NTT DATA Service Description

NTT DATA Cloud Operational Excellence for Azure

Introduction

NTT DATA is pleased to provide NTT DATA Cloud Operational Excellence ("COE") for Microsoft Azure ("Azure") (the "Service(s)") in accordance with this Service Description ("Service Description"). The Customer's quote, order form or other mutually-agreed upon form of invoice or order acknowledgment (as applicable, the "Order Form") will include the name of the service(s) and available service options that you purchased. For additional assistance or to request a copy of your service contract(s), contact NTT DATA technical support or your sales representative.

The Scope of This Service

The Services are designed to provide certain monitoring and operational management activities for the Customer's Azure-hosted infrastructure, using Information Technology Infrastructure Library (ITIL®) based methodologies. Additional services and solutions can be added to complement your Azure cloud environment. Please work with your sales contact to review additional options.

This Service Description describes the Service being provided to you, the Customer (("Customer" or "you") which shall refer to the customer entity identified in the applicable Order Form), by the NTT DATA entity identified on your Order Form or invoice for the purchase of this Service (in case you did not buy from NTT DATA directly, "NTT DATA" shall refer to your respective reseller of the NTT DATA Services).

Definition of Terms

These terms are used within this document.

Priority of Incident	The method that NTT DATA uses to rank and prioritize incidents. The priority determines the order in which incidents should be attended to.
Incident Identification Number ("IID")	This is a unique incident identification number that is used to track all incidents and service requests reported by the Customer or through automatically generated events or alerts.
Incident Owner	The person to whom an IID has been assigned.
Portal, Self-Service Portal, NTT DATA Cloud Portal	Multi-tenant software-as-a-service ("SaaS") solution that delivers IT operations lifecycle management capabilities that spans public and private cloud infrastructure and application elements.

Services

As more fully described in this Service Description, NTT DATA offers the Services to help the Customer manage and operate its Azure-hosted environment.

Separately, and outside the scope of this Service Description, NTT DATA offers additional infrastructure services that span a variety of use cases for a high-performing and secure public cloud environment:

- Cloud migration and adoption strategy planning
- Total cost of ownership (Plan, Assess and Manage)
- Virtual Datacenter (vDC)
- Host protection
- Endpoint security
- Disaster recovery
- Application and workload migration
- Warm backups
- Customized services

Please speak to your NTT DATA representative for more information regarding the above offerings.

Cloud Operational Excellence for Azure

This section presents a summary overview of the features that are included in this prepackaged Service offering, which are more fully described in the "Service Details" section below.

NTT DATA Cloud Operational Excellence Features	
Business Support	Customer Delivery Executive
	Service requests
	Change management
	Monthly and on-demand reporting
Solution Health and Operations Support	Azure Product Support
	Performance tuning and preventative maintenance
	Bandwidth and network management
	Performance analysis & cost optimization
	Operating system administration
	Identity and Access Management
	Firewall Management
Event management	Cloud Lifecycle Management portal
	Performance and availability monitoring
	Alert management
Incident management	24x7 service desk
	Troubleshooting and remediation
	Escalation management

	Root cause analysis & resolution

NTT DATA, will, at its sole discretion, determine the number of personnel and the appropriate skill sets necessary to complete the Services. Customer agrees that NTT DATA resources may include employees of NTT DATA and/or a service provider or subcontractor to NTT DATA.

Service Coverage Products

NTT DATA's Cloud Operational Excellence Service is designed to cover the following Azure products or resources only*:

Scope of Services - Azure Products	
Application Gateway	Service Bus
Application Insights	Storage (block/page blob, table, queue & file)
Active Directory sync	Traffic Manager
Azure ExpressRoute	Virtual Machines
Azure File Storage	Virtual Network, VNET Peering
Azure Resource Manager	Virtual Private Network – Point to Site
Key Vault	Virtual Private Network – Site to Site
Load Balancer	Virtual Private Network Gateway
Log Analytics	Web Access Firewall
Scale-set	

Table: Services Coverage Product Table

The table above reflects the products that will be managed, serviced and supported within the scope of this Service. NTT DATA will provide monitoring and alert management for all Azure products in the Customer's Azure environment, but operational support, as described within this Service Description, shall be limited to the products set out in the Services Coverage Product Table shown above.

*Coverage for additional products and solutions may be available as a supplemental or customized managed services offering.

Service Details

Business Support

Customer Delivery Executive (CDE)

The NTT DATA Customer Delivery Executive ("CDE") will serve as a primary point of contact in delivering the Service, and in providing the following support:

- Establish and manage relationship with identified Customer contacts
- Help manage onboarding process and deployment schedule
- Coordinate with other NTT DATA teams, where applicable, to provide a unified NTT DATA solution
- Work with the operations team to identify opportunities and continually improve Customer experience with respect to the Services under this Service Description

- Manage and enable invoicing and billing process
- Define key measures and periodically review them with Customer
- Advise Customer of any high severity incidents, root causes, and resolution efforts, where appropriate
- Develop and review cloud plans with Customer including forecast and growth projections

Service Requests

Service requests ("SRs") are procedures, as further described below, that are not due to disruption of service (i.e. requests which are not due to any incidents identified in the infrastructure, monitored event or change requests due to root cause analysis).

Post-implementation SRs are limited to twenty (20) requests per month. SRs are assigned as Priority Level 4 and will align with the Service Level Agreement ("SLA") as defined in Appendix A. Additional requests may be supported based on time and effort and will addressed outside of this scope of services. Each request is limited to 1.5 hours of engineering time.

Service Requests include:

- Create point-in-time copies of data
- Move data to Cool storage for retention or archival purposes (pertains to moves of cloud storage from Hot to Cool, within the same region)
- Turn services on or off
- Setup file archiving policies
- Configuration change requests
- Add users to security groups
- On-demand bandwidth control requests or as part of remediation
- Allow or deny IP and ports
- Create or modify a circuit or peering configuration
- Link a VNet to an ExpressRoute circuit
- Other requests will be considered or accepted if time and effort falls within the SR time allocation of 1.5 hours per request.

Service Request process:

- Customer submits request to CDE or in the designated Information Technology Service Management ("ITSM") tool.
- The request is reviewed by the NTT DATA Engineering or Cloud Delivery team, where applicable, and creates a ticket in the ITSM tool for tracking purposes.
- The Engineering team will work with Customer to obtain relevant details.
- The Engineering team consults with the primary Architect or lead Engineer if there will be a material impact on architecture to determine the best course of action or configuration.
- If there is a significant impact on the existing configuration, the Engineering team will propose the recommendations to the Customer for review and approval.
- The update is presented to the NTT DATA Service Delivery or Domain lead to approve the change.
- The proposed updated is sent to the designated approver at the Customer for request approval
- The Engineering team implements the change and notifies the Customer of the update

- The Customer tests the affected workload or application to validate performance and/or behavior, sends approval to the Engineering team
- The Engineering team closes the SR ticket.

Please note: Adding additional Azure products and/or making changes may result in additional Azure usage fees and could impact your services rates. The Engineering team or CDE will address any such changes with the Customer prior to implementation. Only supported products will be considered in scope; see the Services Coverage Product Table (page 3) for details.

Resolution time, as depicted in Appendix A, will not be calculated or tracked when a Customer approval or testing is pending or required.

Change Management

Change management requests are limited to ten (10) per month as included in this service offering. Such requests are assigned Priority Level 4 and provided with SLAs as defined in Appendix A. Additional requests may be supported based on time and effort and will addressed outside of this scope of Services. Each request is limited to 3 hours of engineering time.

Change Management request options include:

- Significant landscape configuration changes (such as, NAT, rules, VLANs, routes, and access)
- Adding a new server or VM
- Upgrading instance size or altering features
- Resizing auto scaling groups to handle increases or decreases in traffic
- Moving instances/services to other regions or availability zones
- Configure a router or VNet Gateway for ExpressRoute
- Migrate a circuit or associated VNets from Classic to Resource Manager
- Other change management requests will be considered if time and effort falls within Change Management time allocation of 3 hours per request

Change Management process:

- Customer submits request to the CDE or in the ITSM tool.
- The request is reviewed by the NTT DATA Engineering or Cloud Delivery team and creates a ticket in the ITSM for tracking purposes.
- The Engineering team will work with the Customer to obtain relevant details.
- The Engineering team consults with the primary Architect or lead Engineer if there will be a material impact on architecture to determine the best course of action or configuration.
- If there is a significant impact on the existing configuration, the Engineering team will propose the recommendations to the Customer for review and approval.
- The update is presented to the NTT DATA Service Delivery or Domain lead to approve the change.
- The proposed update is sent to the designated approver at the Customer for request approval
- The Engineering team implements the change and notifies the Customer of the update
- The Customer tests the affected workload or application to validate performance and/or behavior, sends approval to the Engineering team

- The Engineering team closes the change management request ticket.

Please note: Adding additional Azure products and/or making changes may result in additional Azure usage fees and could impact your services rates. The Engineering team or CDE will address any such changes with the Customer prior to implementation. Only supported products will be considered in scope; see the Services Coverage Product Table (page 3) for details.

Resolution time, as depicted in Appendix A, will not be calculated or tracked when a Customer approval or testing is pending or required.

Monthly and On-Demand Reporting

As further detailed below, NTT DATA provides monitoring and related reports, including availability and performance statistics, through NTT DATA Cloud Lifecycle Management (also referred to as the "Portal" or "CLM").

NTT DATA has created preconfigured reports to provide details for an executive level overview of performance as well as granular assessments of key performance indicators across components and features in your cloud environment.

The CLM also presents the ability to customize views into a Customer's infrastructure based on available selection criteria, dependent upon connected resources. The CDE will help determine your reporting needs and will work with the Cloud delivery team to enable delivery of your report.

The table below shows a sample set of pre-generated, on-demand and scheduled set of reports*: Scheduled reports can be delivered on the cadence and to the recipients the Customer designates.

Category	Report Description	Pre-generated Report	On-demand Report	Scheduled Report
Audit reports	Console audit recordings	✓		
	Login history report		✓	
	Disk space report	✓		
	Hardware report		✓	
	Software report		✓	
	Storage report	✓	✓	✓
	Virtualization report	✓		✓
Network reports	Interface utilization and traffic		✓	
	IP SLA report	✓	✓	✓
	Network backup summary report	✓	✓	✓
	Network devices inventory report		✓	
	Network executive report	✓		
	Network Statistics report	✓		
	AD Health check report		✓	

Preventive maintenance reports	Anti-virus compliance report		✓	
	Anti-virus status report	✓		
	Backup report		✓	
Service reports (per client)	Application audit report		✓	
	Customer executive report	✓	✓	✓
	Device details summary report	✓		✓
	URL monitoring report	✓	✓	✓

* Available reports are aligned to tagged resources which have a CLM agent or gateway installed, or if you have the affiliated solution enabled.

Solution Health and Maintenance

Azure Product Support

Azure Product Support Services are applicable only to Customers who purchase their Azure solutions, products and cloud consumption-based services through NTT DATA as a reseller of Azure. Azure Product Support Services are otherwise outside the scope of this Service Description, but may be offered in addition to the Services outlined herein by executing a separate Service Description.

Where applicable, NTT DATA will provide the following as Azure Product Support Services, which shall be further described under a separate Service Description:

- Determining product support requirements for features and functionality of specific Azure services and solutions
- Making recommendations for optimal performance of Azure products
- Providing affiliated solutions that may include third-party tools to address common use cases (for example: disaster recovery, backup, etc.)
- Providing industry best practice guidance and support as further agreed to address a specific Azure environment

If the Customer purchases their Azure resources directly from Azure or a third-party reseller (i.e. not from NTT DATA), it shall be assumed the Customer purchased any Azure product support through the resale channel.

Performance Tuning and Preventative Maintenance

Performance tuning and preventative maintenance services differ by workload, and includes scanning the resource to check for possible issues and reviewing the resource health status. NTT DATA will investigate issues that surface and will apply corrections where noted below or as identified during the onboarding process for the Azure products identified in the Services Coverage Product Table (page3).

- Capacity, demand, and utilization review and improvement planning.

- Partnering on patching and service updates. Only patches or updates provided by the workload's technology provider (for example, patches from Microsoft for Windows updates) will be applied with Customer consent.
- Evaluate data movement trends, speed and behaviors, if performance is regularly below preferred thresholds, adjust settings or resize resources to meet desired output.
- Assess the storage connected to the VM, for the desired level of performance and increase the IOPS to accommodate the workload.
- Benchmark and monitor workload performance, against predefined metrics provided by the Customer during onboarding.
- Monitor queue depth, healthy host counts, number of connections, rejected connections and response time of Load Balancer to ensure workload performance meets requirements. Validate the Load Balancer is properly configured to support expected influx of traffic as requested or scheduled by the Customer.
- Evaluate auto-scaling groups and back end scalability of the target groups, adjust minimum/maximum thresholds accordingly or per schedule.

Bandwidth and Network Management

Bandwidth and network management Services are included in this Service Description offering. Applicable network scenarios considered in scope are point to site, site to site and virtual private network ("VPN") gateway, Azure ExpressRoute, and the specific activities for which include:

- Monitoring and validating that network connectivity is performing within limits against the pre-defined configurations, determined from dependency mapping or stated specifications.
- Advising on whether public cloud VPN is functioning as designed and within thresholds identified during onboarding
- Rescheduling activities to take place after peak business hours, where possible
- Resolving issues and alerts associated to network connectivity, as defined during the onboarding process or through change requests. Some resolution efforts may require Customer participation and support due to proximity of components and security features of their network. Support is limited to the networking components within the Customer's Azure environment.

Performance Analysis & Cost Optimization

Performance analysis* will vary based on the specific environment configurations and business thresholds coordinated in advance with the Customer, and shall include (where applicable) the following:

- Network and bandwidth utilization analysis
- Evaluation of compute usage and aligned performance metrics, including availability analysis
- Audit of configuration in alignment with Customer requirements
- Recommendations to improve performance
- Quarterly cost optimization* review and recommendations with the intent to identify opportunities to reduce Azure consumption based expenses. Findings will be based on technical review of the NTT DATA Engineering team and results from Azure Advisor.

*Performance Analysis and Cost Optimization service entitlements are applicable to the Azure products defined in the Services Coverage Product Table (page 3).

Operating System Administration

NTT DATA will provide operating system administration Services for Windows and Linux, as supported by Azure. Any operating system which no longer has support from its vendor will be supported by NTT DATA on a commercially reasonable efforts only basis with no service levels, penalties, or other remedies applying to any such activities. NTT DATA strongly recommends maintaining operating system currency for security and operability purposes.

Operating system administration activities will include (where applicable) the following:

- Troubleshooting of reported problems stemming from the Customer, a system generated error or review of activity logs
- Configuration updates/additions/removals
- Software installation support for supported Azure VM instances
- Performance reviews
- System log analysis
- Network connectivity (in coordination with network administrators)
- Configuration, addition, removal, consolidation or file systems

Operating system administration Services excludes:

- Support for applications installed onto virtual machines
- Support for infrastructure services beyond their availability (*i.e.* IIS (Internet Information Services), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), etc.)
- Coding or scripting of programs
- Kernel-level customizations

Operating system administration Services are available for:

Windows: Windows Server 2008 and newer general availability (GA) releases
Linux: Red Hat Enterprise Linux (RHEL) and top Linux distributions

Identity and Access Management

NTT DATA will perform the following basic identity and access management activities in support of the Customer's Azure environment:*

- Add and/or remove users to and from security groups
- Resetting passwords, as applicable
- Add and/or remove users to and from specific resources, devices and regions
- Adjust permissions to resources
- Review audit logs on a weekly basis to assess anomalies
- Assess connectivity to associated multi factor authentication ("MFA") and/or identity management solutions, such as Active Directory. (Outages and administration stemming from MFA and identity management solutions will be escalated to the Customer. It is the Customer's responsibility to

support resolution of such; NTT DATA's support will be restricted to the Azure Active Directory connection only).

* In alignment with industry-best practices, NTT DATA has adopted a least-privilege access policies to help protect the Customer's data and adhere to governance processes. All identity and access requests must be evaluated by the designated Customer contact, submitted as a service request and validated by the NTT DATA Service Delivery Manager.

Firewall Management

NTT DATA will monitor and support enterprise-grade and cloud-compatible firewalls connected to the Customer's Azure environment.

As part of the Services, NTT will monitor an applicable firewall based on key performance requirements, such as solution health, status and functionality. Further monitoring parameters may include CPU, memory and affiliated limits, software update availability and policy application.

NTT DATA will support patching across the system for Customer-approved patches and provide 24x7 support. The Customer may request modifications to the policies, configuration or settings through the change management process as defined within this Service Description. The Customer may also submit Service Requests to obtain audit logs, as defined within this Service Description. Audit log analysis support is available separately from the Services on a time and material basis.

Event Management

Cloud Lifecycle Management Portal with alert dashboard

The NTT DATA Cloud Lifecycle Management tool (the "Portal" or "CLM") is a multi-tenant Software-as-a-Service ("SaaS") solution that delivers IT operations lifecycle management capabilities that spans public and private cloud infrastructure, as well as application elements.

The CLM includes the following features: solution monitoring, management, remote console, executive dashboard, as well as on-demand, weekly and monthly reports.

The alert dashboard component of CLM allows the NTT DATA team to view and manage alerts, create incident and problem tickets, as well as setup automated alert escalations.

The CLM can integrate with over 20 Information Technology Service Management ("ITSM") and solution management tools, including NTT DATA Service Operations Manager, ServiceNow, BMC Remedy, Nagios, and New Relic. Integration capabilities can allow NTT DATA and the Customer to analyze systemic issues that may be impacting performance.

The Customer will be provided account credentials and access to NTT DATA's CLM during the onboarding process.

Performance and availability monitoring

NTT DATA will perform the standard monitoring Services for the agreed upon set of resources or instances in the Customer's public cloud environment*. All cloud resources will be monitored based on parameters determined during onboarding, specific to the Customer's key performance indicators. Changes to metrics monitored can be supported through a service request.

- Performance monitoring: cloud gateway, storage, virtual machines and network
- Availability monitoring: instances, volumes, infrastructure, network and cloud provider (ping and heartbeat)
- Track cloud inventory (instances and volumes)
- Monitor Azure resources using Log Analytics
- Network stability, traffic and performance
- Cloud storage environment
- Service topology monitoring
- Detailed monitoring for virtual machine ("VM") instances to ensure utilization is within specified parameters

*NTT DATA will provide monitoring and alert management Services (see the Alert Management section below for details) on all resources in the Customer's Azure environment, but the scope of operational and incident support will remain limited to the core infrastructure components and products as defined in the Services Coverage Product Table (see page 3). It will be the Customer's responsibility to correct issues outside of the product scope specified in such table.

The Customer is required to have a CLM license on each resource or set of devices in order for NTT DATA to perform monitoring and alert management.

Alert management

NTT DATA will perform the following alert management Services for all resources or instances in the Customer's public cloud environment:

- Alert integration
- Alert validation
- Alert review and analysis
- Event acknowledgement and incident summary provided to Customer; see incident management for further details

As noted in the Performance and Availability Monitoring section above, NTT DATA will provide Alert Management over all resources in the Customer's Azure environment, but operational and incident support as described in the Service Description is limited to the infrastructure components listed in the Service Coverage Product Table (page 3). All other Azure services and resources are considered out of scope. If management of out of scope resources is needed, please contact your NTT DATA representative.

The Customer is required to have a CLM license on each resource or set of devices in order for NTT DATA to perform monitoring and alert management

Incident management

24x7 Service Desk

Customer may assign up to five (5) named contacts to contact the NTT DATA service desk on behalf of the Customer. The NTT DATA service desk is a central point of contact for handling the following technical issues:

- Initial troubleshooting and escalation of incidents within the defined SLAs outlined in Appendix A
- Respond to "how to" questions, such as how to provision or remove cloud instances and migrate data across regions.
- Respond to access issues and requests, see Identity Management for details.
- Support incidents, including:
    - Incident classification
    - Incident prioritization
    - Incident notification
    - Incident escalation
    - High criticality incident management

The service desk can be contacted at:

- Toll-Free number (833-468-8253) – available 24x7
- Email at Cloud.Managed.Services@nttdata.com

Troubleshooting and remediation

NTT DATA predefined standard operating procedure ("SOP") based remediation will be executed when an alert or event is triggered for Azure infrastructure components and products listed in the Service Coverage Product Table (page 3).

Incidents raised are responded to within the predefined SLA as defined in Appendix A to this Service Description.

Specific responses to common issues are discussed, and often determined, during the onboarding process. In some instances, NTT DATA can automate responses to improve resolution time and effort, such occasions are discussed with the Customer in advance of applying such processes.

Incidents, events and issues requiring standard troubleshooting and remediation will follow the process outlined below. Additional details are also available in Appendix A.

Remediation Process:

- Incoming alerts will be validated by the Level 1 ("L1") engineer to identify false alerts or if no action is required

- If the alert was identified as legitimate, the L1 engineer will create an incident or event ticket in the ITSM or CLM portal as identified during onboarding.
- The L1 engineer will investigate the source of the issue and identify applicable SOPs to resolve.
- L1 engineer will implement standard resolution protocols based on findings from the investigation.
- If testing on the Customer side is required, the L1 engineer will reach out to the designated Customer contact to arrange an appropriate time for testing. Resolutions SLAs, as described in Appendix A, will be considered paused while awaiting Customer response or support.
- L1 engineer will monitor the performance after applying the resolution.
- If no further alert is triggered, the incident is closed in the ITSM or ticketing tool.
- If the SOP fails to resolve the problem, the ticket will be updated and escalated to the Level 2 ("L2") engineering team for further troubleshooting and remediation.
- The L2 engineer will investigate the issue and apply identified SOP based corrections. If the resolution effort is successful and further alarms are not triggered, the L2 engineer will notify the Customer and close the incident in the ticketing system.
- Dependent upon the trigger, the L2 engineer may need to escalate the issue to the Level 3 ("L3") engineering team or NTT DATA domain lead to support the investigation and subsequent resolution. The L2 engineer will engage the appropriate NTT DATA subject matter experts to resolve the issue.
- The L3 engineer will review actions taken and utilize their advanced knowledge of the respective cloud platform to assist in resolution of the issue.
- The L3 engineer will apply available workarounds, as available. Due to complexities at this escalation stage, the L3 engineer may need to work with a designated Customer contact for testing or to discuss alternative options, see Escalation management for further details.
- The L3 engineer will use commercially reasonable efforts to troubleshoot and remediate potential issues for the Azure products noted in the Services Coverage Product table (page 3).

Escalation management

In certain cases, an issue may be pervasive or impactful enough that full resolution is not possible or may be due to a technical issue with the cloud or third-party provider. Such cases will be addressed with the cloud provider or vendor, where a vendor support agreement is in place (as applicable), with appropriate options presented to a Customer before action is taken.

NTT DATA will contact the applicable technical support team to address the issue and gain support for further troubleshooting and remediation, if the resource is impacting performance within the Azure environment.

Customers must have valid vendors' maintenance or technical agreement in place, where applicable. The Customer must authorize NTT DATA to act on their behalf when coordinating with the vendor's support team. **Service scope shall be limited to a commercially reasonable efforts only basis, if a vendor maintenance / technical support agreement is expired or if software or hardware is placed into 'End of Life'.** In the event NTT DATA's commercially reasonable efforts do not provide a suitable workaround for solutions that are no longer supported by the vendor, further troubleshooting will need to be completed by the Customer or through a separate agreement with NTT DATA Services. Service

Level Agreements and performance credits as described in the service description and Appendixes do not apply to such scenarios.

Incidents raised are responded to within the predefined SLA as defined in Appendix A, with the exclusion of issues escalated to third-party or cloud providers.

Root Cause Analysis and Resolution

Customers are entitled to root cause analysis services for Critical incidents for the Azure resources shown in the Services Coverage Product Table (page 3), and as defined in Appendix A, to identify underlying problems, issues and risks, and is comprised of the following advanced level analysis and issue remediation tasks:

- Perform alert and incident analysis to reduce unnecessary noise in the environment
- Perform root cause analysis to prevent repetitive incident occurrences
- Document analysis results for quick remediation in the future
- Develop SOPs or automated responses for new or recurring incidents
- Provide insights to the service delivery team on best practice recommendations
- Coordination with affiliated technology providers to address performance issues and outages, as described in Escalation Management.

Root cause analysis ("RCA") is available upon request for Critical Priority incidents, as defined in Appendix A. NTT DATA targets RCA resolution for Critical incidents within 72 hours. Due to the variables, complexities and dependencies on outside factors, the aforementioned timelines are not guaranteed, but based on a commercially reasonable effort basis. Service or Performance Credits will not be offered for RCA, but NTT will use the scenario to drive systemic improvements of service delivery to help prevent recurrence.

Exclusions

For the avoidance of doubt, the following activities are not included in the scope of this Service Description:

- Any services, tasks or activities other than those specifically noted in this Service Description.
- The development of any intellectual property created solely and specifically for the Customer.
- If Customer chooses to use its own element managers or management platforms, and integrate with the Portal, all limitations of those platforms will carry over and NTT DATA does not take any responsibility or liability for any problems, issues or breaches directly, or indirectly, resulting from those platforms.
- If Customer has a non-standard architecture, does not follow industry best practices, or has insufficient capacity on their devices or in their environment, NTT DATA service commitments will be restricted to response SLA only.
- If Customer has non-standard environments, NTT DATA will not provide resolution SLA.
- If Customer does not implement NTT DATA recommendations for reducing alert and incident noise, service level commitments on those devices or resources will not apply. NTT DATA reserves the

right to turn off applicable monitors for resources with pervasive alerts in such circumstances, which will be discussed with the Customer before the monitor is turned off.

- Service level commitments will not apply to environments that are not maintained at current/appropriate patch, firmware and security levels as a result of Customer preference or application requirements.
- NTT DATA will not be responsible for defects or malfunctions in third party software encountered during the process of troubleshooting, resolving, patching, upgrading or performing any other related service.
- Application management services and support of applications, including, but not limited to: development, testing, management, issue and problem resolution, scheduling and knowledge management, except where specifically mentioned elsewhere.
- Costs of any dedicated circuits.
- Any other software licenses required by Customer not specifically listed as in scope.
- End user hardware maintenance.
- Procurement of remote access security tokens (i.e. RSA) or similar authentication hardware devices.
- Additional or third-party tools, licenses or subscriptions
- Azure service or utilization charges are not included within the scope of this service

This Service Description does not confer on Customer any warranties which are in addition to the warranties provided under the terms of your master services agreement or Agreement, as applicable.

THESE SERVICES ARE DESIGNED BASED ON INDUSTRY STANDARD PRACTICES, NOT TO MEET SPECIFIC COMPLIANCE OR REGULATORY REQUIREMENTS (SUCH AS PAYMENT CARD INDUSTRY SECURITY STANDARD (PCI DSS), HIPAA, ETC). THE CUSTOMER IS RESPONSIBLE FOR KEEPING SUCH DATA AND VIRTUAL MACHINES WITH SUCH DATA OUT OF THE ENVIRONMENT BEING MANAGED BY THIS SERVICE AND SHALL PROVIDE A WRITTEN REQUEST TO NTT DATA PRIOR TO MOVING ANY SUCH DATA OR VIRTUAL MACHINES INTO ANY ENVIRONMENT MANAGED BY THIS SERVICE.

NTT DATA can partner with you to evaluate compliance or regulatory needs and requirements, which will be addressed on a case by case basis subject to a change request, and which may be subject to additional obligations (including a Business Associate Agreement where HIPAA would be applicable to the services provided by NTT DATA).

Out-of-scope services

The following list of service activities are not within the scope of described Services provided under this Service Description. These activities can be delivered separately on a time and materials (T&M) basis.

Out-of-scope monitoring

- Customizations to monitoring templates are out of scope - any request for customizations to monitoring templates and/or default profiles are subject to review and acceptance by NTT DATA. NTT DATA will work with the Customer during onboarding to configure monitors to the metrics required, but there are tool and process limitations that prohibit excessive, adhoc and intermittent customization

Out of scope Service Requests

- New solution deployment, provisioning, configurations, and migrations
- Setup of new internal replication process
- Setup of file archiving policies
- Patches, updates, maintenance and support for applications
- Perform implementation or migration of storage
- New site architect/design/re-design/migration of network infrastructure or remote office
- New firewall rules and routing table modifications
- DNS changes and IP allocations
- Network topology changes
- Defining security policies on behalf of the customer
- Auditing firewall logs for anomalies

Out of scope product coverage

- This service description addresses operational support for the Azure infrastructure elements as described in the Service Coverage table, no other products are considered in scope. NTT DATA will provide monitoring and alert management for additional Azure products (such as SQL Server, Containers), but will not manage, troubleshoot or administer these resources. Services may be available to cover these items outside of the scope of this service description.

- Application management and support is not included in the scope of the service offering

- Operating systems, solutions and such products that are not deemed compliant with Azure will not be supported due to infrastructure or platform conflicts.

Any items not explicitly covered within this document are considered out of scope. If the Customer requires support not in scope of this offering, please work with your NTT DATA contact to address such needs.

Offer Specific Customer Responsibilities

Customer will support onboarding activities set forth herein for the Service. Onboarding activities include:

- Customer requirements gathering
- Validation of configuration data and system integrations as applicable
- Review initial alert threshold values
- Provide escalation and notification contacts
- Customer will provide timely access to Customer resources, including but not limited to, virtualization administrators, engineering and project management. NTT DATA and the Customer will agree on standard access protocols.
- Customer is responsible for all design and implementation of network security settings and requirements definitions, with the exception of NTT DATA provided public cloud infrastructure setup services, which are addressed through a separate service description or Statement of Work (SOW).
- Customer is responsible for all application development, management and performance monitoring, in addition to all database development and management.

- Customer is responsible for managing its virtual and local (or on-premises) environment.
- Customer is responsible for any changes/modifications/deletions to Customer's virtual or local environment.

General Customer Responsibilities

Authority to Grant Access. Customer represents and warrants that it has obtained permission for both Customer and NTT DATA to access and use, whether remotely or in-person, Customer-owned or licensed software, hardware, systems, the data located thereon and all hardware and software components included therein, for the purpose of providing these Services. If Customer does not already have that permission, it is Customer's responsibility to obtain it, at Customer's expense, before Customer asks NTT DATA to perform these Services.

Customer Cooperation. Customer understands that without prompt and adequate cooperation, NTT DATA will not be able to perform the Service or, if performed, the Service may be materially altered or delayed. Accordingly, Customer will promptly and reasonably provide NTT DATA with all cooperation necessary for NTT DATA to perform the Service. If Customer does not provide reasonably adequate cooperation in accordance with the foregoing, NTT DATA will not be responsible for any failure to perform the Service and Customer will not be entitled to a refund.

Data Backup. Customer will complete a backup of all existing data, software and programs on all affected systems prior to the delivery of this Service and retain ownership of backups during delivery of this Service. Customer should make regular backup copies of the data stored on all affected systems as a precaution against possible failures, alterations, or loss of data. NTT DATA WILL HAVE NO LIABILITY FOR:

- ANY OF YOUR CONFIDENTIAL, PROPRIETARY OR PERSONAL INFORMATION; AND/OR
- LOST OR CORRUPTED DATA, PROGRAMS OR SOFTWARE;
- DAMAGED OR LOST REMOVABLE MEDIA; AND/OR
- THE LOSS OF USE OF A SYSTEM OR NETWORK ARISING OUT OF OR IN CONNECTION WITH THE SERVICE OR ANY ACTS OR OMISSIONS, INCLUDING NEGLIGENCE, BY NTT DATA OR A THIRD-PARTY SERVICE PROVIDER.

NTT DATA will not be responsible for the restoration or reinstallation of any programs or data within the context of this Service Description.

Third Party Warranties. These Services may require NTT DATA to access hardware or software that is not manufactured by NTT DATA. Some manufacturers' warranties may become void if NTT DATA or anyone else other than the manufacturer works on the hardware or software. Customer will ensure that NTT DATA's performance of Services will not affect such warranties or, if it does, that the effect will be acceptable to Customer. NTT DATA does not take responsibility for third party warranties or for any effect that the Services may have on those warranties.

NTT DATA Services Terms & Conditions

This Service is provided subject to and governed by Customer's separate signed master services agreement with NTT DATA that explicitly authorizes the sale of this Service. In the absence of such agreement, depending on Customer's location, this Service is provided subject to and governed by NTT

DATA's Cloud Solutions Agreement (as applicable, the "Agreement"). Please see the table below which lists the URL applicable to your Customer location where your Agreement can be located. The parties acknowledge having read and agree to be bound by such online terms.

Customer Location	Terms & Conditions Applicable to Your Purchase of NTT DATA Services	
	Customers Purchasing NTT DATA Services Directly From NTT DATA	Customers Purchasing NTT DATA Services Through an Authorized NTT DATA Reseller
United States	www.nttdataservices.com/en-us/contracts	www.nttdataservices.com/en-us/contracts
Canada	Available on request	Available on request
Latin America & Caribbean Countries	Mexico: Your terms and conditions of sale will be sent to you along with your quote	Not applicable
Asia-Pacific-Japan	Available on request	Service Descriptions and other NTT DATA service documents which you may receive from your seller shall not constitute an agreement between you and NTT DATA but shall serve only to describe the content of Service you are purchasing from your seller, your obligations as a recipient of the Service and the boundaries and limitations of such Service. As a consequence hereof any reference to "Customer" in this Service Description and in any other NTT DATA service document shall in this context be understood as a reference to you whereas any reference to NTT DATA shall only be understood as a reference to NTT DATA as a service provider providing the Service on behalf of your seller. You will not have a direct contractual relationship with NTT DATA with regards to the Service described herein. For the avoidance of doubt any payment terms or other contractual terms which are by their nature solely relevant between a buyer and a seller directly shall not be applicable to you and will be as agreed between you and your seller.
Europe, Middle East, & Africa	Available on request	Service Descriptions and other NTT DATA service documents which you may receive from your seller shall not constitute an agreement between you and NTT DATA but shall serve only to describe the content of Service you are purchasing from your seller, your obligations as a recipient of the Service and the boundaries and limitations of such Service. As a consequence hereof any reference to "Customer" in this Service Description and in any other NTT DATA service document shall in this context be understood as a reference to you whereas any reference to NTT DATA shall only be understood as a reference to NTT DATA as a service provider providing the Service on behalf of your seller. You will not have a direct contractual relationship with NTT DATA with regards to the Service described herein. For the avoidance of doubt any payment terms or other contractual terms which are by their nature solely relevant between a buyer and a seller directly shall not be applicable to you and will be as agreed between you and your seller.

Customer further agrees that by renewing, modifying, extending or continuing to utilize the Service beyond the initial term, the Service will be subject to the then-current Service Description available for review at www.nttdataservices.com/en-us/contracts.

To the extent that any terms of this Service Description conflict with any terms of the Agreement, the terms of this Service Description will prevail, but only to the extent of the specific conflict, and will not be read or deemed to replace any other terms in the Agreement which are not specifically contradicted by this Service Description.

By placing your order for the Services, receiving delivery of the Services, utilizing the Services or associated software or by clicking/checking the “I Agree” button or box or similar on the nttdataservices.com website in connection with your purchase or within a NTT DATA software or Internet interface, you agree to be bound by this Service Description and the agreements incorporated by reference herein. If you are entering this Service Description on behalf of a company or other legal entity, you represent that you have authority to bind such entity to this Service Description, in which case “you” or “Customer” shall refer to such entity. In addition to receiving this Service Description, Customers in certain countries may also be required to execute a signed Order Form.

Supplemental Terms & Conditions Applicable to Cloud & SaaS Services

1. Term of Service. This Service Description commences on the date listed on your Order Form and continues through the term ("**Term**") indicated on the Order Form. As applicable, the number of systems, licenses, installations, deployments, managed end points or end-users for which Customer has purchased any one or more Services, the rate or price, and the applicable Term for each Service is indicated on Customer's Order Form. Unless otherwise agreed in writing between NTT DATA and Customer, purchases of Services under this Service Description must be solely for Customer's own internal use and not for resale or service bureau purposes.

2. Important Additional Information

   A. Payment for Hardware Purchased With Services. Unless otherwise agreed to in writing, payment for hardware shall in no case be contingent upon performance or delivery of cloud or SaaS services purchased with such hardware.
   B. Optional Services. Optional services (including point-of–need support, installation, consulting, managed, professional, support, security or training services) may be available for purchase from NTT DATA and will vary by Customer location. Optional services may require a separate agreement with NTT DATA. In the absence of such agreement, optional services are provided pursuant to this Service Description.
   C. Assignment. NTT DATA may assign this Service and/or Service Description to qualified third party service providers.
   D. Geographic Limitations and Relocation. This Service is not available at all locations. Service options, including service levels, technical support hours, and on-site response times will vary by geography and certain options may not be available for purchase in Customer's location, so please contact your sales representative for these details.

Appendix A

Service Level Agreements (SLA)

NTT DATA will follow an SLA-based service delivery model for the Services provided under this Service Description. For the avoidance of doubt, the parties hereby expressly acknowledge and agree that NTT DATA will use commercially reasonable efforts to meet the response SLAs and resolution SLAs specified below in this Appendix A.

The Customer should inform NTT DATA of any device addition or deletion, as well as changes to environment that might impact the SLA. The following table describes the various priority levels associated with incidents. The sources of alerts are either from the monitoring system or from user requests entered via the ticketing system, phone calls or e-mails.

- Resolution SLAs do not apply for those cases that are escalated to vendor technical support, hardware vendors, Internet Service Provider (ISP), cloud platform provider, or third party vendors, as well as connected devices/resources that are outside of the NTT DATA management scope as described in this Service Description
- Resolution SLA timer is paused during ticket statuses where action is not with NTT DATA, for example: (a) "Waiting for SP or Client" (b) "On-Hold" (c) "Under Observation" (d) "Resolved"

- Individual Customer environments and processes influence service level compliances. In cases where the above SLAs cannot be met, NTT DATA will publish those details during the pre-transition / planning phases
- SLAs will be effective after ninety (90) days of steady state operations or as published during pre-transition phases

Priority	Response SLA (Business Hours)	Resolution SLA*	Measured
P1: Critical (Sev 1)	95% within 15 Min	95% of the cases resolved in 4 hours	Monthly
P2: High (Sev 2)	95% within 30 Min	95% of the cases resolved in 8 hours	Monthly
P3: Medium (Sev 3)	90% within 8 Hours	90% of the cases resolved in 72 hours	Monthly
P4: Low (Sev 4)	90% within 36 Hours	90% of the cases resolved (or requests fulfilled) in 240 business hours.	Monthly

* Resolution SLA applies only to solutions managed by NTT DATA.

SLA Calculations

Response time will be measured as the time a ticket is set to an in progress state or assigned to an individual, whichever is earliest minus the date and time a ticket was opened.

Resolution time will be measured as the time a ticket is in a resolved state (a state at with NTT DATA has completed their responsibility for an incident or request) minus the date and time a ticket of the ticket response.

Priority based escalations

The 'Severity Levels' section below describes the various levels of incidence severity in detail.

Priority	Phone	Ticket
P1: Critical (Sev 1)	✓	✓
P2: High (Sev 2)	✓	✓
P3: Medium (Sev 3)		✓
P4: Low (Sev 4)		✓

Severity levels

Priority Level 1 (P1) – Critical Incidents – Severity Level 1

Description: This is an EMERGENCY condition that significantly restricts the use of the cloud platform itself to perform any critical business functions. This could mean that several departments of the Customer are impacted.

The ticket could have originated from multiple sources: an end-user or NTT DATA staff.

Target for response: Follow-up within fifteen (15) minutes of receiving notification or alert a notification (such as email, phone call or voicemail) is sent to the appropriate Customer contact and a ticket is created. A status update will be provided within two (2) hours of the initial incident.

Target for resolution: The target resolution time for is P1 incident is four (4) hours. In some cases the solution may require a temporary workaround until the ultimate solution can be investigated and implemented. In these cases, the ticket will be closed when a workaround is put in place and service is restored. A new ticket will be opened with a lower priority to evaluate alternative solutions. Target resolution time can depend on external parameters including coordination with outside vendors. In the event of an external vendor who does not respond in time, the Customer will be notified.

Inability to use any critical cloud instance(s) by the Customer will require immediate attention by NTT DATA.

Status update: A NTT DATA support team member will provide regular status updates throughout the day until a resolution or workaround can be found.

Response procedure: After a critical incident is reported to the Support team either via CLM or by a Customer Contact:

- The Support representative will report the issue immediately to all designated customer contacts, the incident is logged and it is assigned to the appropriate owner.
- The Support representative will communicate regular status updates to the Customer contact who reported the incident.
- If it is appropriate, the CDE will call an emergency coordination meeting with Support team to discuss an action plan for resolution, including possible recovery efforts.
- The result of this meeting will be reported to the appropriate personnel on the Customer team and the NTT DATA account team. An update will be provided to the Customer stakeholder by the close of business by the CDE or Support engineer.
- There will be a post-incident meeting to discuss the Priority 0 incident in detail. In addition, for Customers who have Cloud Operations Management level of service, the incident will be put through the problem management process.

Escalation procedure:

- Escalation will occur if the incident has not been resolved within four hours and be reassigned to a Level 2 (L2) engineer who will become the incident owner.
- The Support Representative will obtain status updates from the (L2) incident owner and involve the appropriate Customer personnel and/or NTT DATA domain leads if the issue is not resolved within 4 hours

Examples of Critical Incidents:

- Mission-critical server is down
- Cloud instances are down
- NTT supported business-critical components or workloads hosted in the cloud environment are down
- Several users or groups have incidents

Priority Level 2 (P2) – High Priority Incidents – Severity Level 2

Description: A major function, NTT supported business-critical component or workload hosted in your cloud environment, or infrastructure device is severely impacted and there are no quick workarounds available. It is deemed high because of its business or financial impact. The ticket could have originated from multiple sources: an end-user, Customer IT, NTT DATA support staff, or an automatic notification from the CLM monitor on a connected server, network, or application. Substantially degraded performance of any critical system is also categorized as a Priority 2. The primary difference between a P1 and P2 incident is how widespread the incident is. A P1 may impact the entire department or company, whereas a P2 may impact a limited set of users. There is no difference in the amount of resources that will be devoted to a P2 incident compared to a P1 incident.

Target for response: Follow-up within thirty (30) minutes of receiving a notification or alert a notification (such as email, phone call or voicemail) is sent to the appropriate Customer contact and a ticket is created. A status update will be provided by the close of business or sooner if one is available.

Target for resolution: Within eight (8) hours, but it is possible that the solution may require a temporary workaround instead of the final solution. In these cases, the ticket will be closed after workaround is implemented. A new ticket will be opened with a lower priority to evaluate all possible options. Target resolution time can depend on external parameters including coordination with outside vendors.

Status update: Will be provided by Incident Owners to the user by close of business and then on a daily basis.

Failure to respond or report status in a timely manner will result in escalation.

Response procedure: After a High Priority Incident is reported to the Support representative:

- The L1 Support engineer will report the incident to the appropriate domain leads and NTT DATA delivery manager. The Support engineer logs the incident and assigns it to an Incident Owner. The Incident Owner will investigate the incident immediately.
- The Incident Owner will then be responsible for communicating status to the Customer contact until the incident is resolved or priority is downgraded based on findings of the initial investigation.
- These updates will continue until resolution of the incident or an acceptable workaround is found. The Incident Owner will close the incident when it is resolved.

Escalation procedure:

- Escalation to the Level 2 Engineering team will occur if the incident has not been resolved within eight hours or if a resolution is not underway.
- The L2 Incident Owner will involve the appropriate Customer personnel and/or NTT DATA domain leads if an issue remains unresolved.

Examples of High Priority incidents:

- External user is not able to login or see network
- Non-mission critical server is down
- Non-core network element is down

Priority Level 3 (P3) – Medium Priority Incidents – Severity Level 3

Description: The reported incident may restrict the use of one or more features of the system, but the business or financial impact is not severe. The ticket could have originated from multiple sources: an end-user, Customer IT, NTT DATA staff, or notification from the CLM monitor on a server, network or application. The reported incident may be of a critical nature, but sometimes the incident can be downgraded to a Priority 3 because a viable workaround is available as a temporary solution. Many incidents are categorized as a P3 because there is a business justification or a financial impact on completing the task within five (5) business days. Sometimes a critical enhancement to existing functionality can be categorized as a P3 based on the critical nature of its due date and severe impact on business.

Target for response: Within eight (8) hours of an alert or request a notification (such as email, phone call or voicemail) is sent to the appropriate Customer contact and a ticket is created.

Target for resolution: Seventy two (72) hours

Status update: Will be provided to the Customer upon incident resolution. Failure to respond or report status on a timely manner will result in escalation.

Response procedure: After a Medium Priority Incident is reported to the Support team:

- The L1 Support representative will create the ticket and assign it to an Incident Owner.
- The Incident Owner will be responsible for managing the ticket and communicating status to the Customer, including approximate resolution date.
- It will be the responsibility of the Incident Owner to provide a status update pertaining to the major incident within seventy two (72) hours from the time the incident is originally reported.
- The Incident Owner will continue to provide updates as agreed upon by the reporter of the incident or request, until resolution or an acceptable workaround is found.
- The Incident Owner will close the incident when there is confirmation of resolution.

Escalation procedure:

- Escalation will occur if the incident has not been resolved within 72 hours.
- The Incident Owner will involve the appropriate Customer and/or NTT DATA domain leads, if the issue is not resolved or the solution is unknown within the 72 hour window.

Examples of Medium Priority Incidents:

- Termination requests
- Customer can log in, but cannot access application
- An outside salesperson has a network incident, and/or VPN related incident
- Any request or incident that has a direct impact on Customer's daily operations

Priority Level 4 (P4) – Low Priority Incidents – Severity Level 4

Description: The reported anomaly in the system does not substantially restrict the use of one or more features of the product to perform necessary business functions. The ticket could have originated from multiple sources: an end-user, Customer IT, NTT DATA Support, or a notification from the CLM monitor on a server, network, or application that is deemed minor. This severity level is reserved for issues that will not significantly impact operations.

Target for response: Within thirty six (36) hours of an alert or request a notification (such as email, phone call or voicemail) is sent to the appropriate Customer contact and a ticket is created.

Target for resolution: Agreed upon due date with the user or appropriate personnel (otherwise treated as ten (10) business days).

Status update: Will be provided to the user by the Incident Owner upon resolution of the incident.

Response procedure: After a low severity incident is reported to the Support team:

- The L1 Support Engineer will create the ticket for the incident and assign it to an Incident Owner.
- The Incident Owner will be responsible for managing the ticket and communicating status to the Customer, including the approximate resolution date.
- Updates from the Incident Owner will continue as agreed upon by the Customer resolution or an acceptable workaround is found.
- The Incident Owner will close the incident when there is confirmation of resolution.

Escalation procedure:

- Escalation will occur if the incident has not been resolved within ten days
- The Incident Owner will involve the appropriate Customer and/or NTT DATA domain leads, if the issue is not resolved or the solution is unknown within the ten day timeframe

Examples of Minor Incidents:

- Low impact changes in IT processes that are of a non-critical nature
- Any server software or hardware incident for which a workaround exists

Performance Credits

During the term of the applicable Order Form between NTT DATA and Customer for Cloud Operational Excellence for Azure and following the commencement date specified for such service levels, NTT DATA will use commercially reasonably efforts to acknowledge and resolve Severity Level 1, Severity Level 2, Severity Level 3, and Severity Level 4 incidents in accordance with the below-listed service levels, collectively referred to as Performance SLAs. If NTT DATA does not meet a Performance SLA, and so long as Customer's account with NTT DATA is current and not suspended, Customer may be eligible to receive the below-listed performance credit (a "Performance Credit,"). NTT DATA will use reasonably suitable monitoring tools to collect and report on Performance SLA data.

NTT DATA Performance credits are exclusive to services rendered by NTT DATA's Service Delivery team and does not extend to the cloud platform or infrastructure provider or and third party vendor or solution provider.

Definitions: The following definitions apply to these Performance SLAs:

- "**Measurement Period**" means the time during, or frequency by which, a Performance SLA is measured.
- "**Reporting Period**" means the periodic evaluation and reporting frequency for each individual Performance SLA.
- "**Resolution Time**" means the elapsed time between (i) the moment a service ticket is opened in the NTT DATA Service Management Workflow System, until (ii) the moment the service ticket is

closed in accordance with the NTT DATA procedures manual because (A) the incident is resolved and Customer has not provided an accurate notification to NTT DATA that the incident has not been resolved; or (B) a temporary solution that addresses all of the material aspects of the incident (a "Workaround") is provided.

- "**Service Management Workflow System**" means the request management workflow system that enables certain Customer-approved requestors to submit incident, systems change and request management workflows to NTT DATA.
- "**Severity Level 1**" as the meaning provided for Priority Level 1 (P1) in the Service Levels section above
- "**Severity Level 1 Incident Acknowledgment Time**" shall mean the elapsed time between submission of a Severity Level 1 incident in the Service Management Workflow System and the acceptance by a technician through the Service Management Workflow System of an assignment to address the incident.
- "**Severity Level 2**" as the meaning provided for Priority Level 2 (P2) in the Service Levels section above
- **"Severity Level 2 Incident Acknowledgment Time"** shall mean the elapsed time between submission of a Severity Level 2 incident in the Service Management Workflow System and the acceptance by a technician through the Service Management Workflow System of an assignment to address the incident.
- **"Severity Level 3"** as the meaning provided for Priority Level 3 (P3) in the Service Levels section above
- "**Severity Level 3 Incident Acknowledgment Time**" shall mean the elapsed time between submission of a Severity Level 3 incident in the Service Management Workflow System and the acceptance by a technician through the Service Management Workflow System of an assignment to address the incident.
- "**Severity Level 4**" as the meaning provided for Priority Level 4 (P4) in the Service Levels section above
- "**Severity Level 4 Incident Acknowledgment Time**" shall mean the elapsed time between submission of a Severity Level 4 incident in the Service Management Workflow System and the acceptance by a technician through the Service Management Workflow System of an assignment to address the incident.

Incident Acknowledgement Time SLA

Objective	Measures the aggregate acknowledgment time for Severity Level 1, Severity Level 2, Severity Level 3 and Severity Level 4 incidents.
Method	
Data Capture	Incident records in the Service Management Workflow System are used to determine the total number of Severity Level 1, Severity Level 2, Severity Level 3 and Severity Level 4 incidents during a reporting period, the time each incident is received, and the elapsed time between submission of each Severity Level 1, Severity Level 2, Severity Level 3 and Severity Level 4 incident in the Service Management Workflow System and the acceptance by a technician through the Service Management Workflow System of an assignment to address the incident.
Responsibility	

Reporting Period **Management Period**	Monthly Monthly
Service Metric	
Values	Metrics: Severity Level 1 - Incident Acknowledgement Time – fifteen (15) minutes Severity Level 2 - Incident Acknowledgement Time – thirty (30) minutes Severity Level 3 - Incident Acknowledgement Time – eight (8) business hours Severity Level 4 - Incident Acknowledgement Time – thirty-six (36) business hours
Minimum Service Level	In the aggregate, 95% or more of Severity Level 1, Severity Level 2, and 90% or more of Severity Level 3 and Severity Level 4 incidents are acknowledged within, respectively, the Severity Level 1 Incident Acknowledgement Time, the Severity Level 2 Incident Acknowledgement Time, the Severity Level 3 Incident Acknowledgement Time and the Severity Level 4 Incident Acknowledgement Time.
Other	If NTT DATA fails to acknowledge an incident within the applicable minimum service level acknowledgement timeframe set forth above, but subsequently resolves such incident within the applicable minimum service level timeframe for incident resolution, NTT DATA may exclude the incident from its calculation of the minimum service level.
Calculation	(Number of total Severity Level 1, Severity Level 2, Severity Level 3 and Severity Level 4 incidents acknowledged, respectively, within the Severity Level 1 Incident Acknowledgement Time, the Severity Level 2 Incident Acknowledgement Time, the Severity Level 3 Incident Acknowledgement Time and the Severity Level 4 Incident Acknowledgement Time divided by the total number of Severity Level 1, Severity Level 2, Severity Level 3 and Severity Level 4 incidents) * 100
Performance Credit	Severity Level 1 and Level 2 incidents are considered ‘qualifying incidents’ for Performance SLA evaluation, and are monitored and recorded by NTT DATA on a monthly basis. Customers are eligible to claim a Performance SLA credit in the amount of 2% of the total charges on the applicable Order Form for services rendered by NTT DATA Services in the given month if total number of qualifying incidents recorded in the same month meets or exceeds 20. If 20 qualifying incidents do not occur in a particular month then these incidents are carried forward to subsequent month(s) until the cumulative count reaches 20. Once cumulative count of qualifying incidents reaches 20, Customers are eligible to claim a Performance SLA credit for services described in this Service Description, in the amount of 2% of the total charges under the applicable Order Form for the last month over measured period.

Incident Resolution Time SLA

Objective	Measures the NTT DATA resolution time for the resolution of Severity Level 1, Severity Level 2, Severity Level 3 and Severity Level 4 incidents.
Method	
Data Capture	Incident tracking will be recorded and reported using Service Management Workflow System. Severity Level 1 and Severity Level 2 incidents are to be worked 24 hours a day, 7 days a week until Workaround or Services restoration is achieved.
Responsibility	
Reporting Period	Monthly

Management Period	Monthly
Service Metric	
Values	Metrics: Resolution Time – Severity Level 1 – four (4) hours Resolution Time – Severity Level 2 – eight (8) hours Resolution Time – Severity Level 3 – seventy-two (72) hours Resolution Time – Severity Level 4 – two hundred forty (240) business hours
Exclusions	Resolution Time does not include the time that incident management tickets are in "suspend mode" because of hand-off to Customer or Customer's vendors. Service Requests are excluded from SLA calculations. Incidents determined to be within Customer's responsibility to resolve are excluded from the calculations. Incidents determined to be caused by Customer's implementation decisions that go against industry best practices and NTT DATA's implementation recommendation.
Minimum Service Level	In the aggregate, 95% or more of Severity Level 1, Severity Level 2, and 90% or more of Severity Level 3 and Severity Level 4 incidents are resolved within the applicable Resolution Times.
Calculation	(Number of total incidents at Severity Level 1, Severity Level 2, Severity Level 3 and Severity Level 4 closed within the applicable Resolution Time or properly downgraded by NTT DATA to a lower Severity Level within the applicable Resolution Time, divided by number of the total incidents at Severity Levels 1, 2, 3 and 4) * 100
Performance Credit	Severity Level 1 and Level 2 incidents are considered 'qualifying incidents' for Performance SLA evaluation, and are monitored and recorded by NTT DATA on a monthly basis. Customers are eligible to claim a Performance SLA credit in the amount of 2% of the total charges for the given month if total number of qualifying incidents recorded in the same month meets or exceeds 20. If 20 qualifying incidents do not occur in a particular month then these incidents are carried forward to subsequent month(s) until the cumulative count reaches 20. Once cumulative count of qualifying incidents reaches 20, Customers are eligible to claim a Performance SLA credit in the amount of 2% of the total charges under the applicable Order Form for the last month over measured period.

Claim Procedures and Credit Limitations

- Claim Procedure: To receive a Performance Credit, Customer is responsible for making a claim within 30 days of the last date of the reported downtime alleging NTT DATA's failure to achieve the applicable SLA. The claim must be sent to the NTT DATA Customer Delivery Executive (CDE) or NTT DATA Delivery Manager. The claim must include the following information:
- Customer's name; the name of the service to which the claim relates (i.e. Cloud Operational Excellence for Azure); name, e-mail address and telephone number of the appropriate Customer contact;
  the date(s) and times for each claim of a Performance SLA that was not achieved.
- Any "credit" that NTT DATA may owe, such as a Performance Credit for a failure to meet an SLA, will be applied to rates due and payable for public cloud managed services provided by NTT DATA,

and will not be paid as a refund. If a single incident results in multiple acknowledgement time or resolution time defaults (as determined through the NTT DATA root cause analysis), Customer are only eligible to claim the highest Performance Level Credit applicable to such incident. All claims for a Performance Credit are subject to review and verification by NTT DATA in its sole discretion, and all remedies will be based on NTT DATA's measurement of its performance of the applicable Service and NTT DATA's decisions will be final. Customer's sole remedy, and NTT DATA's sole liability, with respect to NTT DATA's inability to meet an SLA are the Performance Credits described above and Customer explicitly disclaims any and all other remedies, whether in law or equity.