BOJ Reports & Research Papers

Financial System Report Annex Series

Financial System Report – Annex

Key Considerations for Risk Management in Using Cloud Services

Financial System and Bank Examination Department
Bank of Japan

March 2021

Computer System Risk and Business Continuity Group, Examination Planning Division,
Financial System and Bank Examination Department, Bank of Japan
csrbcm@boj.or.jp

Background

The Bank of Japan's *Financial System Report* has two main objectives: to assess the stability of Japan's financial system from a macroprudential perspective and to communicate with all relevant parties on any tasks and challenges ahead in order to ensure the system's stability.

The *Financial System Report* provides a comprehensive assessment of the financial system twice a year and is occasionally supplemented by the *Financial System Report Annex Series*, which provides more detailed analysis and insight on specific topics. In this paper, the Bank explains the key issues for risk management in using cloud services.

Abstract

Cloud services are on-demand services that use shared computer system resources (servers, middleware, storage, etc.) accessible via a network, and have become an integral part of many financial institutions' systems. With the digital transformation (DX) trends in recent years, cloud services are often seen as the dominant option for the use of new digital technologies; therefore, it is becoming necessary for the top management of financial institutions to have basic knowledge of cloud services. This has raised questions on how best to manage security and availability[1] in using cloud services.

In this paper, the Bank of Japan summarizes the important issues that financial institutions need to address to dispel such concerns in the order of security management, availability management and resilience assurance, and vendor management. The Bank also provides explanations on cost control, the system development framework and securing human resources, and formulating cloud policies, in order to enjoy the expected benefits of cloud services. In the Appendix, the Bank compiles a list of control items and practices that address these important issues, based on information obtained in cooperation with financial institutions, cloud services providers, and others.

The Bank hopes this paper will help the top management of financial institutions and the stakeholders to maintain and improve their IT governance by increasing their awareness of cloud service and related risk management practices.

[1] Timely, reliable access to data and information services for authorized users.

Contents

I. Introduction

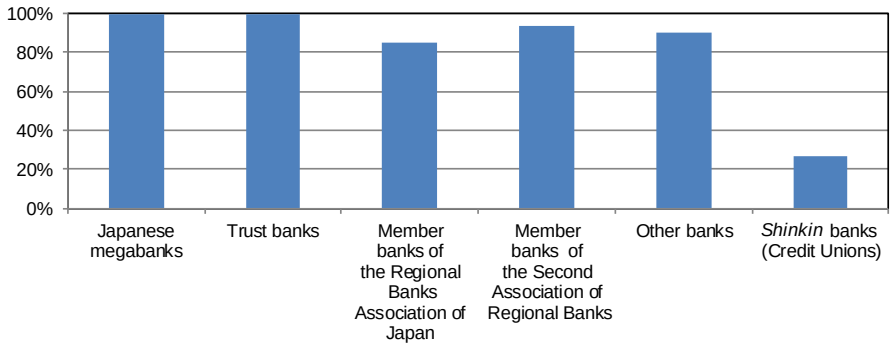
Cloud services are on-demand services that use shared computer system resources (servers, middleware, storage, etc.) accessible via a network.[2] Compared to the prevalent form of installing and managing computing resources by themselves (on premises), cloud services are advantageous in the following respects: a shorter installation period, reduction of operational and management burdens, cost reduction, and prompt adoption of emerging technologies (Figure 1).

Figure 1: Expected benefits of cloud services

Benefit	Specifics
Shorter installation period	Computer system resources can be deployed quickly and easily.
Reduction of operational and management burdens	Some of the burdens from operating and managing hardware, operating systems (OSs), and applications can be reduced by allowing them to be managed by cloud service providers.
Cost reduction	System costs can be reduced through economies of scale by sharing computer system resources, flexibly procuring computer system resources, and reducing system retirement costs.
Scalability and flexibility	Flexibility of use, such as developing a small system and then scaling resources as the number of users increases.
Use of emerging technologies	Emerging technologies (e.g., AI and machine learning) provided by cloud service providers can be used.
Improved security	Advanced security measures provided by cloud service providers can be used.

According to the results of a survey conducted by the Center for Financial Industry Information Systems (FISC), the use of cloud computing at Japanese financial institutions was 100 percent for Japanese megabanks, and 80 to 90 percent for regional banks (Figure 2). It could be said that cloud computing has become an indispensable service for many Japanese financial institutions in building their systems. The Japanese government proposed the "Cloud-By-Default Principle,"[3] which is a guideline to prioritize the use of cloud services in procuring information systems, and has consequently raised the awareness of cloud services significantly.

Figure 2: Use of cloud services



Source: The Center for Financial Industry Information Systems "Fiscal 2019 Financial Institutions Survey"

[2] Cloud computing has been defined by the U.S. National Institute of Standards and Technology (NIST) as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal effort or vendor interaction.

[3] In the "Basic Policy on the Use of Cloud Services in Government Information Systems" (decided by the Liaison Conference of Chief Information Officers [CIOs] of each ministry on June 7, 2018), the government adopted the principle of using cloud services as the first choice when developing government information systems.

Consistent with the digital transformation (DX) trends in recent years, Japanese financial institutions are carrying out business reforms to cope with the low profitability of domestic deposit and loan operations. In this situation, there is a growing trend for Japanese financial institutions to use new digital technologies, among which cloud services are often considered as a reliable option. Therefore, the top management of financial institutions, even if they are not in charge of IT, need to have basic knowledge of cloud services to improve and innovate their business.

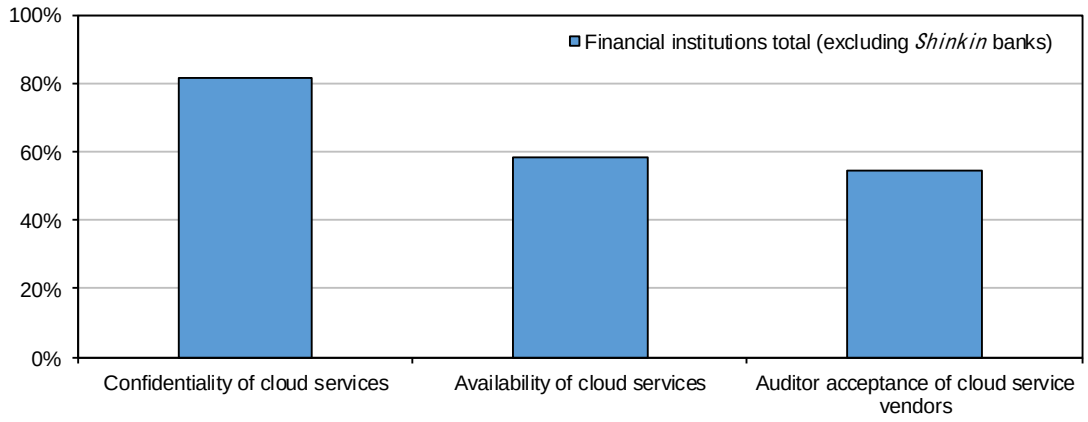
In this paper, the Bank of Japan first describes the features of cloud services, which underlie security and other concerns that are often expressed by the top management of financial institutions. The Bank then outlines key issues that the top management should address in order to dispel such concerns, namely, security management, availability[4] management and resilience assurance, and vendor management. Lastly, in order to reap the benefits expected from cloud services, such as cost reduction and the use of emerging technologies, the Bank explains about cost control, the system development framework and securing human resources, and formulating cloud policies.

[4] Timely, reliable access to data and information services for authorized users.

II. Features of cloud services and concerns raised by financial institutions

According to the results of the *Fiscal 2019 Financial Institutions Survey* released by FISC, more than 80 percent of financial institutions[5] were concerned about the "confidentiality of cloud services" (access control, crypto management, etc.), and more than 50 percent of those were concerned about the "availability of cloud services" (uptime rate, mean time to recovery, etc.) and "auditor acceptance by cloud service vendors" (Figure 3). Financial institutions' concerns arise from the features of cloud services described in the following sections.

Figure 3: Particular concern by financial institutions



Source: The Center for Financial Industry Information Systems "Fiscal 2019 Financial Institutions Survey"

Use of cloud services via a network, and confidentiality

Cloud services are on-demand services in which computer system resources can be used via networks including the internet. Cloud service users are often directly responsible for setting up network access control to limit access to their stored data and to ensure security. Therefore, if a user misconfigures the access control, there is a risk of unauthorized access to confidential data being made through a network, which could have a significant impact. This feature has led to financial institutions being concerned regarding confidentiality when using cloud services.

Shared computing resources and availability

One of the reasons for system outages is hardware and OS maintenance. Since cloud services share computer system resources with other users, it is often difficult for financial institutions to control the timing of system maintenance, unlike on-premises systems, for which they can adjust the timing in advance. These aspects of the situation have led to financial institutions being concerned regarding the availability of cloud services.

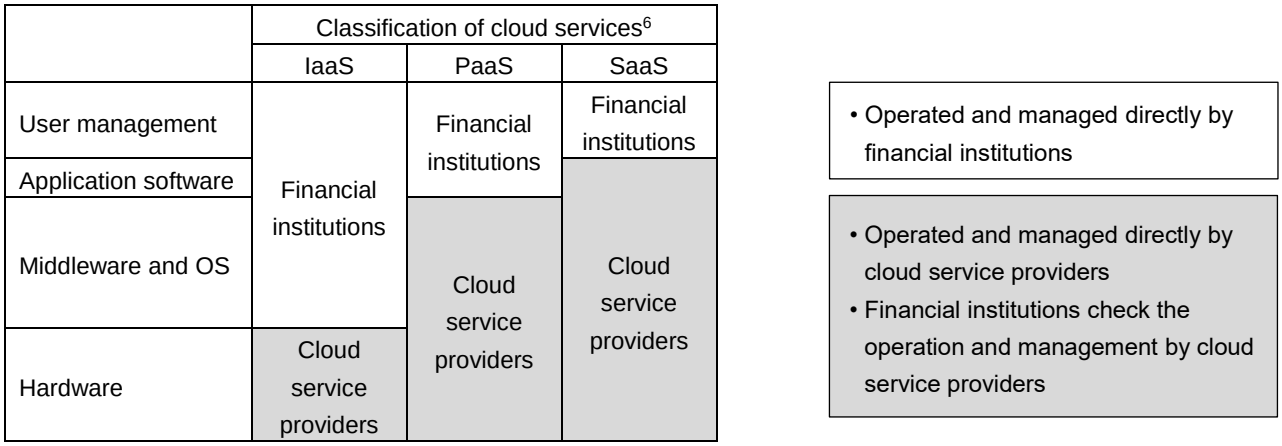
Shared responsibility and vendor management

Based on the framework called the shared responsibility model, the operation and management of systems on cloud services are shared between customers (i.e., financial institutions) and cloud service providers. Financial institutions are responsible for managing information stored in clouds that forms the basis of financial operations, as well as the process of handling that information,

[5] Excluding *Shinkin* banks (many of whom do not use cloud services).

even if a cloud service provider operates and manages other aspects of the system (Figure 4). Therefore, financial institutions are required to ensure the necessary control level under the framework of vendor management in order to ensure the wing-to-wing risk management of the entire process.

Figure 4: Coverage of operations and management by financial institutions and cloud service providers under a shared responsibility model



However, when conducting audits as part of vendor management, there are cases where conventional auditing methods are not applicable. These are cases where financial institutions cannot locate their exact computing resources within the public cloud environment. This aspect of the situation has led to financial institutions being concerned regarding their auditor's acceptance of cloud service vendors.

[6] Cloud services can be broadly classified into three types based on the provided services.
IaaS: Providing basic computing infrastructure
PaaS: Providing execution environments for applications
SaaS: Providing application functionality

III. Key considerations in risk management for cloud services[7]

A. Security management

The requirements for security management of cloud services are basically the same as those for on-premises systems. Specifically, financial institutions are required to set appropriate access control over applications and data, according to the level of confidentiality of the data, to ensure network security including access control, to apply security patches,[8] and to mitigate the risk of data breach by using technologies such as data encryption.

However, it should be noted that, under the shared responsibility model, some areas of cloud services are operated and controlled by cloud service providers and are assessed by financial institutions under the framework of vendor management, whereas other areas of cloud services are solely operated and controlled by financial institutions.

For example, in the case of IaaS, financial institutions are responsible for the operation and control of the entire system except the hardware. Therefore, those financial institutions' responsibilities for managing security are extensive, covering network configuration, adopting software security patches, etc. Such an obligation comes with the benefit of having a great degree of freedom in system design and operation. On the other hand, in the case of SaaS, the responsibilities of financial institutions are often limited to controlling and operating user identity aspects, such as managing access to applications.

Many of the past unauthorized access and data breaches involving cloud services occurred due to user misconfiguration of access controls of the system and/or data, as well as of network settings (Figure 5).[9] The problem of user misconfiguration tends to be more pronounced when setting up a system development environment or migrating from on-premises systems, as these are both environments that tend to be less manageable than a production environment. In the case of a massive customer data breach at a major U.S. financial institution in 2019, regulators pointed out that the financial institution failed to establish effective risk assessment processes in migrating its systems to cloud services, and also failed to establish appropriate risk management procedures for using cloud services, such as procedures for network configuration and data breach prevention.

Figure 5: Examples of incidents caused by inadequate security management over and measures for cloud services

	Incidents
Access control	• When migrating a system to a cloud service, confidential information was leaked because the information was accidentally made publicly accessible, so that anyone could access such information by simply entering a URL. • Improper authorization of access allowed a brute-force attack to gain access to all information assets in a cloud service, which were subsequently deleted. This attack terminated the business operations of the targeted financial institution.
Network security	• When setting up a system development environment in a cloud service, confidential data were leaked due to a brute-force attack. Confidential data

[7] Description in this chapter is made as generic as possible, not depending on the classification of the cloud service (IaaS, PaaS, and SaaS).
[8] Patches provided to resolve information security issues (vulnerabilities) in OS and software.
[9] U.S. National Security Agency, "Mitigating Cloud Vulnerabilities," January 2020, https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF.

	temporarily stored for testing were not deleted and were publically accessible due to misconfiguration of access controls. • Due to misconfiguration caused by a lack of awareness about the initial configuration of the Web Application Firewall (WAF),[10] illicit instructions were given to a web server. Eventually, a vulnerability in a web application was exploited, and a large amount of data were leaked.
Applying security patches	• A database was accessible to other parties because security patches were not applied to the database management system. All data in the cloud service became unavailable due to a ransomware[11] attack.
Data breach countermeasures	• Sensitive customer information and passwords were stored without encryption, which resulted in extensive damage upon the leakage of both.

Therefore, the top management of financial institutions should appropriately supervise the cloud service providers' operation and control within the framework of vendor management. On that basis, financial institutions should control their security by themselves while paying sufficient attention to the points enumerated below. Especially, when deploying a new system development environment in a cloud service within a short period of time, as seen in the enhancement of work-from-home systems in response to the spread of COVID-19, attention should be paid so as not to cause misconfiguration of access control and/or the network. Financial institutions can use tools provided by cloud service providers or third-party diagnostic services when there are difficulties in checking the appropriateness of configurations by themselves.

1. Access control

To prevent unauthorized access, it is necessary to minimize the number of people that can access systems and data, and to minimize the range of systems and data that can be accessed. As a means of access control, it is also effective to use multi-factor authentication[12] and other methods to strengthen authentication. This is particularly true for the management console,[13] which can set access rights to cloud services and can start and shut down the services. Financial institutions must rigorously supervise the management console, as they operate and control it.

2. Network security

In order to prevent unauthorized access from the internet, it is necessary to minimize network access and open ports via network access controls and to appropriately configure network settings, depending on the cloud service that is being used. Furthermore, in the case of handling highly sensitive data via the internet, data protection using encryption technologies such as virtual private networks (VPNs)[14] is also required.

[10] Software or hardware that protects web applications from cyberattacks that exploit web application vulnerabilities.
[11] A type of computer virus. Once infected, data are encrypted and a ransom request to allow decryption is sent. The word combines the words "ransom" and "software".
[12] A method of verifying a person's identity by combining multiple factors of authentication, such as memorized information (e.g., passwords), possessed information (e.g., IC cards), and biometric information (e.g., fingerprints).
[13] Management features that allow users to freely adjust cloud service settings, such as adding/removing virtual machines, user management, and network settings.
[14] A virtual private network which is developed by using encryption and other technologies.

3. Gathering information on cyberattacks and countermeasures

With regard to the fields where financial institutions are directly responsible for operation and control, they should gather information on cyberattacks against cloud services and vulnerabilities of cloud-related products; they also need to appropriately apply security patches (i.e., OS, software, and/or VPN products) in a timely manner, and to review their settings for the cloud service. It is also worthwhile to undergo periodic security assessments of potential risks and vulnerabilities.

B. Availability management and resilience assurance

With respect to availability management, it is important to take into account each business's tolerance of system downtime. For example, in the case of a system that requires very high availability, such as a core banking system, the required level of availability may be ensured by redundant configuration using multiple data centers (zones[15]), or by signing a special support contract with a cloud service provider. Meanwhile, in the case of a development environment or a system that requires less availability, a lower level of system availability can be determined according to the requirements of that business type.

Meanwhile, notifications related to cloud service maintenance are usually provided on the cloud service provider's website or management console. Even if a service disruption is caused by a cloud service provider, usually there is no individual notification. Therefore, financial institutions must be proactive about obtaining such notifications by periodically checking the websites and management consoles of their cloud service providers. They should check the impact of cloud service disruptions on their systems and take the necessary actions.

It is also important for financial institutions to ensure resilience[16] in the event of a cloud service disruption.

C. Vendor management

Under the shared responsibility model, financial institutions must ensure, using a vendor management framework, that the scope of operation and control of the cloud service providers is sufficient for the financial institutions to conduct their businesses.

In managing vendors (cloud service providers), risk control issues do not greatly differ from those in ordinary vendor management (for on-premises systems) such as the selection of a provider, the contract, and confirmation of operational status. However, there are also risk control issues to be kept in mind that are unique to cloud service providers, such as the frequent revisions of terms and conditions and service levels, as well as the method of confirming operational status. It is therefore important for financial institutions to manage their use of cloud services while taking into account risk characteristics particular to those services.

It is also important for financial institutions to confirm that the operational status of cloud service providers meets their required level in terms of security and facility. In order to confirm sufficiency of the operational status, users (financial institutions) need a means of confirmation, such as an

[15] A group of data centers that provide cloud computing and data storage.
[16] The ability to continue critical business operations in the event of a system service disruption, natural disaster, terrorism, cyberattack, etc.

audit of control target cloud bases.[17] To confirm the operational status of a cloud service provider, financial institutions may use SOC 2 reports[18] and audit reports made available by the cloud service provider. In addition, those institutions could choose to secure audit rights of the controlled target cloud bases in the case of serious incidents.

When confirming the status of security measures implemented in cloud services, financial institutions may use certifications, such as ISO/IEC 27017, ISMAP,[19] Cloud Information Security Promotion Alliance CS mark gold (Japan Information Security Audit Association), and FedRAMP (U.S.).

Furthermore, it is important for financial institutions to verify whether the vendors for their critical operations are using cloud services, and, where that is the case, to verify the vendor's risk control of those cloud services.

D. Cost control

One of the expected benefits of cloud services is cost reduction. However, migrating from on-premises systems to cloud services does not guarantee cost reduction; benefits can only be enjoyed through appropriate cost control.

First, it should be noted that cost reduction effects may vary greatly depending on the characteristics of the business operation being transferred to cloud services. For example, systems for business operations with large fluctuations in terms of volume are likely to successfully reduce costs by using cloud services. When running those systems, such as for risk calculation and settlement processing, on-premises systems require peak-time resources at all times to maintain availability, whereas cloud services could flexibly change the usage of computing resources and networks in accordance with the fluctuations in business volume. When running systems for business operations with small fluctuations on the other hand, the cost control effect is likely to be more limited.

The service level required for the system also influences the cost control effect. For example, if a system that requires high availability, such as a core banking system, is developed in a cloud service, it is necessary to ensure system redundancy or sign a special maintenance contract with the cloud service provider, which may increase costs.

Therefore, it is important to perform cost simulations in advance to grasp the expected cost reduction effect of migrating to cloud services. It is also important to have a framework for continuously managing the cost of using cloud services after migrating to such services, so that any unexpected cost rise can be detected and evaluated at an early stage.

---

[17] Control target cloud bases are defined by FISC in their Security Guidelines on Computer Systems for Financial Institutions as business bases having substantive control that provide access to data necessary for control over cloud service providers, including information processing centers. A cloud service provider's data center, operation center, head and branch offices, and other offices could be considered to be the control target cloud bases.

[18] A report on the status of internal control, such as the security and availability of contractors, which the audit firm has verified the effectiveness of in accordance with the international certification of external audits (System and Organization Control).

[19] To facilitate the deployment of cloud services, the Japanese government plans to launch a system (Information System Security Management and Assessment Program [ISMAP]) by the end of fiscal 2020 to list cloud service providers that have been confirmed to have implemented security measures based on the standards set by the government.

E. System development framework and securing human resources

Services provided by cloud service vendors often adopt the latest technologies, requiring frequent changes to the specifications of servers and databases, among other changes. It is therefore important for financial institutions using cloud services to enhance their system development framework so as to keep up with the speed of those changes.

In order to organize a system development framework so as to keep up with the latest technologies provided by cloud services and in order to maintain the functioning of the risk control framework, it is important to secure human resources with the appropriate skills; these human resources form the basis of the system development and risk control framework. Specifically, financial institutes should be concerned about securing human resources with knowledge of the service content and technology of the cloud services in use, and those with skills in controlling security and service configuration, as well as in system development using cloud services. This can be accomplished by training current human resources and/or acquiring the appropriate personnel from outside.

For services adopting emerging technologies such as AI and machine learning, cloud services provide an easy-to-use environment. For example, financial institutions can build new business models and make better market forecasts by combining the flexible scalability of computing resource and storage, which is a characteristic of cloud services, with the large amounts of data that can be stored in cloud services and by analyzing the data with the emerging technologies such as AI and machine learning provided in cloud services.

F. Formulating cloud policies

Sharing computer system resources through a network, such as the internet, is the feature of cloud services. Therefore, as mentioned in "Chapter II. Features of cloud services and concerns raised by financial institutions," cloud services have different risk characteristics compared to those of on-premises systems in terms of confidentiality and availability.

Therefore, in order to promote the use of cloud services, financial institutions need to predetermine the scope of the systems to be developed in cloud services from the perspective of confidentiality and availability. For each system, it is necessary to determine whether to migrate the system to cloud services based on the perceived benefits of cloud services compared to developing an on-premises system, such as the shortening of the installation period, the reduction of the burden of operation and control, and the cost reduction. In addition, as shown in "A. Security management" and "B. Availability management and resilience assurance," it is also necessary for financial institutions to establish a risk management framework that reflects the features of the cloud services.

IV. Conclusion

Responding to the environmental changes accompanied by the progress in digital transformation (DX) is a key challenge for financial institutions. In order to link these changes to revenue growth, an increasing number of financial institutions are aiming at expanding their use of cloud services.

When using cloud services, security is one of the main concerns. Nevertheless, as long as financial institutions can properly control the responsibilities within their scope and the responsibilities within the scope of the cloud service provider are properly managed within the framework of vendor management, the risk is not necessarily higher than that of on-premises systems. Also, risk management is not an overly burdensome task, once financial institutions understand the basics, such as the fact that services are available through a network and the need to clarify in advance the scopes of responsibility of the financial institution and the cloud service provider based on a contract.

The Appendix, "Necessary Management Items and Case Studies on Using Cloud Services," provides a chronological list of management items from the stage of considering cloud service adoption, along with the aforementioned points. The case studies in the Appendix are a compilation of information obtained in cooperation with financial institutions, providers, and others. The Bank expects the information to be helpful to the top management of financial institutions and the stakeholders in maintaining and improving IT governance by appropriately sharing awareness about using cloud services and managing risks, as well as by enhancing their cloud-related risk management framework.

The purpose of this paper is to encourage financial institutions to respond to environmental changes on a risk basis, specifically on the basis of the criticality of their operations and systems, rather than to adopt a uniform approach. This paper does not intend to preclude risk control by other means. The Bank of Japan will continue to support financial institutions' initiatives to enhance their risk management framework for cloud services through on-site examinations, monitoring, and seminars.