System and Organization Controls 3 Report

Report on NTT Managed Services Americas' Infrastructure Hosting Services Relevant to Security and Availability

throughout the period October 1, 2019 to September 30, 2020

Management's Assertion Regarding the Effectiveness of Its Controls Over the Infrastructure Hosting Services Based on the Trust Services Criteria for Security and Availability

November 06, 2020

We, as management of NTT Managed Services Americas, are responsible for:

- Identifying the Infrastructure Hosting Services (System) and describing the boundaries of the System, which are presented in "Description of NTT Managed Services Americas' Security and Availability Controls related to its Infrastructure Hosting Services throughout the period October 1, 2019 to September 30, 2020"
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system
- Identifying, designing, implementing, operating, and monitoring effective controls over the Infrastructure Hosting Services (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirement
- Selecting the trust services categories that are the basis of our assertion

We assert that the controls over the system were effective throughout the period October 1, 2019 to September 30, 2020, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security and availability set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Four of NTT Managed Services Americas' six production data centers are hosted at co-location facilities: the Switch (SuperNap) facility in Las Vegas, NV (DCE), NTT RagingWire facility in Garland, TX (DCJ), NTT e-shelter facility in Frankfurt, Germany (DCH) and NTT e-shelter facility in Rümlang, Switzerland (DCI). These sub-service providers are responsible for physical security and environmental controls. As it relates to services provided to the Company by the Subservice Organizations, we are not aware of instances of any of the following:

- Actual, suspected, or alleged fraud by management or employees of the Subservice Organizations or noncompliance with laws or regulations by the Subservice Organizations, coming to our attention that could adversely affect the Subject Matter or that are otherwise relevant to one or more user entities

- Instances in which the Subservice Organization Controls presented in the system description were not suitably designed and implemented or did not operate effectively or as described, after giving consideration to expected rates of deviation
- Any other known matters related to the Subservice Organizations contradicting the fairness of the presentation of the system description, the suitability of the design or operating effectiveness of the controls to achieve the applicable trust services criteria, or our assertion

Our attached description of the boundaries of the Infrastructure Hosting Services identifies the aspects of the Infrastructure Hosting Services covered by our assertion.

Very truly yours,

NTT Managed Services Americas

Ernst & Young LLP
One Kennedy Square
Suite 1000
777 Woodward Avenue
Detroit, MI 48226-5495

Tel: +1 313 628 7100
Fax: +1 313 628 7101
ey.com

Report of Independent Accountants

Management of NTT Managed Services Americas

Scope

We have examined management's assertion, contained within the accompanying "Report of Management on NTT Managed Services Americas' Operations and Technology Controls related to its Infrastructure Hosting Services" (Assertion), that NTT Managed Services Americas' controls over the Infrastructure Hosting Services System (System) were effective throughout the period October 1, 2019 to September 30, 2020 to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security and availability (applicable trust services criteria) set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Management's Responsibilities

NTT Managed Services Americas' management is responsible for its assertion, selecting the trust services categories and associated criteria on which the its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Infrastructure Hosting Services (System) and describing the boundaries of the System
- Identifying our principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system
- identifying, designing, implementing, operating, and monitoring effective controls over the Infrastructure Hosting Services (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirement

Our Responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of NTT Managed Services Americas' relevant security and availability policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Building a better working world

Our examination was not conducted for the purpose of evaluating NTT Managed Services Americas' cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

NTT Managed Services Americas uses Switch SUPERNAP, NTT Raging Wire and NTT e-shelter (subservice organizations) to provide physical security and environmental controls for four of its six production data centers. Our examination did not extend to the services provided by the subservice organizations and we have not evaluated whether the controls management assumes have been implemented at the subservice organizations have been implemented or whether such controls were suitably designed and operating effectively throughout the period October 1, 2019 to September 30, 2020.

Inherent limitations

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve NTT Managed Services Americas' principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion

In our opinion, NTT Managed Services Americas' controls over the system were effective throughout the period October 1, 2019 to September 30, 2020, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria, if the subservice organizations applied the controls assumed in the design of NTT Managed Services Americas' controls throughout the period October 1, 2019 to September 30, 2020.

Ernst & Young LLP

November 06, 2020

Overview of Operations

NTT Managed Services Americas Business Overview

NTT Managed Services Americas (NTT Managed Services) provides managed cloud services, application hosting, managed services, managed security services, end user services and IT consulting services. Our managed cloud services support customer workloads in private, public, hybrid or multi cloud environments. NTT Managed Services provides managed cloud services in NTT data centers, Microsoft Azure, Amazon Web Services or customer premise.

While NTT Managed Services provides public cloud services in Amazon Web Services (AWS) and Microsoft Azure, physical and environmental controls for the physical location of services are not included as part of this report, as public cloud services are contracted between the public cloud provider and clients.

NTT Managed Services hosted solutions are designed to be highly available and scalable and to incorporate leading-edge technology. We provide customers with full-service technical offerings, from design to production support, with a focus on high availability, security, and disaster recovery practices. To provide support to our customers, NTT Managed Services has developed optimized, repeatable policies and processes to manage our application hosting projects. The processes we use to execute our operations are based on Information Technology Infrastructure Library (ITIL) and Control Objectives for Information and Related Technologies (COBIT), the industry standards for best practice information management processes. Components of the system described in the report will cover the infrastructure, software, people, policies and procedures, call center support service, and data management. Security policies, processes and services are designed and certified to meet ISO 27001:2013, ISO 27017:2015, and ISO 27018:2014.

NTT Managed Services provides services in the following data center locations:

- Plymouth, MI (DCD)
- Southfield, MI (DCB)
- Las Vegas, NV (DCE)
- Garland, TX (DCJ)
- Frankfurt, Germany (DCH)
- Rümlang, Switzerland (DCI)

Principal Service Commitments and System Requirements

NTT Managed Services designs its processes and procedures related to its Information Security Management System (ISMS) to meet its objectives for its managed cloud services, IT operations, applications hosting, managed security services, and IT consulting services. Those objectives are based on the service commitments that NTT Managed Services makes to user entities, the laws and regulations that govern the provision of ISMS services, and the financial, operational, and compliance requirements that NTT Managed Services has established for the services (***Control 3.3***). The ISMS services of NTT Managed Services are subject to the following security and privacy requirements (as applicable to each customer):

- Health Insurance Portability and Accountability Act Administrative Simplification (HIPAA and HITECH)
- Internal Revenue Service IRS-1075 (FTI)
- Export Control (ITAR and EAR)
- Sarbanes-Oxley Act of 2002 (PL 107-204 2002 HR 3763) – Section 404 (PCAOB (Public Company Accounting Oversight Board))
- Securities and Exchange Act, Sections 32(a) and (b) (SEC)
- Federal Information Security Management Act (FISMA) of 2002 (FTC)
- 6 CFR Part 29 Procedures for Handling Critical Infrastructure Information – Department of Homeland Security
- State privacy security laws and regulations in the jurisdictions in which NTT Managed Services operates

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- ISMS and Regulatory Policy and Procedure Employee Training Program
- Employee Background Checks
- Drug Screening
- Security Awareness Training
- Least Privileged Physical and Logical Access
- Physical Access Denied Parties Scanning
- Password Complexity Standards
- Data Encryption Across Multiple Data Centers
- Disaster Recovery
- Business and Privacy Impact Assessments
- Vendor Risk Management
- ISMS/Control Risk Assessments
- Internal Audit of Controls
- Security Incident Management
- Change Management
- Anti-Virus, Vulnerability, and SIEM Security Management

NTT Managed Services establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in NTT Managed Services' system policies and procedures, system design documentation, customer contracts, and contracts with third party services. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees and contracted staff members are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the ISMS.

Infrastructure

Private cloud services and remote management services are provided to users using highly available (N +1) enterprise IT infrastructure equipment located in the data center locations in Plymouth, MI and Southfield, MI. Services are provided using a range of hardware, including Cisco, Oracle, and IBM servers, VMware and Oracle Hypervisors, Oracle, NetApp, Pure and EMC Storage Area Networks (SANs) and backup, and Networking Equipment from multiple providers. NTT Managed Services regularly assesses technical innovations in computing, storage, and network, and it updates its infrastructure.

Public Cloud Services are provided to users running on highly available infrastructure. Public cloud infrastructure is located and physically protected within Hyperscaler datacenters. Each public cloud Hyperscaler deploys their own combinations of commercially available and propriety hardware, storage, and networking technologies. The Hyperscalers updates, patches and maintains its own infrastructure.

Software

NTT Managed Services provides cloud services using the hardware identified under the heading “Infrastructure,” which supports a hypervisor software and operating system software. NTT Managed Services primarily supports Windows and Linux operating systems and may support the installation and/or availability of customer owned applications and these processes follow an established change management procedure for Managed Service Provider (MSP) clients. These are provided from private common and/or dedicated platforms that are maintained and managed by NTT Managed Services. NTT Managed Services will also provide server backups, management of dedicated customer firewalls, and managed load-balancing.

People

Services are provided by NTT Managed Services’ Network Operations, Security, Support, Sales, Billing, Account Management, Product Development, Information Technology (IT), Facilities, and Executive Management teams.

NTT Managed Services teams are recruited and managed using NTT Managed Services policies and procedures, which are described in the following sections.

Policies and Procedures

Formal IT, security and privacy policies and procedures exist that describe incident response, change management, logical and physical security and access, network security, backup and encryption, and system security standards. Personnel are expected to adhere to NTT Managed Services' policies and procedures that define how services should be delivered. These are located on the company's intranet and can be accessed by any NTT Managed Services team member. Policies and procedures are updated as needed, or by the required review date, whichever comes first. Security policies, security training, and regulatory training are required to be reviewed annually. NTT Managed Services has a standard in placed called the Information Security Management System (ISMS) which meets IS0 27001:2013. Changes to policies and procedures are distributed to employees and contracted staff members, who must acknowledge that they have received the information and/or training.

Data

Customer data is managed and stored in consideration with relevant data protection and other regulations (as listed below), with specific requirements formally established in customer contracts. Customer data is isolated from other customer environments and NTT Managed Services management environment by dedicated routing instances and layer 2 and layer 3 separation, and access is limited via least privilege role-based access. This data is managed and stored in a range of database technologies, and Customers may evaluate and select the option to utilize NTT Managed Services services to help meet Customers' compliance with regulatory or legal requirement.

- Securities Act of 1933
- Securities Exchange Act of 1934
- Sarbanes Oxley Act of 2002
- Related rules and regulations of the Securities and Exchange Commission, including Regulation S-X
- Rules, regulations, and listing standards of the New York Stock Exchange
- Rules, regulations, and standards of the Public Company Accounting Oversight Board
- Any other financial control or disclosure requirement imposed by law on public companies
- Gramm-Leach Bliley Act of 1999
- Dodd-Frank Wall Street Reform and Consumer Protection Act of 1999
- Privacy Act of 1974 at 5 U.S.C. 552a
- Privacy Shield
- Applicable Laws in the State of Michigan
- Other compliance requirements which NTT Managed Services may be utilized to meet:
    - GDPR & Other non-US Privacy Regulations
    - HIPAA, HITECH, CMS, FDA and other Regulations on Health Care or Lifesciences industries
    - FTI
    - Export Control Regulations (ITAR/EAR)
    - Other Applicable Laws/Regulations within the USA

Customer contracts may alternatively opt to require compliance with the requirements of the following IT frameworks:

- ISO 27001:2013
- ISO 27017:2015
- ISO 27018:2014
- COSO
- COBIT
- ITIL
- Customer Internal Controls[1]

Customer Responsibilities

Customers are responsible for performing necessary risk assessments and evaluations of the services and agreements which NTT Managed Services provisions for Customer's sole use, and for ensuring that the services support such customer-specific assessments. Customer Risk assessments should include fitness of the services for the Customer's intended purpose or use.

Customers should also have necessary information security policies and procedures which are communicated to their staff and vendors. Customer-employee responsibilities are communicated in the applicable master services agreement and statement(s) of work. The customer is responsible for verifying that customer activities required to meet the controls are communicated to the customer's employees and are covered in the applicable NTT Managed Services agreement.

Customers who purchase managed cloud computing and/or managed private cloud services have application administrator-level privileged and/or domain administrator access to configurations which allows them the ability to perform logical security administration functions for their respective environments. Any customer-initiated changes or modifications to servers, services, or logical access entitlements are exclusively the responsibility of these customers. Similarly, customers are responsible for performing necessary change management procedures when NTT Managed Services is not responsible for the design or implementation of customer changes.

Customers engage with NTT Managed Services to provide an environment meeting data security requirements. NTT Managed Services does not include data processing in contracts and does not process data on behalf of customers. Therefore, it is the customer's responsibility to verify that data placed into the environment is processed correctly and is valid.

Similarly, co-location customers who require an approved access key card to the racks on which their dedicated servers reside, are responsible for the following: notifying NTT Managed Services of any change of employment status for anyone who has key card access, approving customer-initiated server maintenance activities performed by customer personnel, and implementing and maintaining disaster recovery procedures for customer co-located hardware.

[1] Customer internal controls which differ from the controls documented in this report are not included in the scope of the report.

Systems Overview

NTT Managed Services provides support services using the following outlined technologies and service areas. The mix of technologies and service areas provided to MSP clients varies based on contractual agreements and defined SLA's.

Service Area	Depth of Services and Technologies	
IT Administration and Support	Technical Support	24 x 7 Technical Support Desk and Customer Service Manager
	Level 1 Help Desk	USA-based or Global-based
	ITIL ITSM Toolset	S24 CloudLink & ServiceNow
	Active Directory/LDAP	With or without Multifactor Authentication
	Desktop as a Service	DaaS + DaaS vGPU
	Endpoint Management	Altiris
Enterprise Managed Cloud (Virtual and Dedicated)[2]	Server Operating Systems (OS)	Oracle Linux
		Red Hat Linux
		MS Windows
	Virtualized Compute	Oracle VM Server
		VMware ESX/ESXi
	Enterprise Storage & Retention	All-Flash Based
		Hybrid Disk
		App-aware Backup
	Enterprise Network Security	Dedicated Virtual Firewall
		Dedicated Physical Firewall
		IPS/IDS
		Load balancing
		SSL VPN
Managed IAAS	OS-Down Services	Prod, Dev, QA
Disaster Recovery Services	Complete DR Solutions	SLA backed DR
Application Performance Management	End-to-end Optimization from Application to Branch	DC, WAN, Branch
Wide Area Networking	Site-2-Site VPN and MPLS	Vendor agnostic
	Carrier Management	Carrier agnostic
Customer IT Device Support	Remote Management	OS & Network Devices
Managed Security Services	Advanced Network and Host Level Security	
	Endpoint Protection (SEP ATP)	
	Security Incident Event Management (SIEM)	
	Vulnerability Testing	

[2] Services include Backups and Monitoring, as well as compute and storage. Management of dedicated customer firewall is also included, along with managed load-balancing.