NTT DATA group customers through coordination and cooperation between Keane International and the NTT DATA global group companies.

#### About Keane.

Keane, an NTT DATA Company, is an IT services firm headquartered in the US with more than 12,500 professionals worldwide. For 45 years, Keane has been an Application Services specialist with distinguished project management credentials. Today, we offer a flagship suite of Application Services, as well as Infrastructure and Business Process Outsourcing solutions delivered through onsite, nearshore, and offshore resources.

Visit [www.keane.com](http://www.keane.com) to learn how our projects, managed services, and outsourcing engagements deliver value for a range of businesses and government agencies.

#### About NTT DATA CORPORATION.

NTT DATA is a quoted subsidiary of Nippon Telegraph and Telephone Corporation ( "NTT " ). It offers a broad range of IT services including consulting, systems integration and IT outsourcing. NTT DATA recorded total revenues of approx. JPY 1.1 trillion (USD 13.7 billion) for the year ended March 31, 2010, and has more than 36,173 employees as of June 30th. NTT DATA has taken various steps to develop its business on a global scale.

#### For further information please visit :

Http :  
[//www.nttdata.co.jp/en/index.html](http://www.nttdata.co.jp/en/index.html).

**JOHN WMCCAIN.** Mr. McCain is a 22 year veteran of the IT Services industry and joins NTT DATA, after his most recent assignment at Hewlett-Packard Company. He served as senior vice president and general manager of HP Services. Mr. McCain also has led the \$3.6 billion Consulting and Integration business of HP. Prior to joining HP, he held the position of chief executive officer of North America for Capgemini. During 16 years with EDS. Mr. McCain holds a Bachelor of Science degree in Management and Administration from Indiana University, Bloomington and he has completed the Executive Development Program at the University of Pennsylvania's Wharton Graduate School of Management in Philadelphia. 2009-present active here.

**MARV MOUCHAWAR.** Mr. Mouchawar has over 20 years of experience in IT services and software industry, with the last 10 years serving as either a senior executive, officer, or board level capacity at private or publicly traded companies. He began his IT career at Accenture where he worked with multi-national high technology manufacturing companies such as Apple Computer, Amdahl, HP, Sun Microsystems, and SGI, delivering custom and packaged application services. He then became a buyer of IT services and enterprise software in the corporate IT ranks at SGI and Autodesk. At SGI, Mr. Mouchawar's roles included a divisional CIO role that helped pioneer the packaged CRM space working closely with companies and founders from Siebel, Aurore, Clarify, and Scopus. While at Autodesk, he was responsible for global application services that included being the first US-based company to globally implement and maintain SAP R/3. During his tenure at Autodesk, Mr. Mouchawar worked with the founders and key development staff of SAP to develop enterprise solutions specifically for the manufacturing vertical industry. Mr. Mouchawar co-founded Influence Software in 1996. Influence Software was one of the first companies focused on delivering packaged BI solutions for the ERP space. Influence's value-added enterprise applications leverage partnerships with Business Objects, Cognos, Hyperion, and Informatica. He served as the CEO of this company, spearheading its growth to Fortune 100 companies. Influence

**MICHAEL THOMAS.** Mr. Thomas is a seasoned business and sales leader in the technology industry. Previously, who was executive vice president of Global Sales and Marketing at Symphony Services, Prior to Symphony, He was a vice president at Capgemini. In this role, he was responsible for sales in the company's Americas Outsourcing business and general management of its North America BPO organization, specifically focusing on large mega deal activities for companies looking to achieve meaningful transformational change. Mr. Thomas also ran the global sales organization for EDS's professional services business where he led significant year-over-year growth.

**DAVID CROXVILLE.** Mr. Croxville oversees all global finance and IT management and operations. IT services career spans over 20 years holding leadership roles that include controller, managing director of financial planning and analysis as well as CFO of a \$10 billion dollar organization. Mr. Croxville comes to NTT DATA from Pegasus Logistics Group, where he served as chief financial officer and chief operating officer. Prior to PLG, Mr. Croxville had a successful 20-year career with EDS (acquired by HP in 2008). As vice president and chief financial officer, he was responsible for the Americas business, which consisted of the US, Canada, and Latin America, as well as General Motors and Excellerate HRO. He also led EDS' US Government and Navy Marine Corps Intranet (NMCI) business. He began his EDS career in 1988 as part of the company's Accounting and Financial Development program. Mr. Croxville served as controller of various internal industry organizations in addition to being the financial lead for the \$6 billion MCI outsourcing contract awarded in October 1999. Mr. Croxville joined EDS following six years in the United States Marine Corps. Mr. Croxville is a graduate of National University and holds a masters degree of business administration from Southern Methodist University.

14



JOHN M DICK. Antecedents are unknown.

LAWRENCE D WHELAN. Antecedents are unknown.

Business address has changed from 100 City Sq, Boston, MA, 02129 to 5601 Granite Pkwy Ste 1000, Plano, TX, 75024.

#### Business Registration

CORPORATE AND BUSINESS REGISTRATIONS REPORTED BY THE SECRETARY OF STATE OR OTHER OFFICIAL SOURCE AS OF

Jan 29 2016

**Registered Name:** NTT DATA, INC.  
**Business type:** DOMESTIC CORPORATION  
**Corporation type:** PROFIT  
**Date incorporated:** Mar 06 1967  
**State of incorporation:** MASSACHUSETTS  
**Filing date:** Mar 06 1967  
**Registration ID:** 042437166  
**Status:** CHARTER SURRENDER  
**Status Attained Date:** Feb 25 2015  
**Where filed:** SECRETARY OF THE COMMONWEALTH/CORPORATIONS DIVISION ,  
BOSTON , MA  
**Registered agent:** NATIONAL REGISTERED AGENTS, INC. , 155 FEDERAL STREET, SUITE  
700 , BOSTON , MA , 021100000  
**Principals:** KATRINA KROPA ASSISTANT SECRETARY  
JENNIFER M. LURIE ASSISTANT SECRETARY  
C.WHITNEY PEDERSEN ASSISTANT SECRETARY  
CHUCK GILL ASSISTANT TREASURER  
JOHN W. MCCAIN CEO  
JOHN W. MCCAIN DIRECTOR  
KOJI MIYAJIMA DIRECTOR  
KAZUHIRO NISHIHATA DIRECTOR  
JOHN M. DICK EX VICE PRESIDENT  
DAVID CROXVILLE EX VICE PRESIDENT/CFO  
JOHN W. MCCAIN PRESIDENT  
JOHN M. DICK SECRETARY  
LAWRENCE D WHELAN JR TREASURER

#### Operations

09/29/2015

Subsidiary of NTT Data International L.L.C., New York, NY started 1993. Parent company owns 100% of capital stock.

Designs computer integrated systems design and systems software development. Provides prepackaged software. Provides computer related consulting.

**Description:** Fax: 972 624-7940.

Terms are on a contractual basis with monthly billings. Sells to manufacturers, hospitals, financial institutions and insurance companies. Territory : United States & Canada.

Nonseasonal.

**Employees:** 200 which includes officer(s). 199 employed here.

**Facilities:** Leases 73,000 sq. ft. in a multi story building.

**Location:** Central business section on main street.

**Branches:** This business has multiple branches, detailed branch/division information is available in D & B's linkage or family tree products.

#### SIC & NAICS

**SIC:**

1.5

Based on information in our file, D&B has assigned this company an extended 8-digit SIC. D&B's use of 8-digit SICs enables us to be more specific about a company's operations than if we use the standard 4-digit code.

The 4-digit SIC numbers link to the description on the Occupational Safety & Health Administration (OSHA) Web site. Links open in a new browser window.

7373 0000 Computer integrated systems design  
 7373 0100 Systems software development services  
 7372 0000 Prepackaged software  
 7379 0200 Computer related consulting services

**NAICS:**

541512 Computer Systems Design Services  
 541512 Computer Systems Design Services  
 511210 Software Publishers  
 541512 Computer Systems Design Services

## Financials

### Company Financials: D&B

### Additional Financial Data

As of January 27, 2015, attempts to contact the management of this business have been unsuccessful. Outside sources confirmed operation and location.

### Request Financial Statements

Requested financials are provided by NTT DATA, INC. and are not DUNSRight certified.

### Key Business Ratios

D & B has been unable to obtain sufficient financial information from this company to calculate business ratios. Our check of additional outside sources also found no information available on its financial performance.

To help you in this instance, ratios for other firms in the same industry are provided below to support your analysis of this business.

Based on this Number of Establishments

20

Industry Norms Based On 20 Establishments			
	This Business	Industry Median	Industry Quartile
<b>Profitability</b>			
Return on Sales %	UN	4.8	UN
Return on Net Worth %	UN	25.1	UN
<b>Short-Term Solvency</b>			
Current Ratio	UN	2.1	UN
Quick Ratio	UN	1.8	UN
<b>Efficiency</b>			

16



Assets to Sales %	UN	39.1	UN
Sales / Net Working Capital	UN	7.1	UN
<b>Utilization</b>			
Total Liabilities / Net Worth (%)	UN	91.6	UN

UN = Unavailable

## View Snapshots

### View Snapshots

### Detailed Trade Risk Insight™

Detailed Trade Risk Insight provides detailed updates on over 1.5 billion commercial trade experiences collected from more than 260 million unique supplier/purchaser relationships.

#### Days Beyond Terms - Past 3 & 12 Months

3 months from Dec 15 to Feb 16

**6**  
Days

Dollar-weighted average of 41 payment experiences reported from 26 companies

12 months from Mar 15 to Feb 16

**4**  
Days

Dollar-weighted average of 80 payment experiences reported from 44 companies

#### Derogatory Events Last 13 Months from Feb 15 to Feb 16

No Derogatory trade Event has been reported on this company for the past 13 Months

#### Total Amount Current and Past Due - 13 month trend from Feb 15 to Feb 16

Status	Feb-15	Mar-15	Apr-15	May-15	Jun-15	Jul-15	Aug-15	Sep-15	Oct-15	Nov-15	Dec-15	Jan-16	Feb-16
Total	569,874	751,335	2,209,794	1,769,291	2,041,759	1,880,287	2,050,598	555,296	668,705	300,661	562,366	564,360	564,360
Current	143,878	717,559	2,116,535	1,680,878	1,962,382	1,799,852	1,969,072	486,874	554,568	196,881	464,941	466,380	466,380
1-30 Days Past Due	140,145	17,023	85,414	80,108	9,759	13,376	16,582	802	113,021	88,310	89,170	89,691	89,691
31-60 Days Past Due	83,646	13,133	5,278	5,638	66,649	63,380	64,268	65,979	468	14,354	7,089	7,144	7,144
61-90 Days Past Due	143,799	442	461	561	2,129	3,028	24	965	74	489	74	53	53
90+ Days Past Due	58,406	3,178	2,106	2,106	840	651	652	676	574	627	1,092	1,092	1,092

This information may not be reproduced in whole or in part by any means of reproduction.