(Appendix)

March 2021

Necessary Management Items and Case Studies on Using Cloud Services[1]

[1] The purpose of this appendix is to encourage financial institutions to respond to environmental changes on a risk basis, based on the criticality of their operations and systems, rather than to take a uniform approach.

This appendix is organized to be as useful as a general resource as possible, regardless of the classification of the cloud services (IaaS, PaaS, etc.). Depending on the classification of cloud services, the scopes of responsivity of financial institutions and cloud service providers with regards to operation and control vary. However, 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, even if a cloud service provider operates and manages other aspects of the system. Therefore, financial institutions need 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.

Contents

1. Deployment of cloud services	1.1 Prerequisites for deployment	1
	1.2 Considerations for concluding contracts	2
	1.3 Formulation of financial institutions' internal risk management standards for using cloud services	3
2. Security management	2.1 Cooperation with cloud service providers based on a shared responsibility model	6
	2.2 Prevention of unauthorized access from external networks	7
	2.3 Prevention of unauthorized access, etc., including that from within the financial institution	8
	2.4 Data protection	9
	2.5 Ensuring the effectiveness of security management measures	
3. Availability	3.1 Operation management suitable for cloud services	11
	3.2 Ensuring system performance	12
	3.3 High availability system configuration	
4. Resilience	4.1 Ensuring resilience	13
5. Cost control	5.1 Understanding the cost structure and containing costs	15
6. System development framework and securing human resources	6.1 System development framework for cloud services	16
	6.2 Securing personnel for using cloud services	17
7. Vendor management	7.1 Vendor management: grasping the situation	18

Glossary	20

1. Deployment of cloud services[2]

Management Items	Case Studies	Related Standards			
		NIST	ISO	FISC	ISMAP
1.1 Prerequisites for deployment					
➢ Establish an appropriate framework for considering and managing cloud services.	• With the involvement of the management committee and the board of directors, each financial institution formulates its policy on the use of cloud services, as well as the measures required for conducting business operations and the risk management associated with deploying cloud services. • Financial institutions establish a cross-sectional organization that includes not only system-related departments but also risk management as well as procurement and contracts departments, etc. This organization discusses risk management and resolution of the business issues associated with the use of cloud services.	144-9.1	6.1	C20	—
➢ Evaluate confidentiality, availability, and economic rationality of the use of a cloud service for a target business or operation.	• When considering a system migration from an on-premises system to cloud services, financial institutions confirm the level of confidentiality based on the data being processed and the level of availability based on the requirement of the target business or operation, using a checklist. • Based on the fact that the choice of cloud service can make a significant difference in expenses, financial institutions compare expenses by using cost simulations and select the most appropriate service.	144-5.2	15.1.1 15.2	C20	—

[2] The standards shown in "Related Standards" are as follows.
NIST: the U.S. National Institute of Standards and Technology (NIST) "Special Publication 800-144" and "Special Publication 800-146," ISO: International Organization for Standardization (ISO) "ISO/IEC 27017," FISC: The Center for Financial Industry Information Systems (FISC) "FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions," ISMAP: "Information system Security Management and Assessment Program"
The abbreviations used in "Related Standards" are as follows; C: Control Guidelines, P: Practice Guidelines, A: Audit Guidelines.

Management Items	Case Studies	Related Standards			
		NIST	ISO	FISC	ISMAP
➢ Appropriately select a cloud service provider.	• In selecting a cloud service provider, financial institutions check the financial resilience and profitability, service quality, security management framework, support structure, vendor management framework, policy on anti-social elements exclusion, etc. • In selecting a cloud service provider, financial institutions focus on its ability to provide support, such as the provision of tools and information, when migrating an on-premises system.	144-5.2	4.3 18.1.1	C20	—
1.2 Considerations for concluding contracts					
➢ Ensure the appropriateness of the contents of contracts and service level agreements (SLAs).	• Financial institutions review contractual treatment regarding the following: ownership of data on cloud services, data protection, change or suspension of services, billing, outsourcing, providing internal and external audit results, dispute resolution, governing law, user's audit rights, and contract termination. • Financial institutions check SLAs to review the quality of the service (uptime, performance, etc.), fees, support period, and treatment to identify cases where the quality of service commitments, etc., are not being met. • Financial institutions confirm the offered compensation from cloud service providers in the event of a service outage, etc. If the amount of compensation is not sufficient to cover the expected amount of damage, financial institutions transfer the risk by obtaining insurance or other means. • When using a cloud service for critical operations, financial institutions include the terms in the contract such that the cloud service provider will support the transfer of the service to another	144-5.3 146-8.3.2	13.2.4 18.1.1	C21 C24	15.1.1 18.1

Management Items	Case Studies	Related Standards			
		NIST	ISO	FISC	ISMAP
	cloud service provider in the event that the original cloud service provider discontinues its service.				
➢ Make additional contractual arrangements when necessary	• Financial institutions clarify the range of impact of service outages, and supplement the terms in their contracts on advance notification of maintenance and on coordination during an outage window. • An agreement is put in place that the financial institution will be notified in advance about changes in the service specifications, features, or settings, which may affect the financial institution's businesses. • A contractual commitment is in place on the provision of logs during system service disruptions and security incidents based on confirmation by the financial institution of the types and retentions of logs that the cloud service provider has.	144-5.3	18.1.1	C21 C24	15.1.1 18.1
➢ Confirm laws and regulations, including foreign regulations if necessary	• If financial institutions' overseas branches use cloud services, they shall check the regulations in the countries in which the branches reside.	144-4.2 144-5.2	18.1	C21	15.1.1.16.B 18.1
1.3 Formulation of financial institutions' internal risk management standards for using cloud services					
➢ Establish risk management standards for the use of cloud services in line with well-recognized security standards, etc.	• Each financial institution formulates its own risk management standards while referring to the security standards of cloud services and operational and security case studies provided by the cloud service providers. <Examples of well-recognized security standards>	144-4.1	5.1.1 6.1.1 CLD-6.3.1	C1	—

Management Items	Case Studies	Related Standards			
		NIST	ISO	FISC	ISMAP
	Security Guidelines on Computer Systems for Financial Institutions by FISC, ISMAP, ISO/IEC 27017 and 27018, NIST SP800-144/146, FedRAMP (U.S.), Cloud Security Alliance Cloud Control Matrix (CSA CCM), Cloud Computing Information Assurance Framework by the European Union Agency for Cybersecurity (ENISA), “Benefits, risks and recommendations for information security” by ENISA, Center for Internet Security (CIS) Benchmarks, Cloud Information Security Promotion Alliance CS mark gold by Japan Information Security Audit Association				
➢ Conduct timely and appropriate reviews of the risk management standards.	• Financial institutions review their own risk management standards in the following ways. 1) Financial institutions keep a record of correspondence between the security standards referred to and their own risk management standards, and review their risk management standards as the security standards are revised. 2) Financial institutions use external audits and security vendors to identify changes in the security standards referred to. • Financial institutions consider whether to revise their own risk management standards based on changes to the services and technology of cloud services by using Service Organization Control (SOC) 2 reports and other security reports released by cloud service providers. • Financial institutions regularly analyze the causes of cloud service disruptions and security breaches to identify issues regarding their risk management standards and modify those standards accordingly.	144-4.1	12.1.2	C1	—

Management Items	Case Studies	Related Standards			
		NIST	ISO	FISC	ISMAP
➢ Prevent shadow IT in the cloud.	• Financial institutions prevent shadow IT in the cloud by adopting the following measures. 1) Using external services to visualize the usage of cloud services 2) Confirming the lists of utilized services submitted by cloud service providers 3) Making inquiries to the procurement and contracts department about the contract status with the cloud service provider	144-4.1	6.1.1 CLD-6.3.1	—	—

2. Security management

Management Items	Case Studies	Related Standards			
		NIST	ISO	FISC	ISMAP
2.1 Cooperation with cloud service providers based on a shared responsibility model					
➢ Promptly and appropriately confirm the separate responsibilities of the financial institution and the cloud service provider over operations and controls.	• Before the deployment of cloud services, financial institutions check service details, SLAs, and security reports released by the cloud service provider to understand the division of responsibility between themselves and the cloud service provider. • After the deployment of cloud services, financial institutions periodically check whether the scope of operations and controls of the cloud service provider has changed due to additional features, etc. • Financial institutions make inquiries to the cloud service provider about the entity responsible for operating and managing the container base operating system (OS), standard libraries, and so on, when there are unclear items regarding the entity.	144-4.1 146-Appendix A	6.1.1 CLD-6.3.1	C24	6.1.1.13.PB
➢ Cooperate with cloud service providers in preparation for service disruption.	• Financial institutions each establish their own internal communication structure in the event of service disruption or security breach, based on the notification service system of the cloud service provider. • Terms pertaining to the notification method in the event of service disruption or security breach are arranged in advance with the cloud service provider. • Given that cloud services require different computer forensic techniques than on-premises systems in the event of a security	144-5.2 146-8.2 146-8.4.4 146-Appendix A	6.1.1	C21 C23	4.9.2

Management Items	Case Studies	Related Standards			
		NIST	ISO	FISC	ISMAP
	breach, terms pertaining to forensic techniques are agreed to in advance with the cloud service provider. • Financial institutions each make sure that system clocks are accurate at both the financial institution and the cloud service provider.				
2.2 Prevention of unauthorized access from external networks					
➢ Ensure security in communication with external parties.	• For confidential data communication, financial institutions use leased lines, virtual private networks (VPNs), the Software Defined Perimeter (SDP) approach, etc. • When communicating with an external application service provider using application programming interfaces (APIs), the financial institution ensures that the authentication procedure is configured appropriately.	144-4.4 146-4.2	13	P4	13
➢ Restrict external access routes and remote access terminals.	• Financial institutions restrict access routes by using firewalls. • The access to the management console in a cloud service is limited to the Internet protocol (IP) address on an allow list. • Financial institutions ensure the security of terminals for cloud service access by using protective features, such as anti-virus software, data loss prevention solutions, and fraud prevention tools (login management, automatic logoff, etc.)	144-4.4 146-8.5.5	12.2 13	P14 P15	9.1.2
➢ Take measures to detect and defend against abnormal access from external parties.	• Financial institutions periodically review logs for anomalies. • Financial institutions monitor for anomalies when communicating with external application service providers, by checking indicators, such as call frequency, delay, errors, etc.	144-4.4 146-8.2.1	13.1.1	P14 P16	13

Management Items	Case Studies	Related Standards			
		NIST	ISO	FISC	ISMAP
	• Financial institutions use web application firewalls (WAFs) to prevent attacks, such as those that exploit web application vulnerabilities.				
2.3 Prevention of unauthorized access, etc., including that from within the financial institution					
➢ Properly manage access control.	• Financial institutions grant access to management consoles, virtual machines, container environments, and data, in accordance with the principle of least privilege. Also, they establish a framework for the regular inventory of identifiers (IDs), including the prompt deletion of IDs that are no longer needed. • Regarding the controls over the management consoles, financial institutions deploy tools to limit access duration (just-in-time access method), and deploy services to compare actual operations with pre-registered tasks in order to detect any fraudulent use.	146-9.3	9.2 9.4.1	P25 P27	9.2
➢ Prevent unauthorized use.	• Financial institutions reduce the risk of fraudulent use by multi-factor authentication. • Financial institutions allocate a virtual private area within their cloud services to prevent unauthorized use by other cloud service users.	144-4.5	9.4	P9	9.4
➢ Detect unauthorized use by verifying logs, etc.	• Financial institutions regularly review access logs to detect fraudulent use. • Financial institutions monitor the management console operation log in real time and obtain an operation trail by recording the operation log, operation screen, etc.	144-4.9 146-9.1	12.4	P16	12.4

Management Items	Case Studies	Related Standards			
		NIST	ISO	FISC	ISMAP
2.4 Data protection					
➢ Locate and encrypt data, etc.	• Financial institutions organize and regularly check data location, data confidentiality, and the status of access control on a region-by-region basis, including data held in containers, by using ledgers and other tools. • Financial institutions encrypt highly confidential data with appropriate strength. Also, they manage the entire lifecycle of encryption keys, from generation, to use, to disposal.	144-4.7 146-8.1.4 146-8.5.2	8 10	P3 P4 C24	8 10
2.5 Ensuring the effectiveness of security management measures					
➢ Implement cyberattack protection based on the characteristics of cloud services.	• Financial institutions continuously collect information on cyberattacks through financial information sharing and analysis centers (ISACs), cloud service providers' services, etc., and implement countermeasures. • Financial institutions use analyses released by the CSA on security breaches, and verify whether they themselves could address the security risks shown in the analyses.	144-4.4	12.6	C4 C5	12.6
➢ Make sure security measures are effective.	• Financial institutions regularly conduct vulnerability assessments, perform penetration testing, and have security vendors conduct assessments, etc. • When using security tools, such as WAF in the cloud, financial institutions check whether the configurations are effective to ensure security. • Financial institutions deploy mechanisms to automatically detect security-related configuration changes and to recover when a problem is found in the configuration.	144-2.1	12.6	C5	12.6

Management Items		Case Studies	Related Standards			
			NIST	ISO	FISC	ISMAP
		• Financial institutions use cloud service providers' tools and other tools to monitor for fraudulent operations that could affect their security measures.				

3. Availability

Management Items	Case Studies	Related Standards			
		NIST	ISO	FISC	ISMAP
3.1 Operation management suitable for cloud services					
➢ Collect logs and properly monitor.	• Financial institutions collect and monitor logs necessary for managing cloud service operations by utilizing managed services, cloud service providers' tools, and third-party software. • Financial institutions use a unified log management tool that allows them to monitor cloud services and on-premises logs together. • Financial institutions check the time zones of the log entries from cloud service providers.	144-4.9	12.4	—	12.4
➢ Grasp any changes or discontinuation of cloud services promptly.	• Financial institutions regularly check for announcements on changes or discontinuation of cloud services. • Financial institutions regularly meet with cloud service providers to obtain information on service changes, etc., in a timely fashion. • To address the possible discontinuation of cloud services, financial institutions conclude contracts with providers to receive early advance notification. • Regarding the use of cloud services in critical business operations, financial institutions utilize managed services and conclude special contracts with cloud service providers so that they receive prompt notification of any changes in cloud service specifications, features, and configurations, which may affect their critical businesses operations, and thus can respond quickly.	144-3.1 144-4.3	15.2.2	C21	15.2.2

Management Items	Case Studies	Related Standards			
		NIST	ISO	FISC	ISMAP
3.2 Ensuring system performance					
➢ Grasp the system performance required for the business.	• As with on-premises systems, financial institutions estimate the system performance required for cloud services based on workload, business processes, and system configuration.	144-4.4 144-5.3	12.1.3	P47	12.1.3
➢ Monitor system utilization, etc.	• Utilizing tools, such as those provided by cloud service providers, financial institutions collectively monitor their computer resource utilizations, etc.	144-4.3 144-5.3	12.1.3	P47	12.1.3
➢ Enhance system performance timely and appropriately.	• Financial institutions know the scalability and quotas of each cloud service, and raise the system quotas appropriately and in a timely manner as the required system performance changes.	—	12.1.3	P47	12.1.3
3.3 High availability system configuration					
➢ Ensure system redundancy.	• Financial institutions ensure system redundancy through a combination of zones and regions, so that service outages resulting from maintenance or service disruption are less likely to occur.	—	17.2	—	17.2

4. Resilience

Management Items	Case Studies	Related Standards			
		NIST	ISO	FISC	ISMAP
4.1 Ensuring resilience					
➢ Prepare response procedures in case of service outages.	• Financial institutions make use of the service health notifications provided by cloud service providers, and have a framework to detect and understand the details of service disruptions in a timely manner. • Financial institutions determine with their cloud service providers the support service level at times of service disruption, depending on the criticality of their business and the level of availability required. • For systems in cloud services, financial institutions define roles with their system development contractors, such as identification of the impact on the system and the recovery operations (including recurrence prevention) in the event of a system failure caused by a cloud service outage. • During the pilot operation phase, financial institutions organize procedures of service disruption response, and they establish a smooth transition to their use. • Financial institutions ensure the effectiveness of their service disruption response procedures by regularly conducting drills.	144-4.8	15.1.1	P24 P70 P71	—
➢ Organize critical business continuity plans in case of disasters, etc.	• For critical business operations, financial institutions prepare business continuity plans assuming that cloud service data centers have been damaged due to disasters. • In order to secure especially critical data, i.e., data that are essential for organizational or operational continuity, financial	144-4.8	17	P73 P74	17

Management Items		Case Studies
		institutions store backups as needed in their own data center or in a cloud service of a different provider.

Related Standards			
NIST	ISO	FISC	ISMAP

5. Cost control

Management Items	Case Studies	Related Standards			
		NIST	ISO	FISC	ISMAP
5.1 Understanding the cost structure and containing costs					
➢ Understand the cost structure of cloud services properly.	• Given that cloud services often adopt a pay-per-use system, financial institutions regularly identify the risk of expense expansion by simulating cost changes resulting from fluctuations in business volumes. • Financial institutions set alert levels and limits on cloud service expenses so as to prevent unexpected increases of expenses or to detect such increases promptly.	144-4.1	12.1.3	—	—
➢ Implement cost containment measures.	• Financial institutions contain costs by adjusting computer resources (central processing units [CPUs], storage service, etc.) according to the business volume, or by ending their contracts for cloud services that they are not using. • Financial institutions contain costs by choosing services that are aligned with their usage patterns, such as using low-cost services with low availability in a test environment or taking advantage of long-term fixed contract discounts for services that are expected to be used for a long time.	146-8.3	—	—	—

6. System development framework and securing human resources

Management Items	Case Studies	Related Standards			
		NIST	ISO	FISC	ISMAP
6.1 System development framework for cloud services					
➢ Understand changes in the specifications of cloud services.	• Financial institutions actively monitor information, such as specification changes to cloud services documented by cloud service providers on their web sites. • Financial institutions map their operations to the cloud services used for each operation so that they can smoothly check the impact and respond to specification changes, etc. • Financial institutions reconfirm the specifications in SLAs and reports on the cloud services when services are integrated by third-party acquisitions, etc., because those cloud services may have different specifications from other existing cloud services.	144-5.3	12.1.2	—	12.1.2
➢ Enhance system development procedures based on the characteristics of cloud computing.	• Financial institutions review their standard system development procedures based on virtualization technology, scalability, infrastructure configuration, such as region, zone, etc., using case studies available from cloud service providers. • To keep up with the pace of change in cloud computing-related technologies and services, financial institutions promote automation of a sequence of operations, from development, to testing, to release, and integrate system development and operations (DevOps). • When using microservices to improve system development efficiency and maintainability through loosely coupled systems, financial institutions design their systems taking into account the disadvantages of the microservices, such as performance	144-4.1 144-4.4	14.2	P75	14.2

Management Items	Case Studies	Related Standards			
		NIST	ISO	FISC	ISMAP
	degradation due to communication congestion between microservices, increased points of failure, and increased operational complexity, due to complexity of configuration.				
6.2 Securing personnel for using cloud services					
➢ Train and secure personnel with knowledge on cloud services.	• Financial institutions develop a skill-set plan and train personnel with expertise in cloud services through the following measures. 1) Obtaining certifications related to cloud services and participating in events and corporate training held by cloud service providers 2) Accepting personnel from information technology (IT) vendors and external consultants who have expertise in virtualization technologies and infrastructure configuration, such as regions and zones 3) Encouraging system developers to acquire expertise in cloud services • Financial institutions have their internal audit staff acquire technical and specific risk management skills related to cloud services. • Financial institutions present their approaches to cloud services at external seminars and in speeches to show publicly that they provide opportunities for personnel with expertise in cloud services to build a successful career.	144-3.2 144-5.1	7.2.2	C24	—

7. Vendor management

Management Items	Case Studies	Related Standards			
		NIST	ISO	FISC	ISMAP
7.1 Vendor management: grasping the situation					
➢ Grasp cloud service providers' vendor management.	• Financial institutions regularly review SOC 2 reports, audit reports, and reports on services and security of cloud service providers to monitor their security management, operational controls, and vendor management. If there are issues to be addressed, financial institutions prompt the cloud service providers to make improvements. • Financial institutions use SOC 2 reports and other reports to check the operations of cloud service providers when they reuse or dispose of hardware, etc.	144-4.3	15	A1	15
➢ Enable an on-site visit to cloud service providers to confirm their execution of a risk management framework.	• Financial institutions identify the control target cloud bases[3] and secure their audit rights to these locations in case of a major security breach or system failure. • Financial institutions are prepared at all times to respond to requests by supervisory authorities for cooperation, such as Japan Financial Services Agency (FSA) inspections and Bank of Japan on-site examinations.	144-5.2 144-5.3	12.7	C21	4.9
➢ Appropriately monitor subcontractors that use cloud services (hereinafter referred to as simply "subcontractors").	• Financial institutions review cloud service provider's criteria and terms for selecting subcontractors. • Financial institutions obtain a list of subcontractors and verify if there are any inappropriate subcontractors.	144-4.3	15.1.3	C21 C23	—

[3] 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.

Management Items	Case Studies	Related Standards			
		NIST	ISO	FISC	ISMAP
	• Financial institutions monitor vendor management of subcontractors by SOC 2 reports, audit reports, etc.				
➢ Appropriately control vendors using cloud services.	• In regular assessments of vendors involved in critical business processes, financial institutions include a question on the use of cloud services. • Financial institutions create a checklist of important control items for cloud services and use the checklist to regularly inspect the use of cloud services by their vendors.	—	15.1.3	—	—

Glossary

Term	Description
CIS Benchmarks	Guidelines published by the Center for Internet Security (CIS) in the United States with examples of good security management.
Cloud computing	A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Cloud services	On-demand services that use shared computer resources accessible via a network.
Computer forensics	The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.
Computing resources	Computing services, such as network, server, storage, and application services.
Container	An application virtualization environment in which the OS kernel securely runs multiple isolated applications and libraries for various operating systems.
CSA CCM	Abbreviation for Cloud Security Alliance Cloud Control Matrix. A cloud security management standard published by the Cloud Security Alliance, a private organization based in the United States.
DevOps	A system development scheme that allows system development and operation teams to work together so as to automatically and swiftly move from system development to operation.
Cloud Computing Information Assurance Framework	A framework for cloud service security released in November 2009 by the European Union Agency for Cybersecurity (ENISA).
ISMAP	An abbreviation for Information system Security Management and Assessment Program. A program, with the perspective of facilitating deployment of cloud services, to list cloud services that are confirmed to have implemented security measures based on the standards set by the Japanese government.
ISO/IEC 27017 and 27018	Guidelines published by the International Organization for Standardization (ISO) from 2014 to 2015 that provide measurements for evaluating whether cloud services meet the prevalent information security standards.
Loosely coupled systems	Systems in a state such that connections between system components and their dependencies on each other are weak, and there is a high degree of flexibility and mobility in system changes.

Term	Description
Managed services	Outsourcing services that undertake system operation, monitoring, troubleshooting, maintenance, etc.
Management console	An administrative feature that can freely control the settings of a cloud service, such as adding or removing virtual machines, user management, and network settings.
Microservices	Software subdivided by function. Systems can be easily modified and expanded by building a system, that is, by combining disaggregated microservices.
NIST SP800-144	A guideline, which outlines issues and considerations related to public cloud security, published in 2011 by the U.S. National Institute of Standards and Technology (NIST). NIST supports the integration of standards related to industrial technology, etc.
NIST SP800-146	A guideline published by NIST in 2012 that explains cloud services from a technical perspective and provides recommendations for information technology decision makers.
Operational resilience	The ability to continue critical business operations in the event of a system failure, natural disaster, terrorism, cyberattack, etc.
Principle of least privilege	The principle to minimize the privileges to access information assets that people, processes, programs, etc., have.
Region	The area/region where the cloud service is provided and data are stored; this is specified by the cloud service provider when users start using the cloud service.
SDP	An abbreviation for Software Defined Perimeter. A mechanism to increase the security of an external connection by having an intermediary controller other than the destination perform authentication.
SLA	An abbreviation for Service Level Agreement. An agreement or Memorandum of Understanding (MOU) between a service provider and a user regarding the content, scope, and quality of services to be provided.
SOC 2 report	SOC stands for Service Organization Control. This is a validated report that assesses the effectiveness of internal controls over information systems, such as security and availability of service organizations (i.e., contractors). The assessment is made by audit firms in accordance with the international audit standards (SOC).
Standard library	A set of files that collects and consolidates the parts of a program to be used repeatedly.
Virtualization technology/Virtual machine	A technology to flexibly divide and consolidate computer resources without being confined to a physical configuration. A virtual machine is a computer configured by virtualization technology.
VPN	Abbreviation for Virtual Private Network. A virtual private network built by using encryption and other technologies.

Term	Description
WAF	Abbreviation for Web Application Firewall. A software or hardware that protects web applications from attacks that exploit web application vulnerabilities.
Zone	A collection of data centers located within a region. Typically, there are multiple zones prepared in one region.