Navigating your way to the cloud

A practical guide for financial institutions in Japan

Microsoft

Contents

Introduction

As one of the most advanced markets for technology adoption in the Asia-Pacific region and, indeed, the world, Japan is already reaping the benefits of digital transformation in the financial services sector.

Powered by the government's 'World's Most Advanced IT Nation' vision, an increasingly supportive regulatory environment and a commitment to universal broadband access, financial institutions[1] across Japan are deploying digital platforms and services to re-imagine the customer experience, empower their workforce and optimize compliance and risk management.

Institutions across Japan are benefiting from the digital transformation of financial services—whether it is a large regional bank, which is using Microsoft Intune to manage smartphones and mobile apps, reducing staff downtime and improving productivity for mobile employees; a major insurance company, which is using Microsoft Azure to break new ground in InsurTech; or a large life insurance company, which is using CRM solutions powered by Dynamics 365 to enable real-time information sharing for its tenant sales activities.

To a large extent, this digital transformation is powered by cloud computing. Institutions are using cloud services to reduce capital expenditure; leverage elastic scalability to process vast datasets and manage changing customer demands; and enhance security and redundancy to better protect information and systems.

There is now widespread acceptance that financial institutions in Japan can adopt cloud services and continue to comply with their regulatory obligations.

To date, the pace of cloud adoption in Japan's financial services sector has been slower than in many other sectors, largely because of concerns as to whether or not the regulatory environment permits the use of cloud. These concerns typically focus on perceived barriers to the transfer of data outside of Japan and on the ability of cloud service providers to ensure a high level of security and privacy compliance in relation to sensitive information held by financial institutions. While in reality few (if any) regulatory barriers existed, many financial institutions took decisions not to access the benefits of cloud technologies. Interestingly, these perceptions and practices have started to change. While matters such as data privacy and security compliance remain at the core of the financial services regulatory environment in Japan and must be addressed as part of any technology adoption, there is now widespread acceptance that financial institutions in Japan can use cloud services and continue to comply with the necessary regulatory requirements.

At Microsoft, we are encouraged by these positive developments in Japan. Having partnered with financial institutions on many high-profile technology projects in the country and around the world, as well as participating in many discussions with financial services customers, regulators and industry bodies, we have developed substantial experience and a pool of practical resources to help financial institutions navigate the regulatory and risk landscape in the context of cloud deployments. Whether it is providing a map of our cloud services against the FISC Guidelines or making available Microsoft subject-matter experts to assist in all aspects of a cloud adoption, we understand that it is our responsibility as a cloud service provider to support financial institutions on their journey to the cloud.

Designed as a practical roadmap to help financial institutions take full advantage of the transformational benefits of cloud technologies, this paper is a further contribution by Microsoft to the digital transformation journey of Japan's financial services institutions.

We hope that you find this paper useful and we look forward to continuing the conversation as we seek to realize our mission of helping Japan's financial services institutions on their journey toward a bright digital future.

1 In this paper, we use the term 'financial institutions' broadly to refer to regulated financial institutions including banks and insurance companies.

Overview:

The four pillars of a successful cloud adoption

Based on Microsoft's experience of working with financial institutions in Japan and around the world, a successful cloud adoption rests on four pillars, as shown below.

Importantly, Microsoft recognizes that each of these pillars is inter-related and inter-dependent.

By focusing on these four pillars, financial institutions in Japan can move to the cloud in a way that addresses the key regulatory and compliance considerations.

Pillar 1: Understanding the regulatory landscape

A successful cloud adoption begins by understanding the regulatory landscape applicable to the use of the technology. We set out below details of the regulatory environment in Japan and address some of the common misconceptions, with the goal of making the entire process more streamlined for financial institutions.

Are cloud services permitted?

Yes.

One of the most common misconceptions regarding cloud adoption in Japan is that there are regulatory barriers or restrictions on the use of cloud services for certain categories of information or for certain systems. This is not the case. Provided that the right safeguards are in place, financial institutions in Japan can use cloud services, including public cloud services, across a full spectrum of operations.

Who are the relevant regulators and authorities?

- The Financial Services Agency **(FSA)**
- The Center for Financial Industry Information Systems **(FISC)**
- The Personal Information Protection Commission **(PPC)**

What regulations and guidance are relevant?

The key regulations and guidance include the following:

- Act on the Protection of Personal Information (Amended in 2015) **(PIPA)**
- Guidelines on the Personal Information Protection Act **(PIPA Guidelines)**
- Guidelines for Personal Information Protection in the Financial Field
- Q&As on Personal Information Protection in the Financial Field
- FISC Security Guidelines on Computer Systems (Revised Supplement to the 8th edition) **(FISC Guidelines)**

The FISC Guidelines include a number of specific issues for financial institutions to address. Please see **'Compliance with the FISC Guidelines'** below for more information.

Can financial institutions transfer data to cloud service providers?

Yes.

Transfers within Japan

There are no restrictions. As an option, Microsoft provides Japan-based data centers so that customers can choose to store certain categories of data within Japan.

Transfers outside of Japan

Although PIPA contains additional consent requirements where data is provided to a third party outside of Japan, these do not apply if the third party does not handle personal information. A Q&A document issued by the Personal Information Protection Commission provides that an exclusion to handling is achieved where the contract with such third party establishes: (i) there is no handling of the personal data; and (ii) there are proper access control systems in place.

Microsoft meets these requirements because the customer contract clearly establishes that:

(i) The customer, not Microsoft, owns the customer data;
(ii) Microsoft commits to use the data only for the purpose of providing the services to the customer, not for any secondary purpose; and
(iii) Microsoft cloud services have robust access control systems.

This means that customers can choose to transfer their data to Microsoft cloud services where they are provided outside of Japan without having to comply with the additional consent requirements.

Is regulatory approval required?	**No.**
Can public cloud services meet the necessary security and privacy standards?	**Yes.** When undertaking due diligence, many of our customers have found that Microsoft's public cloud services may offer an increased level of operational security, privacy, risk management and compliance relative to a private or on-premises solution.
Are financial institutions required to conduct on-site inspections of cloud service providers?	**No.** The FISC Guidelines do not require financial institutions to conduct on-site inspections of the cloud service provider. The financial institution is entitled to base its assessment on independent third-party audits made available by the services provider. Microsoft is audited as part of its compliance with the ISO/IEC 27001 and SSAE16 standards and it shares the results of these audits with its customers.
Are data deletion certificates required upon termination or expiry of the cloud services arrangement?	**No.** The FISC Guidelines do not require the issuance of a data deletion certificate. However, cloud service providers should commit to deleting data upon termination or expiry. Microsoft makes such a contractual commitment in its customer contracts.

How Microsoft helps

Overview

Close co-operation with regulators and financial institutions in relation to a number of successful cloud adoptions in Japan has given Microsoft an in-depth understanding of the relevant regulatory framework and process requirements. Issuing this paper is part of Microsoft's ongoing commitment to its financial services customers to help them navigate and comply with the regulatory framework as it applies to the use of cloud services.

Microsoft's team are on hand throughout the cloud procurement to help with any questions you may have along the way. You can also access the Microsoft Trust Center at microsoft.com/trust, which includes detailed security, privacy, and compliance information for all Microsoft cloud services.

Compliance with FISC Guidelines

FISC is a not-for-profit organization jointly established by the Japanese Ministry of Finance and several financial institutions in 1984 to promote security in banking computer systems in Japan. Some 700 corporations in Japan are supporting members, and include major financial institutions, insurance and credit companies, securities firms, computer manufacturers, and telecommunications enterprises.

In collaboration with its member institutions, the Bank of Japan and the Financial Services Agency, FISC created guidelines for the security of banking information systems. These include basic auditing standards for computer system controls, contingency planning in the event of a disaster, and the development of security policies and standards encompassed in more than 300 controls.

Although the application of these guidelines in a cloud computing environment is subject to its use scenarios, most financial institutions in Japan that implement cloud services have built information systems that satisfy these security standards, and it can be very difficult to justify diverging from them. The latest guidelines, Version 8 Supplemental Revised, issued in 2015, added two revisions relating to (a) the use of cloud services by financial institutions and (b) countermeasures against cyberattack.

Microsoft has engaged outside assessors to validate that Microsoft Azure, Microsoft Office 365 and Microsoft Dynamics 365 meet the FISC Guidelines. To achieve this validation, Microsoft provided evidence of compliance in each of the following areas:

- Data center guidelines for buildings and computer rooms, power, air conditioning, data center, and facilities monitoring.
- Operational guidelines for organizations, training, access control, system development, and auditing.
- Technical guidelines for measures to improve the reliability of hardware and software, and for countermeasures against security risks including data protection, prevention against unauthorized use, threat detection, and disaster recovery.

Financial institutions can obtain a copy of the completed assessment framework **(FISC Security Reference)** by contacting their Microsoft account representative.

Pillar 2: Full, informed stakeholder involvement

In Microsoft's experience, a smooth cloud adoption depends on full, informed stakeholder involvement from the outset, with decisions being based on a complete understanding of the proposed cloud solution. A key part of this is a detailed understanding of the proposed technology solution. This is both good operational practice and a necessity for institutions to satisfy themselves that the cloud adoption meets the necessary regulatory requirements. Microsoft believes that it is the responsibility of the cloud service provider to provide detailed product and service information to help ensure that the key decision-makers have all of the materials they need to make an informed choice.

Build the core stakeholder team and develop the business case

A multi-disciplinary team should be put in place from day one.

The **technology** and **procurement** teams should take the lead in developing the business case, with a focus on the operational and commercial factors driving the decision to adopt cloud services.

The **legal, risk and compliance** teams should be involved in these discussions from the outset, to map the proposed solutions against legal and regulatory requirements and to build in the necessary time frames to engage with regulators. Many technology projects have been delayed by involving the legal, risk and compliance functions too late in the process.

The **board** and **senior management** of the financial institution will typically require early reassurance in general terms regarding the business need for the use of cloud services and that the oversight, review, reporting and response arrangements will be put in place with the cloud service provider.

Understand the technical solutions available

Any technology procurement project requires that all of the key decision-makers have a full understanding of the technology solution to be deployed.

This begins by ensuring that every member of the core team has a clear understanding of the proposed cloud service and deployment models. A range of options exists, including public, private, hybrid and community cloud. Given the operational and commercial benefits to customers, public cloud is increasingly seen as the preferred deployment model for most financial institutions.

Microsoft has prepared the following summary of the different types of cloud service and cloud deployment models to assist with the early scoping aspect of any cloud project.

Understand the technical solutions available (continued)

Cloud Computing, Cloud Services or **Cloud** means on-demand network access to a shared pool of configurable computing resources. In other words, cloud services provide FSIs with on-demand access, using a network connection, to information technology or software services, all of which a CSP configures to the needs of the FSI.

Service Models. There are three common delivery models for cloud services:

(i) Software as a Service (SaaS) where the cloud service provider makes available software applications to customers;
(ii) Platform as a Service (PaaS) where the cloud service provider provides a computing platform for customers to develop and run their own applications; and
(iii) Infrastructure as a Service (IaaS) where the cloud service provider delivers IT infrastructure e.g. storage space or computing power.

Deployment Models. There are four common deployment models for cloud services:

(i) **Public Cloud.** Infrastructure is owned and managed by the cloud service provider and located off customer premises. Although the data and services are protected from unauthorized access, the infrastructure is enjoyed by a variety of customers. Given the operational and commercial benefits to customers, public cloud is increasingly seen as the most common deployment model.
(ii) **Private Cloud.** Infrastructure is usually managed by the cloud service provider (but sometimes by the customer). The infrastructure is located either on customer premises or, more typically, on the cloud service provider's premises. The cloud services are available exclusively by the particular customer.
(iii) **Community Cloud** serves members of a community of customers with similar computing needs or requirements. The infrastructure may be owned and managed by members of the community or by a cloud service provider. The infrastructure is located either on customer premises or the cloud service provider's premises. The cloud services are available only to the community of customers.
(iv) **Hybrid Cloud** is a combination of two or more of Private Cloud, Public Cloud or Community Cloud.

Obtain detailed product and service information

Having understood the technical solutions at a high level, the financial institution should also obtain detailed product and service information from the cloud service provider. We expand on this in the next pillar, 'Partnering with the right cloud service provider'.

How Microsoft helps

Microsoft believes that digital transformation is a journey. Our expert team is on hand to support you throughout your cloud project, from the earliest stages of initial stakeholder engagement right through to the deployment and rollout of the solution.

The Microsoft cloud product range spans all cloud services and most deployment models and, with our Japan-based data centers and a transparent approach to data location, we provide cloud customers with the flexibility to decide how and where their data will be stored and processed. We have developed a range of materials, including online trust centers (see: microsoft.com/trust) and the FISC Security Reference described in Pillar 1, designed to ensure that you have access to all the information needed to make an informed decision.

Our subject-matter experts are available to meet with you and your core stakeholders to provide specific and detailed information on the technical, contractual and practical aspects of your proposed cloud project.

Pillar 3: Partnering with the right cloud service provider

Financial institutions need to carry out appropriate due diligence based on defined procedures to ensure that a cloud service provider can meet the operational security, risk management and compliance requirements. To ensure that they are getting a compliant solution, a financial institution should develop a set of due diligence and selection criteria mapped against the key regulatory requirements.

While a summary of all applicable compliance obligations is outside the scope of this paper and is dealt with in other papers, such as Microsoft's FISC Security Reference (described in Pillar 1), the table below summarizes what we believe are key cloud service provider selection criteria. This summary is based on the underlying regulations and guidance as well as our conversations with cloud customers. Financial institutions may wish to refer to these criteria as part of their cloud procurement.

Cloud Service Provider Reputation and Competence	Financial institutions will want to carefully consider the cloud service provider's reputation and track record in the financial services sector, not just in Japan but also around the world. This is important not only for complying with the necessary due diligence requirements but also for providing valuable insight into the cloud service provider's global dealings and standing. Financial institutions should make sure that the cloud service provider has the financial position and operational measures necessary to stand behind their contractual commitments.
Confidentiality, Privacy and Security Standards	Given the sensitive nature of information that is held by financial institutions, it goes without saying that the chosen cloud solution needs to be secure. The due diligence process should focus on ensuring that the cloud service provider has measures in place to help ensure compliance with the required confidentiality, privacy and security standards in Japan. These include: • Requirements under PIPA to ensure that organizational, personnel, physical and technical measures are taken to protect personal information; and • Specific requirements under the FISC Guidelines are met.
Confidentiality, Privacy and Security Standards continued	Amongst other matters: • The cloud service provider should have a system in place to report to the financial institution if there has been a security breach or system problem; • The cloud contract should include confidentiality obligations; and • The cloud service provider should help ensure security through measures such as physical security and crime prevention (e.g. prevention of physical intrusion); logical security (e.g. measures to protect against electronic intrusion); prevention of unauthorized use; protection against computer viruses; protection against fire, earthquakes and flooding; and the use of secure access and identification tools. Compliance with national and international security standards such as ISO/IEC 27001, ISO/IEC 27018, and the Cloud Security (CS) Gold Mark of Japan has become an industry standard in financial services. If cloud service providers are compliant with these standards then a financial institution can have a high level of comfort that they can comply with the necessary requirements in Japan.
Supervision, Monitoring and Control	Financial institutions will want to ensure that the cloud service provider has in place appropriate measures to help enable the financial institution and its regulators to supervise the cloud service provider. At a practical level, financial institutions will also want to consider: • If the cloud service provider is assessed by independent third parties and if it shares the results of these assessments with its customers; • If the cloud service provider delivers appropriate information and periodic reports concerning the cloud services; and • If the cloud service provider has a procedure in place to report any service problems to the financial institution. As outlined in Pillar 1, there is no regulatory requirement for a financial institution itself to conduct any on-site inspection of the cloud service provider.

Data Location and Transparency	It is important for financial institutions to check that the cloud service provider is transparent as to where data will be located. Financial institutions may also wish to check that the cloud service provider can configure the service to ensure that certain categories of data are stored within the Japan geography. See Pillar 1, above, for details of the regulatory considerations regarding data transfers.
Limits on Data Use	Cloud service providers should not use the financial institution's data for any purpose other than that which is necessary to provide the cloud service. The cloud service provider should therefore commit not to use customer data for any secondary purpose, such as advertising.
Data Segregation	There are no specific requirements concerning segregation of data under the regulations, which means that all cloud deployment models, including public cloud, are permitted. Financial institutions will want to ensure that whichever cloud deployment model is used, the cloud service provider has in place appropriate technical and logical measures to help ensure that the confidentiality and security of data is not compromised.
Resilience and Business Continuity	The resilience of financial institutions' systems is of utmost importance, given the nature of their operations. As such, Japan's regulations require that financial institutions have appropriate business continuity measures in place. It is therefore essential that the financial institution works with a cloud service provider that offers a high degree of availability and resilience; provides the financial institution with access to and control of its data; and has business continuity and disaster recovery plans in place and tests them regularly. This helps ensure that the use of third-party services does not threaten the continuity of the financial institution's operations. Provided that these measures are in place, financial institutions can use cloud services across the full spectrum of their operations.
Conditions on Subcontracting	There is little value in finding the right cloud service provider if that cloud service provider will simply subcontract all of its obligations to a third party that may not meet the necessary legal and regulatory requirements. Financial institutions should therefore: (i) Request visibility of a list of any subcontractors and ensure there is a mechanism for the cloud service provider to notify it of any updates to the list; (ii) Ensure that the cloud service provider takes overall responsibility for compliance; and (iii) Ensure that the cloud service provider only uses subcontractors that are subject to controls that are equivalent to those applied by the cloud service provider itself.
Conditions on Termination	While financial institutions will often look at cloud services as a long-term solution, they should be prepared for a scenario where the cloud services are terminated. Japanese regulations address this issue by requiring that the financial institution has the ability to terminate the cloud services and that the cloud service provider commits to delete data when the cloud services terminate.

How Microsoft helps

Microsoft understands that, wherever you are on your journey to the cloud, it is vital to work with a service provider that you can trust. Not all clouds are created equal—it is crucial to check the facts and know what you are getting.

Microsoft confirms its ability to meet all of the criteria specified above. Our understanding of the financial services industry, based on experience of working closely with financial institutions and industry stakeholders over a number of years, is market-leading. Microsoft has over 40 years of IT experience, including decades as a cloud service provider running some of the largest online services in the world, and a proven track record of successful cloud rollouts for financial institutions in Japan and globally. We are proud of being at the forefront when it comes to offering cloud services that can help financial institutions maintain compliance with applicable laws, regulations, and key international standards.

We build our cloud services based on the core principle of trust. We are committed to ensuring that your data stays secure, that it stays private and under your control. We are also committed to being transparent about our security, privacy, and compliance practices. We make sure you know how your data is stored, accessed, and secured, and that you can independently verify this.

We are also committed to reliability and choice. That is, our software and services are robust to help ensure you can access your data and services when you need to.

Microsoft invests heavily in compliance to meet multiple regulatory standards. We design and build services using a common set of controls, making it easier to achieve compliance across a range of regulations, even as they evolve. Our approach to security compliance includes test and audit phases, security analytics, risk management best practices, and security benchmark analysis. We've been able to maintain and expand a rich set of third-party certifications and attestations that you can point to in order to demonstrate compliance readiness to your customers, auditors, and regulators. These include the Cloud Security Gold Mark, ISO/IEC 27001, ISO/IEC 27018, SOC 1 and SOC 2. As part of our commitment to transparency, we share third-party verification results with our customers.

In addition, Microsoft's financial services compliance program, developed specifically for financial institutions, extends the compliance features of Microsoft Azure, Office 365, Dynamics and Intune to provide deeper, ongoing engagement with Microsoft, including:

- Access to additional information from Microsoft subject matter experts (SMEs);
- Access to additional compliance-related information developed by Microsoft over time;
- The opportunity for one-to-one discussions with Microsoft's third-party auditors;
- Participation in webcast walk-throughs of ISO and SSAE audit reports with Microsoft SMEs;
- The ability to view the Microsoft control framework for cloud services;
- The opportunity to recommend future additions to the audit scope of the cloud service; and
- Access to detailed reports of external audit penetration tests conducted on the cloud service.

You can access more detailed information about the robust confidentiality and security at the core of each Microsoft cloud service in the Microsoft Trust Center at microsoft.com/trust. And if you wish to assess Microsoft's solutions against the FISC Guidelines, please contact your Microsoft account representative, who can provide you with a copy of our FISC Security Reference, as described in Pillar 1, above.

Pillar 4: A compliant contract

Microsoft understands that assurances made in response to selection criteria are worth little if they are not backed up by appropriate contractual commitments. This is particularly important in Japan, where various underlying regulations and guidance specify terms for inclusion in the cloud contract.

The following terms are those that Microsoft believes to be important, based on the underlying regulations and our discussions with customers in Japan. Financial institutions will want to put in place a binding cloud contract that, as a minimum, includes these key terms. In practice, the cloud service provider should help by demonstrating how their cloud contract meets these requirements.

Privacy and Data Protection	The contract will need to contain appropriate requirements to enable the financial institution to meet its own primary obligations (e.g. ensure that all personal information is dealt with in accordance with applicable privacy and data protection laws).
Security and Data Breach Protocols	The contract should contain appropriate commitments from the cloud service provider to help ensure that information and data are kept secure. The cloud contract should also address what happens in the event of a data breach incident—including the applicable notification procedures.
Data Ownership	The financial institution's data should continue to be owned by the financial institution, not the cloud service provider.
Data Use	The contract should be clear that data will be used only for the purpose of providing the cloud services and not for secondary purposes, such as advertising.
Inspection, Monitoring and Control	The contract should include commitments from the service provider regarding inspection, monitoring and control of the services and associated reporting. Note that there is no requirement for the financial institution itself to have a right to conduct on-site inspections of the service provider and most financial institutions rely instead on the service provider to engage independent third parties to carry out verification and testing procedures and to share the results with their customers.
Availability	As a matter of good operational practice and to ensure requirements regarding business continuity and resilience are addressed, financial institutions will want to ensure that the cloud service provider makes binding commitments as to service availability, with specified remedies in the event of an unscheduled service disruption.
Business Continuity	Again, in the interests of ensuring underlying business continuity requirements are met, the contract should provide for a disaster recovery/business continuity plan together with appropriate testing processes.
Confidentiality	Financial institutions will want to ensure that the cloud service provider makes binding commitments regarding the confidentiality of information stored in the cloud service.
Termination and Exit	Financial institutions will want to have rights to terminate the cloud services in agreed circumstances and for information to be deleted by the cloud service provider.
Conditions on Subcontracting	While subcontracting is permitted, financial institutions will want to ensure that the cloud service provider takes responsibility for compliance and ensures that any subcontractors are subject to controls that are equivalent to those applied by the cloud service provider itself.

How Microsoft helps

The contractual terms for Microsoft's cloud services have been developed based on feedback from thousands of cloud customers across the most heavily regulated industries around the world, including customers in the financial services sector. Microsoft's expert team will be available throughout the contractual review process to answer any questions you have about how Microsoft's contractual terms for its cloud services provide confidence to cloud customers that they are complying with the applicable regulatory requirements and guidelines.

Case Studies

Putting it into practice

A large regional bank

A large regional bank wanted to enable a more mobile, productive workforce but it didn't have the necessary management tools to secure and monitor the smartphones used by its sales force. It adopted Microsoft Intune, a cloud-based service, to manage the smartphones and the mobile apps that the IT department delivers to sales representatives. Working with better managed phones reduced staff downtime and improved productivity for mobile employees who can deliver better service.

A financial services conglomerate

A major financial services conglomerate needed a solution to capture, share and make use of the the vast knowledge and experience of individuals and teams from across its organization. To address this issue, the financial services conglomerate introduced Microsoft Office 365 as a new communications and workplace productivity platform.

An insurance company

A major insurance company needed a 'big data' cloud solution to power its healthy lifestyle application, aimed at extending life expectancy, reducing medical expenditure and improving quality of life. The application needed to be available 24/7 via the internet and to have the flexibility to reflect customers' changing needs over time. It became clear that Microsoft's Azure public cloud was the solution best suited to the insurance company's requirements.

A life insurance company

When a major life insurance company wanted a solution to facilitate information sharing for its tenant sales activities, it had three requirements. The first was the ability to share information in real time. The second was the ability to handle details of building and tenant companies as well as sales information, and to cross-reference these. And the third was to provide ease of use that was equal to or better than that of the existing system. It eventually reached a decision in October 2014 to use the Microsoft Dynamics CRM platform.

More case studies

For more case studies, please visit
www.microsoft.com/ja-jp/casestudies/search.aspx

Using Office 365 to drive workforce productivity

Many financial institutions are looking to cloud services such as Office 365 to improve the productivity and effectiveness of an increasingly mobile workforce. With a single secure synchronized inbox across devices and powerful collaboration and communication tools, staff can work much more efficiently in teams. For financial institutions that have traditionally hosted their data on their own premises, cloud systems enable much greater opportunity for controlled access across locations such as on mobile, from home or at other branches or premises.

Regulatory considerations

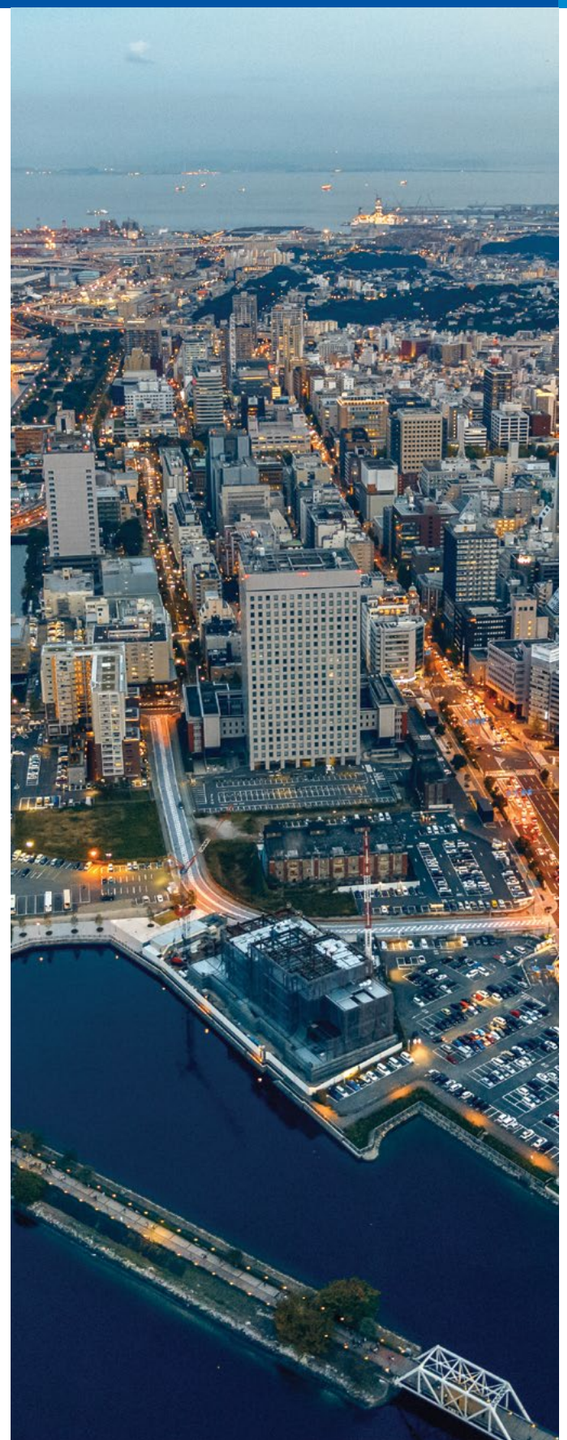
Just as they would for on-premises technology solutions, financial institutions must comply with general privacy law requirements.

Financial institutions must also ensure that data will be kept secure and confidential and, for this reason, Microsoft gives binding contractual commitments regarding the use, disclosure and security of such customer data.

Financial institutions will need to consider where data will be located. The key regulatory considerations are described in Pillar 1. With Microsoft cloud services, financial institutions have the flexibility to choose whether or not certain categories of data will be stored within Microsoft's data centers in Japan.

Steps you should take

1. Understand how your organization is using on-premises equivalents of Office 365 today.
   Is the solution secure? Does it provide the range of services and features available via Office 365? Put in place a multi-disciplinary team to assess where the institution stands today and what its objectives are.
2. Consider potential use cases for Office 365.
   What productivity and efficiency improvements could be achieved by using a cloud-based solution that enables access to documents, data and services across devices and geographic locations?
3. Consider how your institution wishes to configure the solution.
   Your Microsoft contact can help you with any questions regarding service configuration.
4. Assess the compliance of the solution against the FISC Guidelines using Microsoft's Security Reference.
   This is available from your Microsoft account representative.
5. Review the contractual offering for Microsoft Office 365.
   This is available from your Microsoft account representative.



An 'Advanced IT Nation' in Financial Services

Financial institutions in Japan have an unprecedented opportunity to take advantage of the full spectrum of cloud-driven technologies, powered by a supportive regulatory framework, excellent technical infrastructure and a growing range of compliant solutions to choose from.

Whether it is advanced data analytics to streamline operations and reduce costs, cloud-based productivity tools to enhance collaboration in a mobile-first workforce or digital platforms to reinvent the entire customer experience, the range of opportunities is broad and growing all the time.

At Microsoft, we believe that cloud technologies will play a crucial role in the future of financial services in Japan. We look forward to continuing our role at the forefront of this digital transformation, deploying trusted, responsible and inclusive cloud solutions for the benefit of financial institutions in Japan and their customers.

Microsoft

Find out more

Trust Center
microsoft.com/trustcenter

Navigating your way to the cloud
microsoft.com/en-sg/apac/trustedcloud

Service Trust Portal
aka.ms/trustportal

FISC Guidelines Overview
microsoft.com/en-us/TrustCenter/Compliance/FISC

Online Services Terms
microsoft.com/ja-jp/licensing/product-licensing/products.aspx

Financial Services Amendment
Contact your Microsoft Account Manager

Compliance program for regulated financial services customers
Contact your Microsoft Account Manager

Service Level Agreements
microsoft.com/ja-jp/licensing/product-licensing/products.aspx

SAFE Handbook
aka.ms/safehandbook