NTT DATA Services

POINT OF VIEW | FINANCIAL SERVICES

Considerations for Data Protection When Outsourcing Core Functions

FEBRUARY 2019

NTT DATA

Follow Us:

@NTTDATAServices

Connect With Our Experts:

David.Tyrrell@nttdata.com

Siddharth.Sharma12@nttdata.com

Financial institutions across the globe are under constant pressure to make the best use of technology to optimize costs and improve the customer experience. Lloyds Bank recently revealed that it is speeding up the process of deploying a core banking application from the cloud.[1] According to the U.K. bank, its new cloud environment is expected to make development 10 times faster and three times cheaper.[2]

Through the bank's hybrid-platform-as-a-service model, the bank aims to make systems work together whether they are hosted in-house, in its offsite private cloud or on public cloud platforms. At the same time, the bank must carefully navigate the regulatory concerns of technology outsourcing, especially when outsourced functions involve customer data.

The European Banking Authority (EBA) released recommendations on outsourcing to cloud service providers in June 2018. The recommendations focus mainly on risk management by identifying specific challenges to banks, including "data protection and location, security issues and concentration risk, not only from the point of view of individual institutions but also at industry level, as large suppliers of cloud services can become a single point of failure when many institutions rely on them."[2] With the recent data breaches, regulators can't emphasize enough the importance of a proactive understanding of the risks associated with outsourcing any aspect of banking business operations.

Banking functions ripe for outsourcing

The matrix graphic on the right illustrates the banking functions that are ripe for outsourcing. Those in the upper left quadrant are good candidates for outsourcing customer data functions, according to NTT DATA research. This matrix takes into account factors such as criticality of service, volume of data interactions, value associated with data interaction or cost, whether service or functional typically deal with PII (personally identifiable information,) customer data and data classification, such as type of data interactions.

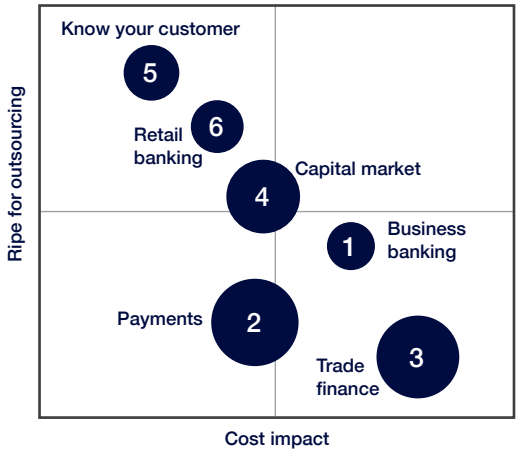
Let's take the example of now your customer (KYC) operations, which have high readiness for outsourcing with high potential for cost savings. In order for banks to perform the identity verification and screening for a corporate customer, the only information required by a third-party provider is the registered name and legal entity identifier. This makes it simpler for the banks to control what data is used to complete the process. In a scenario where the KYC application has been hosted on a cloud, controls like virtual desktop and data masking can be adopted to protect data in transit or data at rest. KYC processes can be standardized or defined, which makes them a good target for outsourcing.

While understanding the business function and type of data is important before deciding to outsource, banks have to also take into account regulatory activities. Regulators are taking a deep interest in the banking functions being outsourced. Two major regulations have a big influence on how and what functions are outsourced by financial institutions, the General Data Protection Regulation (GDPR) and the Committee of European Banking Supervisors Guidelines on outsourcing.

Regulators' perspective

The European Banking Authority will issue its final guidelines during the first quarter this year on what banks and financial institutions should have in place when outsourcing some of their functions to third parties, including cloud providers. However, there have already been many regulations that have emphasized the importance of securely managing confidential data as part of outsourcing arrangements.

General Data Protection Regulation (GDPR)
The recent General Data Protection Regulation (GDPR) requires organizations to ensure that their data processing activities are carried out in accordance



* The size of the sphere represents the extent of customer data usage

with data protection principles. Similarly, the Irish Data Protection Bill 2018 creates a new regulatory framework for the enforcement of data protection laws in Ireland in accordance with GDPR. The initial reaction by banks to GDPR guidelines has been to avoid outsourcing data processing services for applications handling personal data to a non-EU location. While this is a misplaced interpretation of the bill, GDPR impacts data processors and data controllers to a similar extent, bringing data protection practices to the forefront of business the agenda. The two most important aspects of the regulation from a personal data perspective require data controllers and processors to:

1. Take appropriate security measures against unauthorized access to personal data, or unauthorized alteration, disclosure or destruction of personal data, particularly where the processing involves the transmission of data over a network.
2. Put in place appropriate security provisions for the protection of personal data with regard to the current state of technology, cost, the nature of the data and the harm that might result from unauthorized processing.

Committee of European Banking Supervisors (CEBS) Guidelines on outsourcing and EBA Guidelines on cloud outsourcing:
The recent recommendations from the EBA on use of cloud services providers by financial institutions have confirmed that the financial institutions need to ensure they have a real understanding of the risks involved in outsourcing any aspect of banking functions and operations. The recommendations supplement the CEBS Guidelines.

Some of the key aspects of the risks are around:

- How **personal information** is **stored**
- How **personal information** is **used**
- How **customer data** is **protected**
- How much **dependency** is on **third-party providers**
- How the **security** of **cloud infrastructure** is **defined**

The potential for financial data to be mixed with other data on shared servers has also been an area of concern. According to the EBA's recommendations, this risk should be addressed by banks prior to getting into a cloud outsourcing arrangement, by deciding on "an appropriate level of protection of data confidentiality, continuity of activities outsourced, and integrity and traceability of data and systems in the context of the intended cloud outsourcing."[2] Financial institutions should also check whether measures are required for specific scenarios, including "data in transit, data in memory and data at rest, such as the use of encryption technologies in combination with an appropriate key management architecture."[2]

The three key aspects of these guidelines enable the financial institutions to:

- Ensure rights of access and audit by making sure that the agreement with the cloud service provider include provisions regarding rights to access the cloud service provider's premises and to inspect and audit without restriction by both the institution and competent authorities

- Implement appropriate levels of security of data and systems by making sure the service provider undertake to meet specific standards in terms of confidentiality, integrity, traceability, continuity of services and performance

Risks associated with chain outsourcing are addressed by the subcontractor fully complying with the outsourcing institution's obligations. Additionally, the service provider needs to make sure any changes to the subcontracting arrangement is completely visible to the financial services institution in case the new arrangement result in the initial risk assessment that the financial institution had conducted.

Service providers' perspective:

The GDPR and EBA guidelines are a step change in regulatory data protection expectations and have placed significant requirements on IT service providers in the EU and globally. To manage applications and operations, especially from a non-EU locations, banks should verify that their IT services providers adhere to the following guidelines:

1. **Data policies and procedures:** The internal policies of IT service providers need to align with data classification policies. Additionally, procedures must be in place to ensure correct implementation of personal data protection policies in compliance with a client's contractual requirements.
2. **Subject matter expertise:** IT services firms must have the tools, processes and people to ensure that all contractual clauses with clients pertaining to personal data are given adequate attention in terms of data management and confidentiality, compliance and legal expertise. This should include defining and particularizing multi-country data adequacy and data localization laws.
3. **Incident management for data breach and mitigation strategy:** Regular testing of the data management program in order to keep it up to date to provide timely notifications to the relevant stakeholders. There needs to be visibility on the data breach mitigation plan with multiple impacted customers.
4. **Outsourcing architecture compliant with privacy by design:** The provider's outsourcing solution architecture should be monitored and safeguarded regularly for any change in technology that might impact the personal data.
5. **Accountability and governance:** With a special emphasis by most regulators, the providers must establish a data protection office for senior-level responsibility to ensure the policies and processes are adhered to.
6. **Training programs:** Data protection training is provided on a regular basis to create awareness of personal data issues and regulations.

NTT DATA's perspective:

Outsourcing by financial services firms involving customer data is on the rise with firms now looking at third parties to manage some of their business functions and associated core applications. Regulators are leaving no stone unturned to tighten controls around data management and avoid any potential breaches, especially with financial services firms opening up to the use of cloud. The recent guidelines from EBA have made it clear that it is the accountability of banks to make sure any personal data being processed or stored on the cloud stays secure, with clear visibility into potential risks involved and a mitigation plan in place. The guidelines clearly define how banking institutions can make their agreements watertight with provisions to conduct necessary audits and fix responsibility. At the same time, service providers are proactively devising programs with adequate controls in order to ensure adherence to regulations with great transparency.

Whether or not to move any application or service involving personal data to the cloud is a strategic decision that involves a detailed understanding of costs and risks involved. The challenges of outsourcing business functions touching "all important client data" are evident from the measures (regulatory and otherwise) that banks have to undertake. However, the benefits of moving to a cloud-based outsourcing model are now proven, and banks have slowly started adopting this environment. Maximizing the benefits, while minimizing the costs and downside risks requires disciplined and comprehensive risk management. Banks need to do their due diligence when selecting the provider, carefully crafting service-level agreements (SLAs) and other safety nets such as using appropriate clauses to cover any potential risks, performing ongoing monitoring and audits, and developing and maintaining contingency plans for terminating relationships, etc. Any change that positively impacts the traditional ways of doing business has associated risks. While data is becoming the new oil, the stakes are high for both the outsourcers as well as the service providers. Eventually, it is both the bank and the service provider who share the risk, when it comes to the security of outsourcing operations, SLAs and data.

For more information about how NTT DATA can help you plan your cloud strategy, contact:

David Tyrrell
Country Manager
David.Tyrrell@nttdata.com

Siddharth Sharma
Business Consulting Director
Siddharth.Sharma12@nttdata.com

Sources

1. Kulkarni, Tatjana. "Why Lloyds bank is moving its core to the cloud in 2019." Bank Innovation. December 6, 2018. https://bankinnovation.net/2018/12/why-lloyds-bank-is-moving-its-core-to-the-cloud-in-2019/
2. Springfield, Cary. "The Impact of Cloud Computing on the Banking Sector." International Banker. September 3, 2018. https://internationalbanker.com/banking/the-impact-of-cloud-computing-on-the-banking-sector/