NTT DaTa

Accelerating Application Migration to the Cloud

NTT DATA welcomed Dell Services into the family in 2016. Together, we offer one of the industry's most comprehensive services portfolios designed to modernize business and technology to deliver the outcomes that matter most to our clients.

About NTT DATA

NTT DATA is a leading business and IT services provider and global innovation partner with 100,000 professionals based in more than 50 countries. NTT DATA emphasizes long-term commitment and combines global reach and local intimacy to provide premier professional services, including consulting, digital, managed services, and industry solutions. We're part of NTT Group, one of the world's larger technology services companies, generating more than $100 billion in annual revenues and partner to 85% of the Fortune 100.

Introduction

Increasingly, banks and financial institutions are taking a business-first approach to digital transformation and adopting cloud-based computing to achieve greater business agility and competitive differentiation in the market. Banks need to choose the right cloud strategy and application migration approach to realize the real benefits of cloud. Banks also need to overcome challenges in addressing security and compliance to regulations such as Federal Information Security Management Act (FISMA) and Payment Card Industry Data Security Standard (PCI DSS).

This paper provides quick insights into how banks are adopting cloud, approaches for migrating applications to the cloud, and solutions for addressing challenges with security and regulatory compliance, and getting started with the cloud journey. It also explores a detailed case study where NTT DATA helped a major global bank adopt cloud for achieving greater business benefits while ensuring security, privacy, residency of data and compliance to regulations.

Cloud adoption trends in banking, investment and financial services

Major global banks are increasing their cloud investments and shifting enterprise workloads to both public and private cloud. In fact, a recent RightScale survey found that private cloud adoption increased from 63% to 77%, driving hybrid cloud adoption up from 58% to 71% year over year.

71%
hybrid cloud

Shifting Private To Hybrid

Private cloud adoption increased from 63% to 77%, driving hybrid cloud adoption up from 58% to 71% year over year.[1]

New low-code platforms deliver at digital clock speed

Banks, and insurance and financial services organizations are using innovative low-code platforms to quickly build multi-channel customer-facing cloud applications.[2]

Cloud-native and cloud-enabled continuous delivery

Banks, and insurance and financial services organizations are using innovative low-code platforms to quickly build multi-channel customer-facing cloud applications.[2]

11%
shift of IT budget from traditional in-house IT delivery toward cloud computing as a new delivery model by 2016.

60%
of new applications will use cloud-native application architecture to enable faster innovation and agility by 2017.

35%
of new applications will use cloud-based continuous delivery by 2018.[3]

Banks adopt public cloud in many areas, which include but are not limited to:

- **Collaboration:** Connecting employees across branches to access banking systems
- **Development and testing:** Enabling banks' development and testing teams to quickly and easily create virtual environments, which increases agility
- **Analytics:** Integrating customer data across banking platforms to enable near-real-time insights
- **Business intelligence on demand**

Major global banks follow a hybrid approach due to security, privacy and regulatory concerns. Public cloud-based services are leveraged for non-critical functions such as email management, collaboration and content management. Enterprises adopt externally hosted, private cloud-based services for application development, test environments and processing and analytics.

1. "2016 State of the Cloud Report." RightScale. January 2016.

2. "The Forrester Wave: Low-Code Development Platforms, Q2 2016." Forrester and OutSystems.

3. "IDC FutureScapes 2015."

NTT DATA

Cloud application migration approach

Typically, organizations who want to move to cloud need to have a cloud strategy in terms of choosing the right cloud models and cloud service providers (CSPs) based on their business and IT strategy. Organizations also need to have an application migration strategy to choose the right migration paths and options for their applications based on their goals, priorities, risks, return on investment, technology, platform and tools. Some applications can be deployed in the cloud using re-host or lift-shift strategies while others need to be optimized for cloud to realize the real benefits.

The decision to choose the right cloud strategy and application migration strategy is primarily based on an organization's existing application and infrastructure portfolios. This means the cloud application migration journey begins with the assessment phase. While there are different approaches for migrating applications to the cloud, NTT DATA suggest an incremental and phased approach. Figure 2 depicts one of the suggested approaches for migrating applications to the cloud.

This approach is based on an application portfolio analysis where existing applications are analyzed for complexity, dependency on external applications, design elements and user interfaces. Redundant applications are grouped based on their functionalities, so they can be optimized to reduce the number of applications on the target cloud platform during the migration phase. Figure 3 depicts our framework for cloud readiness assessment.
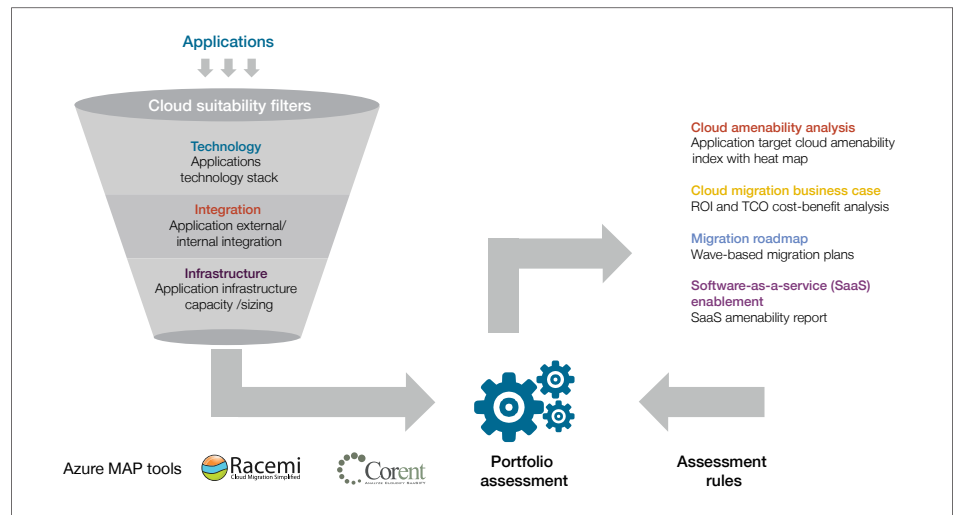

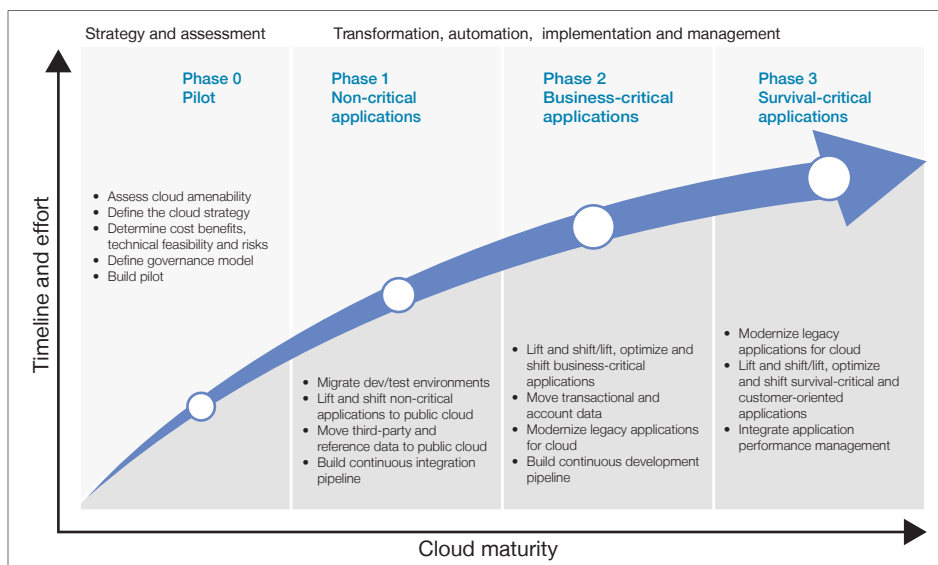Figure 3: NTT DATA cloud readiness assessment framework

Figure 2: Cloud application migration approach and roadmap

NTT DATA

An assessment of cloud readiness is performed based on workload patterns, resulting in a cloud amenability map that lists various groups of applications and their risks. Figure 4 depicts the classification of sample applications and business processes for investment banking.

	Non-critical applications Public cloud	Business-critical applications Hybrid cloud	Survival-critical applications Private on-premises cloud
Trade management (front office)	• Client/partner/trading portals • Pre/post-trade analytics	• Customer service • Customer acquisition	• Pricing and structuring • Trade capture and enrichment • Client onboarding
Middle office	• IT trade support • Reference data management	Deal confirmation	• Risk analysis • Post-trade compliance
Clearing (back office)	Regulatory reporting	• Regulatory reporting • Depository and investor services • Securities lending • Collateral management	• Investment/fund accounting • Income and dividend processing
Common business processes	Email, employee collaboration tools	CRM, AML, SOX risks management	Risk monitoring and reporting
Data management services	Market reference data, Securities reference data		Product data, pricing data, trade data, advisory data

Figure 4: Sample applications/business process classification for investment banking — actual classification may vary depending on assessment of an organization's applications and business processes

Based on the assessment results, the deployment architecture is designed and a migration plan (for existing applications) and execution plan are created. One or more of the following application migration options are chosen based on the outcome of the assessment:

- Re-host or lift-shift: Redeployment of existing applications on cloud infrastructure changing an application's code and infrastructure configuration
- Refactor or optimize: Change of application code and configurations for open source and deployment of refactored applications on cloud infrastructure
- Re-architect: Breaking up monolithic application functions into modular services based on distributed and modern architectures such as microservices architecture
- Rewrite: Rewrite existing applications leveraging cloud-native platforms such as Pivotal Cloud Foundry for accelerated delivery
- Replace: Replace existing applications with commercial SaaS to satisfy the business requirements

Addressing security and regulatory compliances

CPSs, such as Amazon Web Services (AWS) and Microsoft Azure, offer out-of-the-box cloud services that can be used off the shelf by banks. This helps them overcome challenges with security and regulatory compliance such as:

- Compliance with regulatory standards: CSPs assure compliance through various certifications. For instance, Azure and AWS are compliant with FISMA Moderate standards and with PCI DSS. With PCI DSS, AWS complies with a set of controls important to companies that handle credit card information. With the FISMA standards, AWS complies with a wide range of specific controls required by U.S. government agencies.
- Data security and residency: Use encryption and tokenization services provided by CSPs for securing data at transit and at rest depending on the requirements. For data residency requirements, a tokenization mechanism can be used to replace sensitive fields with randomly generated tokens that are structurally similar, but have no mathematical correlation to the original data. The encryption and tokenization methods, keys and tokens can be securely stored on-premises and controlled by banks.
- Auditing and logging: Banks can keep a signed audit trail of which users performed what actions leveraging audit trail services provided by leading CSPs. Banks can implement sign-in certification and encryption mechanisms for the log files to be stored in the cloud. They can also implement robust audit logging and best practices to quickly detect unauthorized access to services, resources and applications in cloud.

NTT DaTa

Client success story

Private cloud deployment for a leading bank and financial institution in the U.S.
Background

A leading provider of banking, mortgage, investing, card, insurance, consumer and commercial financial services in the U.S. wanted to embark on their cloud transformation by migrating 1,400 applications across lines of business to private cloud. They had concerns about security, privacy and residency of their transactional, account and customer data, and approached NTT DATA Digital Business Services for a solution.

Challenges:
- Risk of moving applications to the cloud due to security, privacy and regulatory compliance
- Security threats associated with cloud services — sensitive information needed to be protected to ensure only authorized users could access sensitive data
- Reduced performance for data-intensive applications due to cloud network bandwidth and latency
- Unable to ensure availability of cloud services and the ability to build applications in the cloud for high performance
- Difficulty integrating applications and data between multiple environments
- Longer lead time accessing 1,400 applications and identifying candidate applications for cloud
- Longer time to provision and install all required software
- Needed to improve application delivery speed — with no compromise on quality or regulatory compliance

Solution:
- Enabled assessment of all levels of security - policy security, environment and infrastructure security, systems and platform security and data security
- Accelerated cloud amenability analysis of applications and business processes with the Cloud Portfolio Assessment solution by NTT DATA that automatically generates a heat map report based on the inputs from the application portfolio analysis
- Built a private cloud using a Microsoft Cloud Platform System (CPS) joint solution that provided portals for self-provisioning of virtual machines
- Automated the provisioning of environments using our pre-built environment provisioning patterns and templates
- Implemented robust data security and data residency solution using Secure Sockets Layer, encryption and tokenization techniques
- Developed a comprehensive disaster recovery and availability plan, optimally designed and configured input/output operations per second for I/O intensive workloads in Microsoft CPS and demonstrated improved performance by running capacity test cases under various loads and conditions
- Built continuous delivery pipeline through integration of various tools including testing tools and orchestrated release processes using the DevOps Automation solution by NTT DATA with extended Microsoft Azure plugins and adapters
- Enabled self-service and automated deployment of applications to private cloud using our pre-built deployment blueprints, templates and scripts

Results:
- Created a private cloud environment similar to a public cloud platform-as-a-service environment
- Provided a foundation for ensuring all four levels of security prior to migration with our risk assessment framework
- Enabled faster assessment of applications in just three weeks with our cloud amenability framework
- Enabled provisioning of environments in one day using our pre-built templates and code with Microsoft CPS
- Scaled cloud-migrated applications to meet scalability, performance, integration and security
- Built a one-click deployment to deploy to Windows Azure Pack
- Enabled feedback to developers in one to two hours
- Reduced application release time to one day
- Estimated expected reduction in production and environment related issues around 75%

Summary
Enterprise organizations should follow a hybrid approach and, based on their cloud readiness and risks assessments, adopt an incremental phased migration strategy, leveraging different cloud service models and migration types for a better return on investment and business benefits.

Visit **nttdataservices.com** to learn more.