NTT

Outcome-based delivery success criteria for managed services

Business mandates to improve the client experience, combined with rapid technology change, are leading many companies to rethink the role of their internal IT organizations. Technology changes and the integration of legacy and cloud-based infrastructure brings complexity in terms of interoperability and management. Our research indicates that 60% of all companies engage in digital transformation through outsourcing and partnering. Managed service providers can de-risk transformational change and deliver a more efficient operating environment that enables IT leaders to turn more of their focus on driving business transformation.

A managed service provider's ability to support their clients in meeting these objectives is dependent on several key capabilities:

- Reducing the complexity and risk in managing a hybrid IT landscape.
- Employing automation to accelerate time to value with new digital transformation initiatives and technology deployment.
- Integrating seamlessly into the client's existing processes and in-place technology investments.
- Demonstrating the security and data privacy in their development and operational processes and practices.
- Offering ongoing innovation that is transferred to their clients.

These are the success factors NTT uses, both in the development of our Managed Services Platform and the operation of our Managed Services. Our Managed Services Platform is the foundation upon which we deliver our Managed Services and the operational outcomes our clients expect.

It is a combination of our global tools, processes, technology, and intellectual property, with capabilities that are ITIL aligned, vendor-independent, and delivered consistently around the world.

Table of Contents

Managing a hybrid IT landscape

Today, the IT landscape throughout all companies has become significantly more complex. Non-programmable infrastructure (e.g. physical network routers, switches, and physical servers) continues to operate, along with cloud-based and programmable infrastructure (e.g. SDWAN applications, cloud control wireless access, voice applications). Heterogenous and distributed endpoints will continue to proliferate. More and more data is being gathered and often analysed at the edge, closer to the clients and end-users. Workloads are often required to run across different infrastructure platforms to improve redundancy, aid in migration and/or to reduce cost.

A managed service provider must be able to efficiently manage and improve the client's operational environment across this diverse landscape. A managed service provider should demonstrate the capability to enable their clients' workloads (all the individual capabilities and units of work that make up a discrete application – inclusive of software and the virtual and physical infrastructure required to run the application as expected) in the cloud, on-premises, or in a hybrid IT environment.

We offer a unique architectural approach to workload and IT operational task automation and management to reduce complexity by decoupling the workload from the underlying IT operation and leveraging reusable micro-service capabilities to accelerate time to value in workload deployment.

An architecture built on microservices that can be used repetitively, as needed, eliminates the duplication of complex tasks across workloads and reduces human error. Our reusable components enable us to configure our Managed Services to improve client outcomes. Our objective is to deliver sustainable improvement to our clients' IT operations, supporting their technology, process innovation, workload migration, and systems integration.

Microservices approach

Microservices approach segregates functionality into small autonomous services, and scales out by deploying independently and replicating these services/ VMs/containers.
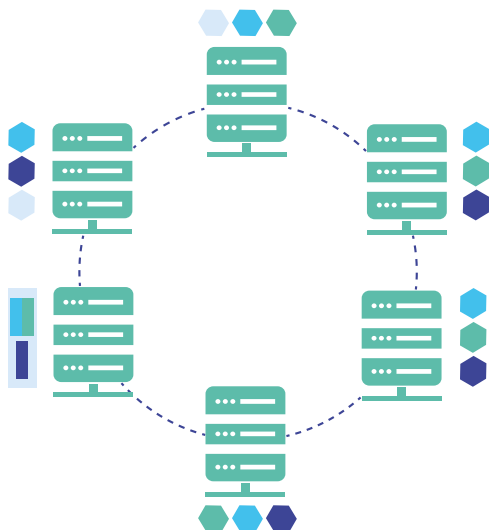
VS

Traditional approach

A Traditional application (Web app or large service) usually has most of its functionality within a single process (usually internally layered), and scales by cloning the whole app on multiple servers/VMs/ containers

App 1   *App 2*

App 1
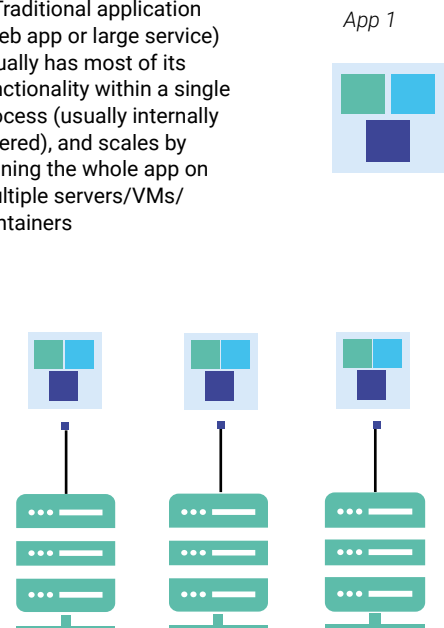
Another essential element of reducing complexity in a hybrid environment is by providing a window into the client's IT landscape, so that they have readily accessible views of the health and status of their environment and can call up detailed service and asset lifecycle reports on demand. This gives clients the self- service ability they require to improve their IT decision making and access real-time visualization of key performance indicators.

Our Manage Center interface provides a window into the health and performance of our clients' IT operating environment and the self-service capabilities needed to interact with us. Its award-winning design enhances the user experience. This self- service interface provides management dashboards, along with drill down capabilities that provide a real-time, highly transparent view on the status, health and performance of their environment at any time.

The Manage Center enables real-time, self- help services to clients. For example, as the client describes a situation, we can read this information in real-time, and with this visibility and intelligence the system can serve up appropriate knowledge articles that are directly related to the situation described, to provide the client with self- help assistance when they require it.

Employing automation to accelerate time to value

Fast-moving business and the need for rapid deployment of new technology necessitates speed. Additionally, given the critical IT skill shortage faced by most IT organizations, supplementing in-house capabilities is critical in outcome-based delivery.

Process automation not only reduces cost but improves availability and the overall quality of service delivery. Manual provisioning and patching processes introduce costly errors, impact availability and delay implementation. Automation improves governance, simplifies processes and improves availability.

Embedded within our Managed Services Platform are the automated processes and tools that support service level management, service activation, incident management, release management, vendor management, problem management, and change management.

Operational automation capabilities span diagnosis, remediation, and service operations. We leverage machine learning to continuously improve our capabilities to automate, diagnosis and restore.

Diagnosis capabilities include eliminating noise to reduce the number of false positives and facilitating diagnosis by enriching the incident information with contextual information. Restoration is automated where feasible. It is invoked for many MACD changes and to validate the health of IT infrastructure components through proactive testing. We use multiple sources of data to predict capacity and service degradation. This allows us to take preventative actions, anticipating outages and proactively taking action to prevent them.

Automation can be used to monitor the end-user experience. An example of this might be a point of sale system, where we would test every system remotely every morning to make sure they are able to perform a transaction. If there is an issue, the root cause can then be determined, and the appropriate steps taken to resolve it - sometimes with no human interaction necessary.

Automation at the workload level is used to spin up a machine, back it up, and complete user administration, making life- cycle management of these environments more efficient.

With our Managed Services Platform, a standardized reference architecture can be deployed for an entire workload on premise, in a private enterprise cloud, or in a hyper cloud environment like Amazon or Microsoft Azure. A reference architecture provides the ability to take a client infrastructure function - like voice communications - and transform it onto a best practice configuration and infrastructure that is vendor certified, scalable and standardized, to allow for a high degree of automation in the build and configuration.

Adopting a reference architecture accelerates delivery and time to value, providing a sound basis for governance that simplifies hybrid management across multiple environments. It can reduce outages, improve administrative responsiveness, and improve resilience for our clients.

Integrating seamlessly into processes and in-place technology investments

The ability to integrate into the client's existing processes and in-place technology investments is a key dependency in reducing complexity, improving overall IT operational efficiency, and securing the overall IT environment. Given the dynamics and speed of change required by client organizations, service integration capabilities should be made available through the universal language of open APIs (application programming interfaces), so they can be used by different workloads, on different kinds of infrastructure.

Points of integration should include the following:

- Integration of systems management processes between the client, the managed service provider and technology vendors.
- Event integration to manage and distribute inbound and outbound events and support third party integration.
- Allowing for operators to easily enable services for newly onboarded configuration items.
- Invoking automation from any capable platform and capture output.
- Data replication to support synchronization between master and transactional data.
- Integration with client monitoring tools.

Within our Managed Services Platform, the Service Integration Layer decouples workloads from the underlying IT operations. The Service Integration Layer enables all the complex functions common to workloads to be provided as a service. When an application requires a specific function, it leverages the micro-service that represents that function eliminating duplication of complex tasks. Our Service Integration Layer works in conjunction with the infrastructure and workload operations management components to enable automation and integration with client systems, and third-party systems for both service processes and transactional data.

## Demonstrating security and data privacy in development and operational management processes and practices

Fundamental to the success of managed services providers and essential in a client's selection of a provider are the management practices used in software, offering development and their ongoing service operations, which ensure that data is secure and data privacy requirements are maintained.

We recommend inspection within the following areas:

- security practices and standards embedded within the provider's system development processes
- industry certifications and standards
- privacy and data sovereignty practices
- privileged access management
- vendor management

Although clients inquire and inspect operational security processes for prospective managed service providers, many fail to ask the right security questions around software development. IEEE Software Magazine reported that although the best commercial software companies remove about 95 percent of all known defects before releasing software to the customer, the industry average is less than 85 percent.
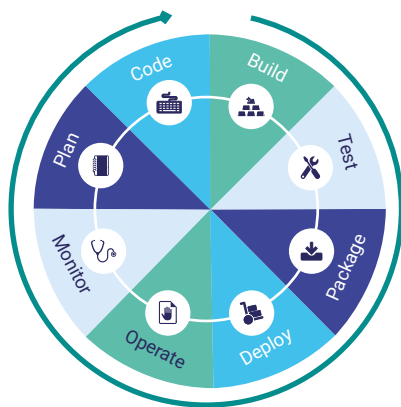
DevSecOps (Development Security Operations)

Security must be planned and managed at every stage of the software development life cycle to protect sensitive information and ensure that the application is devoid of viruses, trojan horses, logic bombs, worms, agents, applets, and any other malicious code. Security activities that include static analysis, code review, and architecture design review are critical within software security assurance processes.

These security activities are required to find and eliminate:

- web application security risks and common security weaknesses
- design and or logic issues
- any issues associated with authentication, credential management, privacy, logging, and firewalls

It is also important to ensure that any third- party products used to deliver a service are secure and are implemented securely.

Prior to and after deployment, penetration testing or 'white hat' hacking needs to be employed to find any security vulnerabilities that an attacker could exploit.

Security certifications - and the use of recognized industry best practices - are other criterion that are used to evaluate and select managed service providers. **The following certifications and best practices should be required by your provider**:

- ISO/IEC 27001
- ISO/IEC 27018
- SSAE-16
- CSA STAR

Managed service providers privacy and data sovereignty practices are now more critical than ever to maintain compliance with regional and national requirements for protecting personal data and abiding by applicable laws that define who has control over and access to cloud-stored data.

Questions to be answered by the provider should include: Who has access to what data and when? How and when is personal data protected? What access control and audit processes are deployed? The ability to integrate into the clients' enterprise identity access management systems is also key to ensuring consistency of permissions and assignments.

Is privileged access management in place? Privileged access management uses a secure repository that requires authentication to isolate the use of privileged accounts (typically admin accounts) and reduce the risk of these credentials being stolen.

Logging and monitoring is maintained for these privileged accounts. Operator access to client devices needs to be recorded and the recordings available to the client. Multifactor authentication should also be required on all administration accounts.

Just as these practices are critical to be in place with the managed service provider, it is equally important that the provider's vendor management process use these criterions in their selection of the technology and software they deploy as integral components of their service offering.

Your provider should be able to demonstrate that they have a mature information security practice, with broad threat monitoring and established incident management. A good indicator of how a service provider will secure a client is how they secure themselves.

With our platform, we support all of these practices. Additionally, with our microservices approach we can decouple authentication from authorization adding yet another security layer. Our user directory microservice can be integrated with our clients' active directory. Sensitive information is always protected using permissions, encryption, and masking.

Offering ongoing innovation that is transferred to their client base

Clients should require continuous innovation from their managed service provider. Questions regarding the service development process and approach to ongoing development and innovation should be posed to prospective providers.

Our approach to development is to create an intelligent core and an intelligent edge. The core is where we build scale and functional capabilities that are common among all our clients. The edge is where we cater for the unique requirements of each client. As unique functionality is found to benefit many clients, we can capture this and integrate into the intelligent core easily with the underlying microservices architecture.

We've adopted the **Scaled Agile Framework (SAFe)** as our development methodology – the way we develop our services and bring them to market. This process enables us to focus development on the right market requirements, control change, make modifications quickly when required, and bring new capabilities to market quickly.

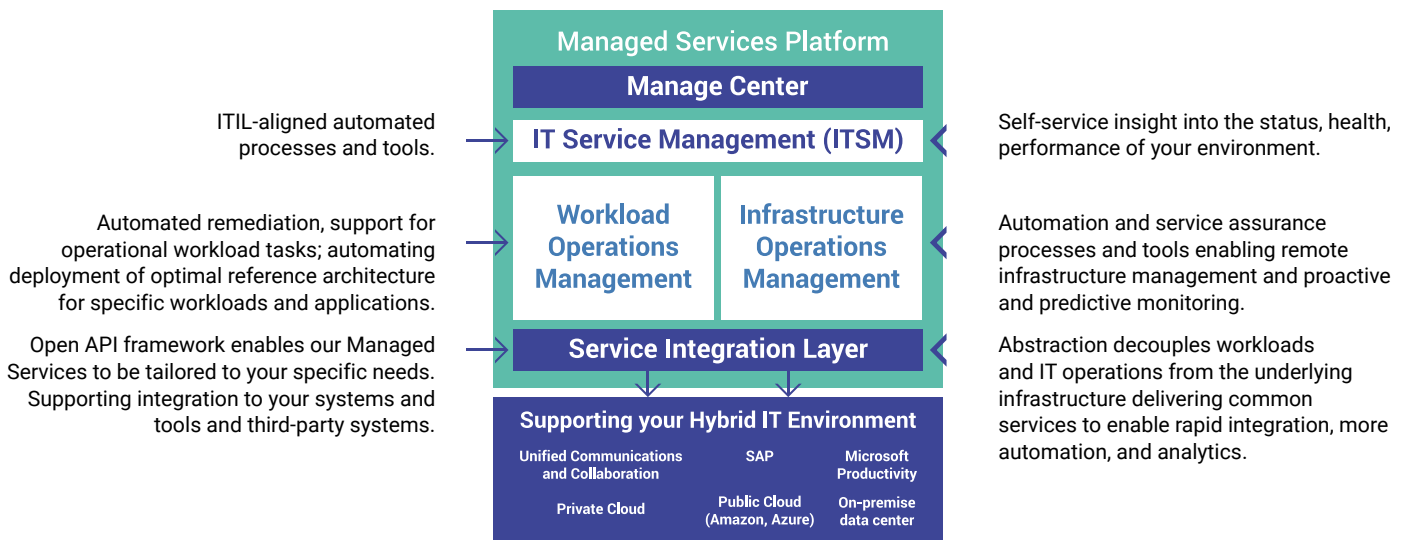## Overview of NTT's Managed Services Platform

The Managed Services Platform provides the capability to integrate, automate, manage, and optimize operations in a vendor-independent fashion within a hybrid IT landscape at scale, globally, and consistently to deliver substantiated SLA-based outcomes.

It enables us to proactively and cost-effectively manage our clients' collaboration, productivity, contact center and cloud workloads, as well as the programmable platforms, programmable infrastructure and non-programmable infrastructure that underpin these workloads. It also provides our clients with visibility into their operating environments. Our Managed Services, delivered via our Managed Service Platform, allows us to support organizations in improving the control of their hybrid IT environments and automate key processes.

Key capabilities of the Managed Services Platform are summarized in the diagram below.

The platform:

- Enables the automation of operational tasks to accelerate change and resolve issues faster.
- Provides capabilities needed to simplify the management of complex hybrid and multi-cloud IT operating environments.
- Seamlessly integrates programmable platforms, programmable infrastructure, and non-programmable infrastructure.
- Supports faster deployment of new technology and workloads.
- Improves service quality improvement through process automation, preemptive and proactive support.
- Delivers near real-time visualization of key performance indicators.

ITIL-aligned automated processes and tools.

Automated remediation, support for operational workload tasks; automating deployment of optimal reference architecture for specific workloads and applications.

Open API framework enables our Managed Services to be tailored to your specific needs. Supporting integration to your systems and tools and third-party systems.

Managed Services Platform

Manage Center

IT Service Management (ITSM)

Workload Operations Management

Infrastructure Operations Management

Service Integration Layer

Supporting your Hybrid IT Environment

Unified Communications and Collaboration

SAP

Microsoft Productivity

Private Cloud

Public Cloud (Amazon, Azure)

On-premise data center

Self-service insight into the status, health, performance of your environment.

Automation and service assurance processes and tools enabling remote infrastructure management and proactive and predictive monitoring.

Abstraction decouples workloads and IT operations from the underlying infrastructure delivering common services to enable rapid integration, more automation, and analytics.

Conclusion

Managed service providers can de- risk transformational change and deliver a more efficient operating environment. To be successful in achieving these objectives, the provider should be able to demonstrate their capabilities to: manage a hybrid landscape; use automation to enable efficiency, time to value and reduce human error; integrate with the client's IT systems; use security practices in both development and operations; and, deliver ongoing innovation to their clients.

Our Managed Service Platform that forms the foundation for our services enables these capabilities.

Industry analysts indicate that we offer a unique architectural approach to workload and IT operational task automation by decoupling the workload from the underlying IT operation and developing reusable micro-service capabilities to accelerate time to value in workload deployment.

We demonstrate innovation in the use of abstraction, micro-service capabilities, and container technology. Our Managed Services Platform, combined with our experience, differentiates us from our competition.

Automation, tools, and platforms provide efficiency, scale, consistency, risk mitigation, uptime, and insight into software, hardware, and systems. IDC believes the increased use of automation **will be transformative to the way that services will be delivered and consumed as a result of** integrating automation into service delivery **as it will impact people and process, and the value that enterprises derive from their IT investments.**'

– Leslie Rosenberg, Research Director, Network Life-Cycle Services

IDC, Future of Services Delivery

Disclaimer: The work described in this thought leadership was performed while the company was known as Dimension Data.

NTT