Client Service Description

Managed Hybrid Infrastructure Services (MHIS)

15 May 2020 | Document Version 20.5.15

Confidentiality

Document History

Version Number	Date	Description
V1.0	15 October 2019	First version of consolidated CSD
V1.01	20 February 2020	Revised Public Cloud Management services
V20.5.15	15 May 2020	Revised to reflect entire MHIS Portfolio

Table of Contents

List of Figures

List of Tables

1. Managed Hybrid Infrastructure Services (MHIS)

Systems running on hybrid infrastructure (public cloud, private cloud, data centre and co-location) must be monitored, measured, and reported on by key staff who need to focus on delivering service to the business in addition to supporting technology.

NTT has developed its approach to managing Hybrid IT with these factors in mind. Our managed services are focused on driving operational standards to manage the daily operations of client infrastructures through:

- Building on a core of industry best-practice processes (ITIL, ISO20000)
- Driving automation to enable higher levels of availability and enable enhanced and consistent user experience
- Ensuring continual service improvement, and empowering clients with the information to make business decisions about their IT environment through data collection, analysis and dissemination
- Providing an integrated service delivery model with centralised service delivery combined with regional and country resources to provide support when and where needed
- Combining our cross-competencies in Cloud, DevOps, network, workplace and collaboration, datacentre and security to provide an integrated and standardised end to end managed service experience across the entire IT estate

1.1. MHIS Portfolio Overview

NTT has developed MHIS (referred to in this document as the “Service”) in a modular fashion with four service offers; Managed Public Cloud, Managed Private Cloud, Managed Datacentre Infrastructure, and Managed Application Infrastructure. Each of these service offers contain multiple service offer options. Clients work with NTT to contract for one or more service offer options so that a managed services solution can be deployed that meets technical and budgetary requirements.

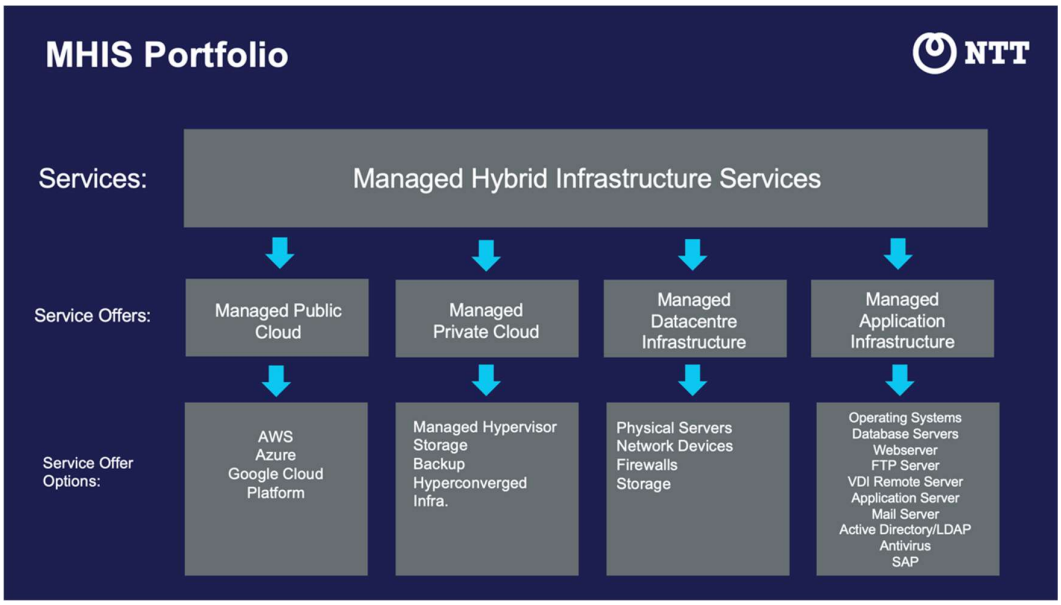

Figure 1 – Managed Hybrid Infrastructure Services (MHIS) Portfolio

1.2. MHIS Documentation

The complete service is defined by the combination of the following documents:

- **Client Service Description** – this document, that describes MHIS features and service delivery
- **Services Guide** – service details that are specific to each service offer option within the MHIS service offers

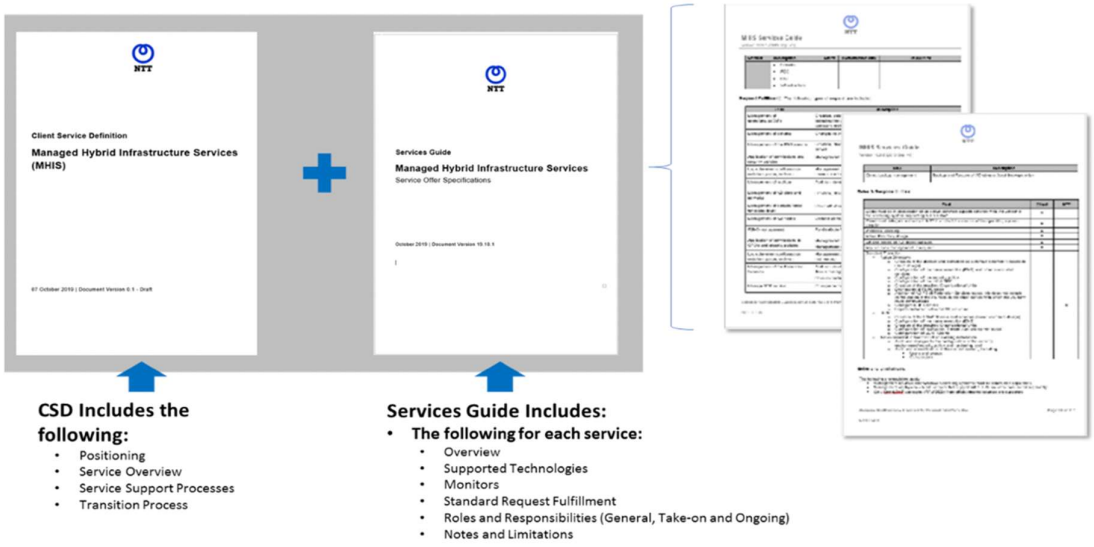

Figure 2 – Managed Hybrid Infrastructure Services (MHIS) Portfolio Documentation

2. Managed Hybrid Infrastructure Service Design

2.1. End to End Services

NTT has developed an end-to-end enablement program to support clients through a complete transition to our Managed Hybrid Infrastructure Services. Our *Consult and Deliver* services provide the design and planning needed to systematically move the workloads into a managed environment. *Operate* services provide support and ongoing maintenance of the client's systems while transformative *Optimize* services promote continuous improvement and cost efficiency.

Figure 3 – End to End Services by MHIS

MHIS supports systems running on the following platforms:

- Public Cloud
- Private Cloud
- Multi-cloud
- Traditional Infrastructure on premises or in a co-located datacentre

2.1.1 Consult

All engagements begin with *Consulting* to understand the client's existing technology landscape, business objectives and management requirements. Depending on the client's needs, Consult Services will include one or all of the following activities.

Activity	Description	Reference
Hybrid Migration Assessment	Information gathering and analysis in order to provide a migration plan to hybrid or private clouds • Discovery Scanning • Workshops	Further detailed in *MHIS Hybrid Migration Assessment* Offer Description. Professional Services charges apply.

Public Cloud Consulting	Advisory and Planning Services for migrating workloads to the public cloud • Sprint based • Supports '6 Rs' migration strategies	Further detailed in *MHIS Cloud Consulting* Offer Description. Professional Services charges apply.
Audit and Planning for Takeover of an existing solution	Due diligence and planning required for NTT to take over the management of an existing solution	See Section *4.0 Service Transition Management Processes* of this document

Table 1 - Cloud Consulting

2.1.1.1 Blueprints

MHIS recognizes that standardization is key for scalability and efficiency. In order to streamline the consulting process, we have developed a set of pre-defined, approved architecture blueprints to support the most typical environments. These blueprints apply our standards for availability and security and provide the foundation for the technical and service designs developed during the *Consult and Deliver* phases.

2.1.2 Deliver (Migration and Takeover)

With due diligence and planning complete, NTT moves into the *Deliver* phase. If workloads are to be migrated, migration plans, including a detailed low-level technical design, migration timeline and cost proposal are presented to the client. Upon client approval, the migration is executed, and workloads are moved to the target platforms. For further details on NTT's migration practice, please refer to the *Hybrid Cloud Migration* Offer Description.

In the event that a migration is not in scope, and NTT is simply taking over an existing solution, an audit will be performed to identify any problems with the platform, or any issues that present a risk to the delivery of services. The client is then responsible for resolving these issues in order to prepare the environment for takeover by NTT. If needed, the client can request NTT's assistance in the resolution of identified problems for an additional cost. For more details, see section *4.0 Transition Service Management* of this document.

2.1.3 Operate

MHIS *Operate* activities provide ongoing support and management of the client's solution, covering public and private cloud, datacentre infrastructure and application infrastructure. The following activities are included by default:

Activity	Description

Monitoring and Event Management	• Automated agent deployment • Standard, technology specific monitoring configurations • 24 x 7 Global Service Desk • Call handling and basic triage
Incident Management and Problem Management	• Technology specific standard operating procedures (SOPs) • Defined client runbooks • Proactive problem management using automated aggregation of repetitive alerts
Service Requests	• Standard Requests fulfilled via predefined runbooks
Change and Release Management	• Structured and traceable change management and release management procedures • Change Advisory Board process
Availability and Capacity Management	• Platform and individual component availability, performance and capacity • Deviations detected via monitoring and periodic reviews analysed and resolved
Continuity Management	• Backup management • Optional Disaster Recovery management
Patch Management	• Patching via automated tooling • Regular patching schedule for essential OS patches • Fastrack procedures for emergency patching

Table 2 - MHIS Operate Activities

2.1.4 Optimise

In addition to daily maintenance, the following continuous improvement and optimisation activities are included as part of the service:

Activity	Description
Continual Service Improvement	• Regular review of recurrent issues to identify underlying problems • Resolution activities managed and reported back to client
Risk Management	• Identified risks identified and mapped to related support processes • Mitigation tracked and reported with periodic reviews
Cost Optimisation	• Public cloud cost optimisation reporting • Provide options to improve economic efficiency • Periodic capacity reviews to optimise cost of the platform
Architecture Optimisation	• Cloud Architect consults on adoption of new public cloud technologies and planning the evolution of IT • Performance improvement recommendations for compute, storage and network layers

Table 3 - MHIS Optimize Activities

2.2. Technology Standards

NTT has developed standard offers for our entire service portfolio which provide specific monitoring configurations, client requests and setup tasks for all supported technologies. These technology specific standard offers are described in the *MHIS Services Guide*.

2.3. Billing

The client contracts for one or more service offers for each IT asset that is to be managed by MHIS. Each IT component under management is referred to as a Configuration Item ("CI"). A configuration item (CI) is any service component or

infrastructure element that needs to be managed, such as a router, an operating system or a database.

The client is billed on a monthly basis for each CI under management. Flexible billing is available to accommodate dynamic environments that scale up and down from month to month.

For public cloud scalable assets, the client is billed only for the base image and its software components (regardless from the number of servers deployed from it).

For public cloud PaaS, Serverless and Container solutions are billed based on the platforms used, use case, and complexity. In these scenarios, per CI charges do not apply.

2.4. Limitations

- MHIS does not provide installation of physical devices (compute, storage or network).
- Client must have a hardware maintenance contract (with NTT or another vendor) that matches the SLO of the service (e.g. 24/7/365 with 4-hour on-site support).
- Client must provide/procure "smart hands" support (i.e. physical restart of a device). Per individual contract, this may be outsourced to NTT or another vendor.

2.5. Service Levels

Managed Hybrid Infrastructure Services include a standard set of service level commitments included within the service.

2.5.1 Incident Response Service Level

NTT will respond to Incidents reported by the client as per Table 4 below. NTT shall meet this service level in respect of no less than 95% (ninety-five percent) of all Incidents closed in a given calendar month.

Priority	Response Time
1 - Critical	15 minutes
2 - High	30 minutes

Table 4 – Incident Response Time Service Level

2.5.2 Request Fulfilment Response Time Service Level

NTT will respond to requests for information and standard changes for as per Table 5 below. NTT shall meet this service level in respect of no less than 95% (ninety five percent) of all defined requests in a given calendar month.

Feature	Action	Response Time
Request for Information	Response	24 hours
Standard Changes	Response	24 hours

Table 5 - Request Fulfilment Response Time Service Level

2.5.3 Request Fulfilment Service Level

NTT will fulfil requests for information and standard changes as per Table 6 below. NTT shall meet this service level in respect of no less than 95% (ninety five percent) of all defined and accepted requests in a given calendar month. The following times start when NTT has received all the information required to carry out the work.

2.5.3.1 Limitations for Service Requests

NTT reserves the right to suspend or re-schedule any request that implies an interruption of the service, and therefore needs to be resolved within a maintenance window.

NTT reserves the right to suspend any service request that implies a change to the scope of either the contracted managed services. Such changes include, but are not limited to:

- Installing new software;
- Changes to the monitors required;
- Addition/removal of a server or other platform element; and
- Changes to the network architecture.
    - Such changes will be treated as a new project and may be subject to additional fees.

Feature	Action	Response Time
Less than 30 minutes of work required	Fulfilment	24 Hours
Between 30 minutes and 2 hours of work required	Fulfilment	Next Business Day
More than 2 hours	Fulfilment	Not before the next Business Day

Table 6 - Request Fulfilment Time Service Level

2.5.4 Incident Notification Service Level

NTT will monitor for Events which may impact availability and capacity attributes (specified as “monitoring attributes”) for the below-specified Managed Hybrid Infrastructure Services as per Table 7 below. Should there be an Event which causes such impact, the Event will be categorised by NTT as an Incident and the client will be notified within 15 (fifteen) minutes of the Incident being logged by NTT. NTT shall meet the Incident notification service level in respect of no less than 95% (ninety-five percent) of all Incidents closed in a given calendar month.

The following service level commitments are provided for the Managed Hybrid Infrastructure Services only with the additional management option:

Feature	Service Level
Availability failure or capacity thresholds not met	15 minutes

Table 7 - Service Availability Service Level

2.6. Service Level Credits

a. NTT shall measure the service levels in respect to Section 2.5

b. In the event of non-achievement of service levels, and subject to notification by client in accordance with clause (2.6)(h) below, NTT shall be liable for service credits as per clause (2.6)(d) below.

c. All service level measurements will be carried out exclusively by NTT through NTT systems and/or tools.

d. Service credits will be calculated monthly in arrears, and will apply as follows:

Service Level	Service Credit
Incident Notification	5% of Monthly Fee
Incident Response Time	5% of Monthly Fee
Request Fulfilment Response Time	5% of Monthly Fee
Request Fulfilment Time	5% of Monthly Fee

Table 8 - Service Level Credits

e. In no event shall NTT’s liability to the client in respect of the aggregate sum of service credits for a service in any given month exceed 20% (twenty percent) of that specific service’s monthly charges (or 100% of the service unit value for the service request in breach) for the month in which the service level defaults have occurred.

f. No service credits shall be incurred for non-achievement of the service level targets arising as a result of any of the events clauses specified in clause 2.7 below.

g. NTT shall not be liable for any service credits to client under the Statement of Work in the event that, at the time the service credits would have been incurred, any fees owing from client to NTT for the service have been outstanding for 90 (ninety) days or more.

h. Service credits will not be granted by NTT automatically in the event of a service level default. Should client elect to invoke the service credits client shall notify NTT in writing within 30 (thirty) days after the service management report for the applicable measurement period has been made available to client. Such written notification must stipulate full details of NTT's non-achievement of service levels, including but not limited to, the service levels which NTT has failed.

i. Where more than one service level default occurs as a result of the same event and service credits are payable to client in respect thereof, NTT shall only be liable for a service credit in respect of a single service level default, as determined by client in its notification of such default.

2.7. Service Level Exclusions

NTT shall in no way be liable for service level defaults resulting from one or more of the following events, and no service credits shall be payable to client as a result hereof:

a. Defaults caused by any of the events specified in clause 20 of the General Terms and Conditions;

b. Defaults caused by absence of a patch, repair, policy, configuration or maintenance change recommended by NTT but not approved by client;

c. Defaults caused by scheduled downtime in respect of NTT equipment (including upgrades, repair or component replacement or scheduled backups) or any other mutually agreed-to downtime;

d. Defaults caused by changes made by client to covered configuration item or protected server configurations where client has not notified NTT;

e. Defaults caused by unavailability of access to site;

f. Defaults caused by damage or delay arising from client's failing to carry out an action or contractual obligation required by NTT in order for it to render the Services in a timely manner and/or in accordance with the agreed SLA;

g. Defaults caused by time for hardware maintenance vendor to respond, as specified in client maintenance agreement

h. Defaults caused by damage to equipment used to render the services and which are within the client's environment by abnormal operating conditions such as high or low temperatures or humidity or dust levels or fluctuations of electrical power, which are beyond the published environmental specifications of the product manufacturer;

i. Defaults caused by modifications, repairs or replacements or attempted modifications, repairs or replacements not performed by NTT or not approved by NTT in writing prior to such modifications, repairs or replacements being performed or attempted by any other party, including the client;

j. Defaults caused by the restoration of any lost data from any products, or devices connected to products, without NTT's knowledge;

k. Defaults caused by products where the client has failed to licence such products and such licence is a prerequisite of the manufacturer or where such licence is no longer current or valid or when such products have been purchased outside of acceptable purchasing norms (commonly referred to as 'grey-market' products);

l. Defaults caused by failure of non-NTT applicable software tool;

m. Defaults caused by damage during any transportation or relocation of Products not carried out by NTT;

n. Defaults caused by electrical work, not performed by NTT;

o. Defaults caused by failure of unsynchronised data; and

p. Defaults caused by of a virus, worm, distributed denial of service, or any other malicious activity.

3. Service Delivery Processes

3.1. Service Coverage

NTT recognizes that not all IT assets require the same level of management and service availability. While production environments typically require 24x7 availability, other systems (e.g. Disaster Recovery (DR) target sites) have lesser service requirements until they are activated for business continuity.

To accommodate these different requirements, NTT provides the following options;

- **Full Coverage (24x7):** Full coverage is typically used for production environments, providing 24x7 incident resolution and the highest level of service guarantees.
- **DR Coverage:** Disaster Recovery (DR) coverage is intended for the management of redundant IT architectures, which are maintained in *standby* mode and are used only when a system's primary architecture fails. DR coverage provides Full Coverage services only when the redundant architecture is *active.* Note: that the client must be contracted for a separate DR solution.

3.2. Service Management Frameworks

ITIL v3 and ISO 20000 are the global de facto frameworks for IT Service Management best practices and MHIS service delivery process are structured to be directionally aligned. As such, MHIS service delivery includes:

- Service asset and configuration management
- Event management
- Incident management
- Problem management
- Request fulfilment
- Change management
- Continual Service Improvement
- Service Level Management
- Access management
- Availability and capacity management

As part of service transition, NTT works with the client to identify how best to interlock operational processes.

3.2.1 Service Asset and Configuration Management

NTT is committed to ensuring that the information in its Configuration Management Database (CMDB) is consistent with the scope of services contracted by the client and continuously updated for accuracy. Configuration Management is the process that provides governance and a systematic approach for ensuring this consistency.

Configuration Management is a critical component of MHIS, underpinning and interlocking all relevant processes, people and tools.

- The accurate capture of relevant information is a primary responsibility of the Service Transition process.
- This information will be loaded into the CMDB and used for service delivery processes
- The Change Management process is responsible for updating the information related to changes to live Configuration Items.

NTT relies on automated processes for loading the information into the CMDB to minimize human error and help ensure consistency between the contracted scope of services and the number of devices under management. These processes are performed using auto-discovery and other CMDB enrichment tools.

3.2.2 Event Management

NTT will provide monitoring services for all systems under management, using technology specific Standard Monitoring configurations. In the event the client requests a modification of standard configurations, specific monitoring requirements shall be defined and agreed upon by NTT and the client.

Monitoring will be performed at a set frequency. If an anomaly is detected, the system will recheck twice automatically and, if the anomaly is persistent, generate an alert.

The response to monitoring alerts will be as follows, depending on the criticality and expected associated action:

Alert response	Output
No alert, data only	The monitor does not generate an alert nor an Incident ticket. The data is collected only for informational purposes.
Email only	The monitor does not generate an alert nor an Incident ticket. An email with the alert information is sent to the client's specified contacts
Priority 1, Priority 2, Priority 3	This will generate an alert ticket that will be managed by the operations team.

Alert response	Output
Service Monitor	This will generate a major incident and create an associated Incident ticket. Service monitors are configured for measuring the solution availability of the client solution.

Table 9 – Response to Monitoring Alerts

Once an alert ticket is generated, engineers in the Ops Center will manually re-test the alert (except for Service Monitors).

- If the monitor that triggered the alert has returned to normal values, the alert is cleared, and no Incident ticket is created.
- If the manual re-test fails, an Incident ticket is generated with the associated severity and Incident Management activities will be initiated.

MHIS employs toolsets to continuously detect and aggregate the most repetitive alerts and to identify the top polling events. The data generated is then analyzed within the Problem Management process.

3.2.3 Incident Management

3.2.3.1 Prioritization of Incidents

Tickets regarding Incidents will have a priority assigned to them which is determined by the impact and the urgency of the Incident.

The table below illustrates how priorities are assigned to Incident tickets:

Priority		Impact		
		High	Medium	Low
Urgency	High	Priority 1	Priority 2	Priority 3
	Medium	Priority 2	Priority 3	Priority 4
	Low	Priority 3	Priority 4	Priority 4

Table 10 – Priorities of Incidents

Additional description of the priorities is provided in the following table.

Priority Level	Description
P1	Solution availability immediately impacted Multiple component failures affecting critical services within a client solution or multiple solutions
P2	Solution performance degraded or availability likely to be impacted Multiple component failures within a client solution not affecting solution availability
P3	Incident has the possibility to degrade either performance or availability if not resolved
P4	Single component failure with a non-critical threshold. The incident has the possibility of degrading performance if not resolved.

Table 11 – Description of Priority Levels

The urgency and the impact of a ticket will be agreed upon by the client and NTT and may be applied automatically by the alerting mechanism, based on the associated monitoring.

3.2.3.2 Ticket Backlog

Incidents without a response from the client are eventually closed. Our support team will update the ticket requesting the client's answer every 7 days. After the third failed attempt the ticket will be set to a resolved state. If the client does not reactivate the ticket within 7 days, the ticket will be automatically closed.

Incidents with impact where the client does not cooperate in its closure will be registered as risks and closed. Should the monitoring continue to generate Events due to the unresolved Incident, the related monitoring will be suspended until the risk is mitigated.

3.2.3.3 Major Incident Management

Where NTT has determined that both the impact and urgency of an Incident is High (P1), a special Major Incident Management process is followed. During this process, multiple engineering teams may be involved in the problem resolution and the client is continually notified of the resolution progress.

3.2.3.4 Disaster Recovery

In the event that NTT has been contracted to provide Managed Disaster Recovery services, the client is responsible for invoking DR site failover. NTT will provide any available information to assist the client with the decision-making process.

3.2.4 Problem Management

Problem Management is the process of identifying the underlying causes of an Incident and establishing a formal process for resolution. The primary objectives of Problem Management are to prevent problems and resulting Incidents from happening, to eliminate recurring Incidents, and to minimize the impact of Incidents that cannot be prevented.

Problem Management will be initiated in one of two ways:

- Reactive Problem Management - initiated in response to an Incident where the root cause is unknown
- Proactive Problem Management - initiated as a result of the analysis of repetitive alerts and recurring Incidents

3.2.4.1 Reactive Problem Management

The Reactive Problem Management Process will apply to the following within the Major Incident Management process:

- All P1 Incidents
- P2 Incidents as requested by the client
- Recurring Incidents

During this process, a ticket NTT's engineering teams will determine the root cause for the problem. Once this is done, the configuration management process will be invoked to update runbooks, document the problem and solution, etc.

3.2.4.2 Proactive Problem Management

NTT continuously aggregates and identifies the top repetitive alerts and the issues causing recurring Incidents. NTT Problem Managers are responsible for resolving these problems through Proactive Problem Management. A Problem Owner is defined based on the nature of the problem:

- Technology related issue: in this case, the Technology Team will own the problem until its resolution.
- Client solution related issue: the Lead Engineer within the Solutions Engineering Team will help ensure that the root cause is identified and that appropriate changes are applied. If the client refuses to collaborate on resolving an issue, NTT reserves the right to suspend monitoring and the SLA of the affected Components.

3.2.5 Request Fulfilment

A service request is a ticket that contains a request for information, advice or a change which is within the scope of MHIS. This is distinct from the response to alerts or urgent change requests in response to incidents.

3.2.5.1 In-Scope Service Request

Service requests that are considered part of the MHIS service offered are considered “in-scope” and therefore, do not incur a client charge. These requests will be processed after NTT has received all pertinent information. Within the category of “in-scope” services, requests, there is a sub-category of standard service requests.

- A standard service request is an agreed upon and repeatable in-scope service request which has an associated runbook and predefined template which the client completes with each submission. The list of Standard Service Requests will be agreed to by the client and NTT.

3.2.5.2 Out-of-Scope Service Requests

If NTT determines that the client has requested activities which are not in-scope of MHIS, the following process will apply:

- NTT will notify the client that the request is not in-scope and therefore, it may be chargeable
- If the requested activities are chargeable, NTT will notify the client. NTT and client will agree upon the price.
- Once written approval is received, NTT engineers will proceed with the request.

3.2.5.3 Fair Use Policy

NTT does not charge clients for individual MHIS in-scope service requests, nor does NTT apply any accounting system for ‘purchasing’ service requests. Rather, NTT employs a “Fair Use” policy that reserves the right to limit the number of in-scope service requests after an extended timeframe where the client has violated this policy. Unless this policy is invoked, there is no limit to the number of MHIS in-scope service requests generated by the client. See the MHIS Statement of Work (SOW) for details.

3.2.6 Change Management

The main objectives of the Change Management process are:

- To document all changes executed to help ensure traceability
- To help ensure proper preparation of a change based on its complexity and assessed impact or risk

The following principles are used to define Change Management:

- A Change Advisory Board (CAB) in the Change Management process helps to manage risk, as well as inform technical and business stakeholders of potential impacts;
- The client will retain ownership of the Change Advisory Board (CAB) for IT infrastructure; and
- NTT's support engineers will follow the established Change Management process for every change.

The Release Management process is embedded in the Change Management process and is responsible for ensuring that the change execution is performed in a standard and consistent way.

3.2.6.1 Approval Process

All changes will be categorized based on the impact and risk of the change, and in some cases will require the approval of the Change Advisory Board. The table below describes each category, and whether CAB approval is required.

Categorization of Changes			NTT			Client & NTT	
Type	Use Case (Source)	**Details**	Tech. Auth.	Queue Mgr.	Major CAB	Client CAB	Emergency CAB
Standard	Standard Request	Pre-approved change for immediate action.	✗	✗	✗	✗	✗
Standard Scheduled	Standard Request requiring scheduling	Pre-approved change for immediate action.	✓	✓	✗	✗	✗
Normal Minor	Service Request, Problem Management, Project Management	A low/medium impact/risk change.	✓	✗	✗	✓	✗
Normal Minor Scheduled	Service Request, Problem Management, Project Management	A low/medium impact/risk change.	✓	✓	✗	✓	✗
Normal Major	Service Request, Problem Management, Project Management	A high impact/risk change. It always requires scheduling.	✓	✓	✓	✓	✗
Emergency	Incident	Low impact/risk change for immediate action.	✗	✗	✗	✗	✗
Emergency Minor	Incident	Medium impact/risk change for immediate action.	✓	✗	✗	✗	✗
Emergency Major	Incident	A high impact/risk change. Requires client approval.	✓	✗	✓	✗	✓

Table 12 – CAB Approval Matrix

Technical Authority - the NTT Technical Authority will vary depending on the significance or risk associated with the Change but may *not* be the same engineer that is managing the Change Request

Queue Manager - NTT Engineering Team Leader. This approval helps ensure that there will be resources available for executing the Change

Client CAB - Technical and business stakeholders as defined by the client

Major CAB - One or more NTT Operations Directors

Emergency CAB - A representative identified by the client that is authorized to approve Emergency Changes and who can be contacted 24x7 along with the Service Delivery Manager.

3.2.7 Continual Service Improvement

3.2.7.1 Risk Management and Mitigation

As part of ongoing support, NTT will document all risks identified within the client Solution. Identified risks will be tracked in a risk register that contains the following information:

- Risk
- Impact
- Related Ticket
- Mitigation plan
- Notification Date
- Informed Stakeholders

Furthermore, each of the risks identified will be mapped to the related Support Process (e.g. Capacity Management, Availability Management, Continuity Management, etc).

Once documented, the risks will be communicated to the client and actions taken according to the mitigation plan.

3.2.7.2 Service Improvement Plan

NTT will work with the client to address service issues, client complaints and service improvement tasks. All items will be documented in the service improvement plan (and related service improvement register), which is maintained by NTT.

3.2.8 Service Level Management

NTT will report on service performance to the client on a regular cadence. A predefined report will be produced containing:

- Ticket summary report (Event, Incident, Request and Changes)
- SLA reporting: based on Service Level Monitors
- Capacity*
- Backup report*
- Available patches*
- EOL

- Risks
- Service Improvement Plan

* Reporting on capacity, backup and available patches is available for only certain technologies. Refer to the related Service Description for further details.

3.2.9 Platform Access

To deliver the Service, the NTT Operations Team must have remote access to the client solution. This access requires a high level of availability, reasonable latency and sufficient bandwidth.

NTT's access management approach encompasses the following areas:

3.2.9.1 Identity Management - Advanced Management Zone (AMZ)

Primary management activities will be performed from NTT' Advanced Management Zone (AMZ). The AMZ is a remote access solution that uses multi-factor authentication (MFA) and session recording to provide NTT with the necessary access to manage solutions while tracking the identity and activity of each user. The AMZ provides an advanced level of governance which is critical for organizations subject to regular compliance audits (such as PCI).

The primary features of the AMZ are:

- Multi-Factor Authentication (MFA)
- Session Recording
- Full tracking and auditing
- Role Based Access Control (RBAC)
- PCI audited
- Anti-virus and Anti-malware
- File Integrity Monitoring
- High Availability - hosted across multiple regions

3.2.9.2 Connectivity to the Client Environment

NTT requires that the connection from the NTT operations facility to the client environment is performed over one or more of the following transports:

- An IPSec VPN tunnel established between the client platform and NTT's AMZ. This is the default option that provides encryption of all the communications from firewall to firewall

- IPsec VPN must be routed with no network address translation (NAT) between NTT and the client; IP ranges in the client platform must be assigned by NTT
- If IPs can't be assigned by NTT (for example if taking over an existing platform), NTT will require that destination NAT is configured at the client-end. If this requirement cannot be met, NTT may determine that the solution cannot be supported;

- An MPLS link between the client platform and NTT's AMZ. This method is highly secure as it provides a Private Network. As communications do not flow through public networks, encryption is not mandatory unless otherwise stated by the client. Additional setup and recurring charges will apply

Optionally, for an increased level of resiliency, NTT can use an out-of-band method (such as a remote console server accessible via another Internet uplink) to access the devices.

Client MFA (multifactor authentication) systems are not supported by MHIS. MHIS already has their own MFA methods.

Any access methods outside of those listed above will be subject to NTT approval and may be subject to additional charges.

3.2.9.3 Privileged User Access (Admin Rights)

NTT will deploy and configure servers and devices with the users and associated level of Admin Rights required to provide the Service. NTT will be the only party having Admin Rights on all items under management. If special business requirements justify a shared management model whereby the client or a 3rd party requires admin rights, this may be granted for an interim period and the following caveats shall apply:

- NTT's SLA will not apply during the interim period as NTT cannot ensure the supportability of the client solution
- Monitoring alerts may be deactivated to avoid false alarms being generated by the client or 3rd party activity on the devices or service components
- In cases where the client or 3rd party engages NTT to perform troubleshooting of any issues caused as a direct result of the use of Admin rights by the client or 3rd party, such activity may be subject to additional charges
- Once the interim period is over and NTT has been requested to resume management services, NTT reserves the right to conduct an audit of the affected Components to help ensure the client solution is still supportable. The time incurred for the audit and for corrective actions or changes required to re-align the systems and services as deemed necessary by NTT, may be subject to additional charges

3.2.10 Management Tools

The configuration and placement of NTT's management tools are dependent upon solution requirements. The following guidelines generally apply:

- For platforms consisting of twenty (20) or more managed devices, NTT will require dedicated management tools, which can be hosted within the client's infrastructure or within a dedicated management zone;
- For platforms consisting of fewer than twenty (20) managed devices NTT may use shared management tools but subject to the following restrictions;
    - For full stack platforms (systems and networking) shared management tools require no destination NAT between NTT and the client platform; the use of NAT will require certain tools such as monitor collectors to reside within the client's infrastructure, on a dedicated server.
    - Networking-only platforms carry no NAT restrictions;
    - Bidirectional connectivity is required for some management tools and must be considered when NAT is used;
- For platforms with PCI compliance requirements, dedicated tools are required regardless of platform size;
- Ticketing and monitoring are delivered with NTT's own toolsets;
- Certain managed services may require the installation of additional agents and tools; and
- Knowledge Management content will be stored in NTT's current tool.

3.2.11 Capacity and Availability Management

Capacity and availability management reports are compiled and delivered by a local service delivery manager on a monthly basis. The data is compiled on a continuous basis by the standard MHIS monitoring solution and periodic reviews.

Capacity Management

MHIS provides reports for capacity management across the following parameters:

- Disks (e.g. free space, LUNs). These parameters are reported on in the Managed Physical Storage, Managed OS, Managed HCI, Managed Hypervisors and Core mode service offer options.
- CPU and Memory (e.g. loading). These parameters are reported on in the Managed Physical Storage, Managed OS, Managed HCI, Managed Hypervisors and all Managed Data Centre Network service offer options.
- Networks (e.g. ports, bandwidth) These parameters are reported on in the Managed OS and all Managed Data Centre Network service offer options.
- Hypervisor resources (e.g. VMs, datastores). These parameters are reported on in the Managed HCI service offer option.

Availability Management

Availability reports are generated for 'business services' (or workload, see Section 4.4.4 for details) and compared against SLAs. Any deviations are highlighted for review. The availability of individual components of a business service/workload are not reported.

3.2.12 Continuity Management

In order to ensure service continuity of the client solution, NTT will propose a backup solution. MHIS Backup Management services are defined in the *Managed Backup Service Description* of the *MHIS Services Guide.*

For solutions which require additional protection against disasters, NTT can provide managed DR services. Our approach to DR Management services is defined in the *Disaster Recovery (DR) Services Description* in the *MHIS Services Guide.*

3.2.13 Patch Management

As part of the service, NTT will provide Patch Management services:

- Applying upgrades for Minor versions of the supported software/firmware is included. Major upgrades are not included by default, and their implementation may be chargeable; and
- Infrastructure required for implementing patching services will need to be deployed and may be chargeable to the client (e.g., WSUS server deployment and management)

3.2.13.1 Patch Categories

As part of the Patch Management service, NTT defines three patch categories:

- **Essential OS Patches:** OS patches regularly published by WSUS for MS Windows and RHEL Satellite for RHEL which can be deployed via automated tools throughout the client solution (due to known risks of OS patches affecting Oracle DB servers, any OS with Oracle Database Server installed is excluded.)
- **Emergency Patches**: Critical patches released by vendors to correct security vulnerabilities that present either a high risk to stability, potential exploitation or that are actively being exploited; and
- **Minor Version and Firmware Patching:** patches published by vendors on an *ad hoc* basis which are not deemed high risk and which fall into one of the following groups:
    - OS and Applications - RHEL minor version changes not included in the RHEL defined repository list, Microsoft OS Service Packs/roll-ups, or NTT Managed Applications; or
    - Infrastructure - Software/firmware updates for network, switching, and security devices, storage systems, physical servers and hypervisors.

3.2.13.2 Frequency of Reporting and Patching Process

The scope and maximum frequency of each patching category are as follows:

1. Essential Patching

Microsoft OS High/Critical Patches:
NTT will report on these patches with a maximum frequency of once per calendar month. The maximum frequency for the installation of patches is also once per calendar month (except in cases where a one-month timeframe is not sufficient due to the number of patches or size of the environment).

Linux OS All Patches:

NTT will report on these patches with a maximum frequency of once per calendar month. The maximum frequency for installation of patches is also once per calendar month (except in cases where a one-month timeframe is not sufficient due to the number of patches or size of the environment).

NTT will aggregate the relevant available patches for the client solution and will deliver a list to the client on a monthly basis. Where NTT is aware that the installation of patches may impact the stability of the client solution, NTT will notify the client of said risk so that they can determine which patches are required and provide NTT with a list of the patches to be applied.

2. Emergency Patching

NTT regularly checks for critical vulnerabilities that affect its supported technologies.

In the event that a vendor publishes a patch that addresses a vulnerability, NTT will analyse and determine the criticality of the vulnerability against the client's solution. If a vulnerability is declared a threat or to have a high risk of outage, it is considered an Emergency, and NTT will inform the client within 2 working days of receiving the notification. NTT and client will agree to the required action and schedule a specific maintenance window.

NTT will follow the standard Change Management processes to install the patch, leveraging any available non-production environments for testing.

3. Minor Version and Firmware Patching

Operating Systems: NTT will not perform regular patch reviews or installation of minor OS version patches. Client may submit a ticket to request that NTT review any managed OS for available Application Service Packs, roll-ups or minor version changes. NTT will assess the available minor version patches against the latest NTT supported versions and, if accepted, NTT will schedule the upgrade following the standard *Change Management* process. This activity may be subject to additional charges depending on the resources and client requested maintenance windows and or additional processes to achieve the upgrade.

Applications: These patches will be reviewed as and when NTT considers it necessary. Additionally, the client can request that these patches are reviewed

once per year, per technology (for example, SQL Server, Exchange Server, Oracle Server).

Infrastructure Devices:

Storage Devices, Storage Networking Devices, SAN Switching: NTT will proactively review available versions for storage devices, including any software and firmware, once per calendar year. NTT will notify the client of supported versions of vendor-defined critical updates and recommend patching as necessary.

Hypervisors: NTT will proactively review available versions for hypervisor physical servers, including any software, with a minimum frequency of 3 months. NTT will notify the client of supported versions of vendor-defined critical updates and recommend patching as necessary.

Networking and Security Devices: NTT will not proactively review any network or security devices. The client may request once per 6 calendar months, via a ticket, that NTT review the client's networking and security devices. NTT will recommend patching to the latest NTT supported version as deemed necessary due to vendor-defined critical updates being required. If an upgrade is successful and accepted by the client during the agreed upon maintenance-window then any subsequent rollback requested at a later date by the client may be subject to additional commercial charges at the discretion of NTT.

These patches are reviewed at varying frequencies or reactively when requested by the client or NTT and can be deployed as part of the Standard Patching scope according to the guidelines and frequencies set out in this document.

3.3. Service Management

The service management function is delivered through a local service delivery manager on a monthly basis.

3.3.1.1 Key Functions

The key functions of the service management function are

- To provide an NTT interface who can manage the service delivery relationship between your NTT and the client.
- To conduct operational reviews and business performance reviews following a defined management cadence
- To provide a key point of escalation for the client (e.g. through major incidents escalations)

3.3.1.2 Management Cadence

These sessions occur on a schedule mutually agreed to by the client and NTT and are designed to allow for a regular review of service reports, service operations and planning for any actions required to maintain service quality. These sessions include:

- Review of monthly service level achievements and other key performance indicators
- Review of any major incidents from the previous month and any associated service improvement activities required to prevent re-occurrence
- Review of identified problems, root cause analyses, known errors and permanent fixes planned
- Review of changes implemented within the previous month and highlighting any issues or concerns with the planning or implementation of changes
- Review of potential areas of escalation or concern and action plans to remediate
- Identification of any tactical improvements to service delivery

The operational statistics and reporting provided during the review sessions, including meeting minutes and any action plans are made available online.

3.3.1.3 Key Benefits

- Helps ensure strong communication channels between the client and NTT in a true partnership model
- Enables regular interaction between the client and NTT to review the health and performance of the IT environment, to identify any adverse trends and to take remediation actions
- Provides a forum for discussing the performance of the service, identify issues, take corrective actions to avoid service dissatisfaction

4. Service Transition Management Processes

Service Transition refers to the process of moving a solution into the management responsibility of NTT MHIS and applies broadly to the following scenarios:

- Migration of an existing solution to a new platform
- Deployment of a new system on a new platform
- Takeover of an existing solution

The sections that follow describe the process of transitioning a new or existing solution to NTT MHIS.

In cases where a solution is to be migrated, NTT MHIS recommends that management responsibilities are transitioned to MHIS, prior to the migration as long as conditions allow. For further details on the migration process are described in the *MHIS Migration Service Offer*.

4.1. Service Transition Phases

4.1.1 Pre-Transition Phase

The following high-level activities will be performed during this phase and are typically those activities we perform before the Transition Commencement Date and Contract Signature.

- **Due diligence**. The objective of the Due Diligence / discovery is to verify all information received, confirm solution and pricing proposed, and to collect the required information to complete the design and transition planning.
- **Design Phase**. Create a client solution that will meet all client needs through a combination of standard service offer options and any required bespoke technical components. While the goal is to use 100% standard service offer options, NTT recognizes that many clients have complex environments that require some bespoke components and stands ready to support all client needs.
- **Contract negotiations**: Define, negotiate and agree all legal agreements between the client and NTT. This includes Service schedules, definitions and commercial terms.
- **Detail transition planning**: The initial phase of the NTT transition project is the planning and preparation phase. The success of the transition relies heavily on the time and effort spent on various assessments, implementation of transition governance, and ultimately detailed planning, and will include:
  - Initial transition project planning
  - Confirming transition activities from agreements & due diligence report
  - Defining the transition (transition management plan)
  - Defining sub-streams, resources, work packages & deliverables

- Establishing transition governance
- Kicking-off the project with the core project team.
- Establishing a communication framework
- Project risk documentation and examination
- Project plan development and review
- Final planning and sign-off

4.1.2 Transition Phase

The following high-level activities will be performed during this phase, and are typically those activities we perform to build, deploy, test and hand-over all the contracted services.

- Continuous communication as per the agreed communication plan
- Human resource transition
- Documentation of service operations procedures
- KPI analysis and reporting development
- Training planning and implementation
- Allocate all account and support staff
- Implement / Integrate Service Desk
- 3rd party alignment & contracting
- Start with change management
- Establish intercompany connectivity
- Establish and configure management toolsets
- Define, agree & implement all process touch points
- Detail services hand-over planning
- Exit incumbent (if applicable)
- Go-live of services

4.1.3 Post Transition Phase

The objective of the post transition phase is to help ensure the support environment is stable and delivering as per agreement, implement corrective actions, complete final operational documentation, and to formally close the project.

Activities during this phase include:

- Ensuring all documentation is updated and stored safely
- Ensuring delivery as per the agreement
- Implementing any corrective measures where needed

- Handing over transition results to the Operations Manager
- Reviewing subcontractors
- Documenting lessons learned
- Releasing all resources

4.2. Programme Management

The overall management of the entire transition project is facilitated through the transition manager, and a joint steering committee, if required. If implemented, the steering committee will make all executive level decisions regarding the direction of the project and resolve any major conflicts or concerns presented by the transition manager.

NTT desires a collaborative approach to jointly develop and agree for the provisions of the transition planning. This approach, based upon joint fulfilment, is a substantial requirement and critical success factor for the successful completion of the transition. There are specific tasks that the client will be responsible to complete during transition.

4.3. Our Critical Success Factors

NTT collects metrics and performs analytics on all service transitions, to review our critical success factors for service transitions and to identify opportunities to improve our approach. Critical to our success is:

- Utilising automated discovery and automated activation – to reduce the lead time to on-board MHIS into the client's environment
- Leveraging our Manage Centre to have an open engagement with you and to communicate time-value clearly and regularly
- Using a clear set of acceptance tests to help ensure a successful operations handover

4.4. Key Deliverables

4.4.1 Project Management Plan Documentation

The project management plan provides guidelines for both project execution and project governance. This documentation must be approved by the client and NTT. The primary functions of this documentation are to document planning assumptions and decisions, facilitate communication among project stakeholders and baseline approved scope, cost and schedules.

4.4.2 Project Change Request Documentation

The Project Change Request documentation is the project management tool used for requesting any changes to a project. Typically, this is needed when discrepancies

are discovered between the design and the actual client environment. All changes will be evaluated by NTT and the client and are executed once accepted by all parties.

4.4.3 Handover Documentation

Handover documentation is delivered as confirmation that the scope defined in the Project Management Plan documentation has been successfully completed. The Handover documentation requires formal agreement and validation from the client and NTT before the project can be transitioned to service operations.

4.4.4 Business Services

Business services (also known as workloads) are client-defined “objects” that deliver an outcome for the client. An example of a business service is a payroll system that consists of web servers, database servers, firewalls, load balancers and routers. Defining these business services during the transition phase allows client discussions to be outcome-focused rather than asset-focused.

During service transition, NTT will work with the client to define these business services (i.e. what individual IT assets (servers, storage, etc.) comprise each business service). The business service definitions are loaded into the NTT platforms and the client can manage service tickets against them.

4.4.5 High Level Design Document

The High Level Design document (HLD) provides a description of the solution explaining architectural principles and high level design for the infrastructure. The HLD must be formally accepted by the client as part of completing the Solution Design. All of the key information used to create the HLD is documented and maintained as part of the MHIS Knowledge Management process.

4.4.6 Low Level Detail Document

The Low Level Detail document (LLD) is an extension of the HLD which provides low-level details for infrastructure, applications, storage and the networking design for the solution. The LLD is used by the technical teams to deploy and configure the components of the technical solution.*

***Projects involving SAP require a more detailed HLD than standard projects, and therefore a separate LLD is not required. See the *Managed SAP Common Activities* service description for more details.**

4.5. Specific to Take Over an Existing Solution

For projects that require the take over of an existing solution, NTT will perform an audit of the system. Specific audit activities are dependent on the scope of the service and the devices to be managed. Audit activities may include, but are not limited to the following:

- Platform including services running, software and component dependencies, etc;
- Inventory of Infrastructure, including hardware support contracts and requirements;
- PaaS/SaaS services, if any;
- Network design and requirements;
- Storage;
- Datacenter including location, remote hands requirements, escalation procedures;
- Cloud tenancy including any escalation requirements;
- Versions all systems;
- Licensing;
- Contingency plans including HA, Backup and DR;
- Security Standards and Requirements
- Service Quality, including service quality indicators

4.5.1 Key Deliverables

4.5.1.1 Audit Report

In addition to providing key information about the system, the Audit Report is used to identify any risks that may affect the delivery of the Service, and evaluates them as follows:

- **High Risk:** Take over of the service is not possible until remediation steps are completed by the client (in some cases NTT may provide remediation as a chargeable activity).
- **Medium Risk:** NTT can take over the service but SLAs will not apply until remediation is completed by the client (or NTT as a chargeable activity).
- **Low Risk:** NTT can take on the service, but recognizes that the solution does not yet conform to NTT standards. Risks will be remediated during service operations. SLAs apply.
- **Informative**: NTT can take on the service, but documents certain recommendations with which to improve the service. These are generally recommendations that are not urgent, and that can be implemented over time.

5. Service Delivery Roles and Responsibilities

5.1. Overview

NTT believes that operations delivery is most effective when the same resources are engaged in the entire service lifecycle of a solution. For this reason, many Service Delivery team personnel are responsible for both the project implementation and the ongoing service operations of a client. Other roles are limited to the implementation (e.g. Service Transition Manager) or on-going service operations (e.g. Service Delivery Manager).

The diagram below illustrates how the different teams are involved along the service lifecycle.

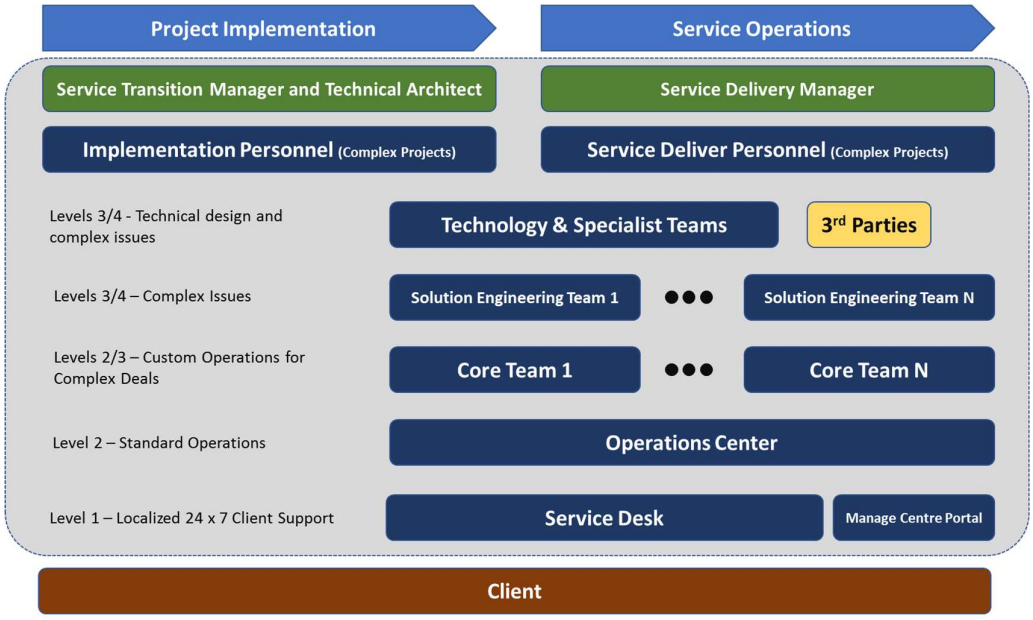

Figure 4 – Service Delivery Teams

5.2. Manage Centre Portal

Manage Centre is NTT's award-winning client-facing portal with which MHIS tickets can be managed. Clients manage their service tickets relative to "business services". Business services are client-defined "objects" that deliver an outcome. An example of a business service is a payroll system that consists of web servers, database servers, firewalls, load balancers and routers.

5.3. Service Desk

The service desk is the primary Point-of-Contact (POC) for the client. Clients can make service requests, report incidents and check on tickets via phone and/or email. The service desk is localized to the client's country or region.

5.4. Ops Centre and Engineering Teams

The Ops Centre is the main team responsible for managing the client. Its three primary tasks are:

- 24 x 7 x 365 response to monitoring alerts;
- 24 x 7 x 365 incident management (runbook based)
- 24 x 7 x 365 standard service request fulfilment

Supporting the Ops Centre are various engineering teams, each with a different focus and specific skillset. *Core* engineering teams are generally semi-dedicated and are assigned to a small group of clients, allowing for a level of familiarity with the systems they support. For solutions of a larger scale and greater complexity, a dedicated engineering team may be assigned. For some solutions, specialist engineering teams may be assigned to support technologies that require specific expertise (for example, SAP). In all cases, these semi-dedicated and dedicated engineering teams are responsible for all escalations, and any Incidents or Requests which cannot be resolved via standard operating procedures (SOPs) or client runbooks.

5.4.1 Lead Engineer

Each project is assigned a Lead Engineer. The Lead Engineer is responsible for executing project tasks during the solution set-up and is the ultimate internal escalation point for the most complex technical issues related to the client. The Lead Engineer ensures that all the necessary aspects of the technology and MHIS are accurately documented.

5.5. Complex Project Roles

Where NTT has evaluated a project as being "High" or "Very High" in complexity, the following roles may be assigned:

5.5.1 Technical Lead

The Technical Lead (TL) is a technical architect internal to NTT. As a member of the Technology Team, the TL is the technical authority within NTT and responsible for the technical scope of the project, coordination between internal teams and 3rd parties contracted by NTT and ensuring that the solution design meets the client's technical requirements.

Independent of the client solution, the TL manages the process of certifying any new technologies which need to be standardized by NTT.

5.5.2 Service Transition Manager

The Service Transition Manager (STM) is the internal project owner for NTT. The STM is responsible for managing the scope, coordinating internal teams and 3rd parties contracted by NTT, ensuring project tasks are completed on time while adhering to NTT quality standards, managing risks, project cost control and general communications.

5.5.3 Service Architect

The Service Architect (SA) begins supporting an opportunity during the sales engagement process and is primarily responsible for understanding the project requirements and defining all elements of the Services Delivery Model. The SA focuses on the tactical aspects of service delivery, such as mapping services to the client's business functions, making sure that the tools and documentation are set-up properly for client support and to meet client expectations.

5.5.4 Compliance Manager

A Compliance Manager (CM) is assigned to accounts that require a high level of security or require compliance with certain standards or regulations. The CM begins supporting the opportunity during the sales engagement process and is primarily responsible for understanding a project's security requirements and helping to define the elements of Service Operations so that security requirements are met. Once the project is delivered, the CM will verify that the security controls that have been implemented are maintained and functioning to meet the client's security and compliance requirements. The CM is also the person responsible for any security aspect related to the service provided.

5.5.5 Cloud Architecture Community

This virtual community is comprised of public cloud domain specific experts. Public Cloud is evolving so frequently that specialist skills are required to client solutions can evolve at a similar pace.

As such NTT provides a central governance, best practice and standards function comprised of senior Cloud Architects. This team works with NTT Cloud Architects based in each country who work and directly interact with client.

The NTT central team is responsible for:

- Standardization and sharing of processes and methodologies
- Providing technical support to regional Cloud Architects
- Leading regular review sessions with regional Cloud Architects

The regional Cloud Architect is responsible for:

- Working directly with the client to consult, analyze and recommended solution optimizations and evolutions.

- Capturing public cloud design requirements and reviewing these with NTT to ensure a fit for purpose solution which can be delivered and operated.

6. Further Information and Next Steps

6.1. Additional Details

Additional details for each of the service offer options are available in the MHIS Services Guide. The Services Guide addresses:

- Supported technologies
- Monitors
- Notifications
- Requests
- Maintenance Tasks
- Roles and Responsibilities

The NTT sales team can answer any questions that this MHIS CSD and the MHIS Services Guide do not answer.

6.2. Next Steps

NTT's clients are all in a unique place on their IT transformation journey and no one solution is 100% aligned to all client needs. It is the goal of MHIS and other NTT managed services to meet the client where they are and accelerate their IT transformation journey. To this end, the NTT sales team will engage solutions architects and other Subject Matter Experts (SME's) to design a client-focused managed services solution, of which MHIS may be only one part. Consulting and professional services are available as needed.

As always, NTT is ready to assist at any required level of engagement.