Alibaba Cloud User Guide

Financial Services Regulations & Guidelines in The Philippines

Alibaba Cloud

Legal Notices

Alibaba Cloud reminds you to carefully read through and completely understand all of the content in this section before you read or use this document. If you read or use this document, it is considered that you have identified and accepted all contents declared in this section.

1. You shall download this document from the official website of Alibaba Cloud or other channels authorized by Alibaba Cloud. This document is only intended for legal and compliant business activities. The contents in this document are confidential, so you shall have the liability of confidentiality. You shall not use or disclose all or part of the contents of this document to any third party without written permission from Alibaba Cloud.
2. Any sector, company, or individual shall not extract, translate, reproduce, spread, or publicize, in any method or any channel, all or part of the contents in this document without written permission from Alibaba Cloud
3. This document may be subject to change without notice due to product upgrades, adjustment, and other reasons. Alibaba Cloud reserves the right to modify the contents in this document without notice and to publish the document in an authorized channel as and when required. You shall focus on the version changes of this document, downloading and acquiring the updated version from channels authorized by Alibaba Cloud.
4. This document is only intended for product and service reference. Alibaba Cloud provides this document for current products and services with current functions, which may be subject to change. Alibaba Cloud makes the best effort to provide an appropriate introduction and operation guide on the basis of current technology, but Alibaba Cloud does not explicitly or implicitly guarantee the accuracy, completeness, suitability, and reliability of this document. Alibaba Cloud does not take any legal liability for any error or loss caused by downloading, using, or putting trust in this document by any sector, company, or individual. In any case, Alibaba Cloud does not take any legal liability for any indirect, consequential, punitive, occasional, incidental, or penalized damage, including profit loss due to the use of or trust placed into this document (even if Alibaba Cloud has notified you, it is possible to cause this kind of damage).
5. All content including, but not limited to, images, architecture design, page layout, description text, and its intellectual property (including, but not limited to, trademarks, patents, copyrights, and business secrets) used in this document are owned by Alibaba Cloud and/or its affiliates. You shall not use, modify, copy, publicize, change, spread, release, or publish the content from the official website, products, or programs of Alibaba Cloud without the written permission from Alibaba Cloud and/or its affiliates. Nobody shall use, publicize, or reproduce the name of

Alibaba Cloud for any marketing, advertisement, promotion, or other purpose (including, but not limited to, a separate or combined form to use the name, brand, logo, pattern, title, product or service name, domain name, illustrated label, symbol, sign, or similar description that may mislead readers and let them identify that it comes from Alibaba Cloud and/or its affiliates, of or from Alibaba Cloud, Aliyun, Wanwang, and/or its affiliates) without the written permission from Alibaba Cloud.

6. If you discover any errors or mistakes within this document, please contact Alibaba Cloud directly to raise this issue.

Contents

1. Introduction

The Philippines financial sector is in the midst of the rapid transformation, powered by cloud computing technologies. The Bangko Sentral ng Pilipinas (“BSP”) has issued regulations and guidelines to govern the use of cloud computing technologies.

Alibaba Cloud provides a comprehensive suite of global cloud computing services to help power and grow customers’ business worldwide. We strive to provide customers with consistent, reliable, secure, and compliant cloud computing services, helping customers ensure the confidentiality, integrity, and availability of their systems and data.

Alibaba Cloud is committed to facilitate the financial institutions to meet the requirements in the BSP’s regulations and guidelines and partner with the customers to make the transformation journey from on-premise infrastructure to cloud infrastructure as smooth as possible. In this article, Alibaba Cloud attempts to clarify its responsibilities and controls in key areas that financial institutions would have focuses on to help customers to clear the roadblocks in their cloud journey.

2. Regulatory Landscape of The Philippines

Bangko Sentral ng Pilipinas (“BSP”)

The BSP supervises and conducts periodic or special examinations of BSP-supervised Financial Institution (“BSFIs”), over the covered persons including banking institutions and non-bank financial institutions, quasi-banks, trust entities, non-stock savings and loan associations (“NSSLAs”), pawnshops, foreign exchange dealers, money changers, remittance and transfer companies, electronic money issuers and other non-bank financial institutions[1] (“NBFIs”) , and their subsidiaries[2] and affiliates[3].

What Legislations, Regulations and Guidelines are relevant?

This user guide outlines the key consideration areas that should be aware in cloud migration from the below relevant Regulations and Guidelines issued by the BSP.

- Circular 808 – Guidelines on Information Technology Risk Management
- Circular 951 – Guidelines on Business Continuity Management
- Circular 982 – Enhance Guidelines on Information Security Management
- Circular 1019 – Technology and Cyber-Risk Reporting and Notification Requirement
- The Manual of Regulations for Banks (“MORB”)
    - Section 148 – Information Technology Risk Management, including
        - Appendix 78 – IT Outsourcing/Vendor Management; and
        - Appendix 103 – Documents Required under the Revised Outsourcing Framework for Banks
    - Outsourcing in a Cloud Environment Questionnaire

[1] NBFIs shall refer to investment houses, finance companies, trust entities, insurance companies, securities dealers/brokers, credit card companies, NSSLAs, holding companies, investment companies, government NBFIs, asset management companies, insurance agencies/brokers, venture capital corporations, FX dealers, money changers, lending investors, pawnshops, fund managers, mutual building and loan associations, remittance agents and all other NBFIs without quasi-banking functions.

[2] A subsidiary shall be defined as an entity more than fifty percent (50%) of the outstanding voting stock of which is owned by a covered person.

[3] An affiliate shall be defined as an entity the voting stock of which, at least twenty percent (20%) to not more than fifty percent (50%), is owned by a covered person.

What do the above Legislations, Regulations and Guidelines cover?

BSPs Regulations and Guidelines	Coverage
Circular 808 – Guidelines on Information Technology Risk Management	The Guidelines on Information Technology Risk Management was issued on August 22, 2013. The BSP releases guidelines to strengthen risk management, security operations and IT-related activities, as well as enforce consumer protection regulations in for BSFIs
Circular 951 – Guidelines on Business Continuity Management	The Guidelines on Business Continuity Management was issued on March 20, 2017. The BSP incorporates cyber-resilience in the BSFIs' business continuity planning process to adequately capture the potential impact of cyber events.
Circular 982 – Enhance Guidelines on Information Security Management	The Enhance Guidelines on Information Security Management was issued on November 9, 2017. The BSP sets forth enhanced guidelines covering a holistic framework on information security risk management to address the growing concerns on rapidly-evolving cyber-threats.
Circular 1019 – Technology and Cyber-Risk Reporting and Notification Requirement	The Technology and Cyber-Risk Reporting and Notification Requirement was issued on 31 October, 2018. The BSP further strengthens the BSP's cyber-threat surveillance capabilities by tightening the reporting regime for BSFIs on technology and cyber-risk-related incidents and disruptions.
The Manual of Regulations for Banks ("MORB") Section 148 – Information Technology Risk Management, including Appendix 78 – IT Outsourcing/Vendor Management;	The 2018 Manual of Regulations for Banks was issued on December 31, 2018. The BSP provides practical requirements to address risks associated with emerging trends in technology and growing concerns on cybersecurity.

BSPs Regulations and Guidelines	Coverage
Appendix 103 – Documents Required under the Revised Outsourcing Framework for Banks; and	
Outsourcing in a Cloud Environment Questionnaire	The BSP has issued the attached “Cloud Computing Questionnaire”, which contains a number of questions about a FSI’s decision to use a cloud computing solution. The main purpose of the Cloud Computing Questionnaire is to establish that your organization has carried out appropriate due diligence and that the proposed service complies with applicable regulatory requirements in relation to issues such as data security, confidentiality and disaster recovery. The Cloud Computing Questionnaire itself contains some questions which ask for confirmation that certain specific items are covered in the Bank’s contract with its service provider.

General Security Compliance FAQs

Q1: Is cloud permitted in The Philippines?

Yes, subject to the following criteria:

Applicability	Cloud Type	Prerequisite
BSFIs	Public Cloud	Core operations and business processes[4] Currently not allowed. Non-core operations and business processes[5] Prior approval by the BSP is required, which

[4] Core operations and business processes whose importance is fundamental in ensuring continuous and undisturbed operation of IT systems used to directly perform banking and financial services (e.g.,Current accounts/ Savings accounts (“CA/SA”), Loans, Trust and Treasury systems, ATM switch operations, Electronic delivery systems and Systems used to record banking operations).

[5] Non-core operations and business processes which do not directly involve sensitive BSFI and customer data (e.g., email, office productivity, collaboration tools, claims and legal management, etc.) which support the core-operations and business processes.

Applicability	Cloud Type	Prerequisite
		shall include: - To comply with the BSP exiting rules on Outsourcing; - To implement more robust risk management systems and controls, including: ● Vendor management ● Information security ● Audits ● Legal and regulatory compliance ● Business continuity planning - To address issues in Annex A[6] under Appendix 78; - To allow onsite validation prior the cloud computing arrangement by the BSP; - To complete "Outsourcing in a Cloud Environment Questionnaire" and submit to the BSP.
	Private Cloud	Prior approval by the BSP is required, which shall include: - To comply with the BSP existing rules on Outsourcing; - To implement more robust risk management systems and controls, including: ● Vendor management ● Information security ● Audits ● Legal and regulatory compliance ● Business continuity planning - To address issues in Annex A under Appendix 78;
	Community Cloud	
	Hybrid Cloud	

[6] Annex A outlines the BSP's concerns on the following areas: Legal and Regulatory Compliance, Governance and Risk Management, Due Diligence, Vendor Management/ Performance and Conformance, Security and Privacy, Data Ownership and Data Location and Retrieval and Business Continuity Planning.

Applicability	Cloud Type	Prerequisite
		- To allow onsite validation prior the cloud computing arrangement by the BSP; - To complete "Outsourcing in a Cloud Environment Questionnaire" and submit to the BSP.

Q2: What are the customers' responsibilities in maintaining the data?

It is stipulated in Alibaba Cloud's Membership Agreement, which is publicly available on Alibaba Cloud official website, that Alibaba Cloud will not access or use customer's content except as necessary to maintain or provide the Alibaba Cloud Services or as necessary to comply with applicable laws or regulations.

Customers retain exclusive ownership over all its data. Customers are responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

Customers are accountable for complying with the requirements and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party.

Customers shall also designate an individual or individuals who are accountable for the organization's compliance. The identity of the individual(s) so designated shall be made known to any data subject upon request.

Q3: Where is the customers' data stored?

Alibaba Cloud operates 80 availability zones in 25 regions around the world. Region refers to a physical node on a global scale. Each region is composed of multiple zones, and a zone is composed of one or multiple scattered data centers which offers higher availability, error tolerance capabilities, and extendibility than a single data center.

In 2021, Alibaba Cloud releases data center in the Philippines. Customers can choose to use any availability zones and their data will be stored in the availability zone selected. To ensure optimal coverage, customers are suggested to select a data center region closest to their end-users.

Q4: Is data allowed to be transferred to outside The Philippines?

Yes, subject to the jurisdictions that uphold confidentiality and privacy. Customers are required to continuously monitor government policies in their cloud service provider's host country. The customers must submit to the BSP as part of the approval process a list of territories where data will be stored.

Q5: What is the regulatory application and approval process?

Regulatory Requirement

MORB Section 148 – Information Technology Risk Management Appendix 78 – IT Outsourcing/Vendor Management

Under what circumstance do the customers have to inform the BSP?

Commitment on cloud computing subjects to compliance with existing BSP rules and regulations on outsourcing. Implementation of private cloud is allowed, customers should consult BSP before making any significant commitment on cloud computing.

On the other hand, adoption of public, community and hybrid cloud deployment models may also be allowed with prior BSP approval. Under current regulation, BSFIs and its subsidiaries and affiliates can only use public cloud for non-core operations and business processes and usage of public cloud in core operations and business processes is prohibited.

BSP requires the cloud service provider to grant access to its cloud infrastructure for determining compliance with applicable laws and regulations and assessing soundness of risk management processes and controls in place.

What information is required for the application from the customers?

The following documents are required for the application and should be available to the authorized representatives of the BSP for inspection:

- A comprehensive policy on outsourcing duly approved by the board of directors
- Secretary's certificate on the minutes of meeting of the board of directors or a local/regional management committee (for foreign banks), explicitly approving the activity to be outsourced, the determination of the materiality of the outsourcing arrangement and the selected service provider with which the bank is entering into an outsourcing contract
- Profile of the selected service provider
- A central record of all outsourcing arrangements
- Service level agreement (SLA) of contract between the customer and the service provider

Also, the BSFIs are required to complete “Outsourcing in a Cloud Environment Questionnaire” and submit to the BSP for assessment.

Proposed Timeline

As a best practice, BSFIs shall submit the required documents to BSP **30 banking days** prior to the implementation of new or changes in material outsourcing arrangement. BSP reserves the right to issue a notice of objection or require additional documents from the bank, within 30 calendar days from receipt of the notification letter, related to the bank’s engagement in material outsourcing arrangements. In this regard, a bank that did not receive any notice of objection from the BSP within the said 30-day period may proceed with implementation of the material outsourcing arrangement.

3. Compliance User Guide

Overview

Data security and user privacy are the top priorities of Alibaba Cloud. Alibaba Cloud is committed to building a public, open, and secure cloud computing service platform. Alibaba Cloud aims to turn cloud computing into a state-of-the-art computing infrastructure by investing heavily in technical innovation to continually improve the computing capabilities and economies of scale of its services. Alibaba Cloud strives to provide customers with consistent, reliable, secure, and compliant cloud computing services, helping customers ensure the confidentiality, integrity, and availability of their systems and data. For details, please refer to the *Alibaba Cloud Security Whitepaper*. (See “Useful Resource – 2. Alibaba Cloud Security Whitepaper, Version 2.0”).

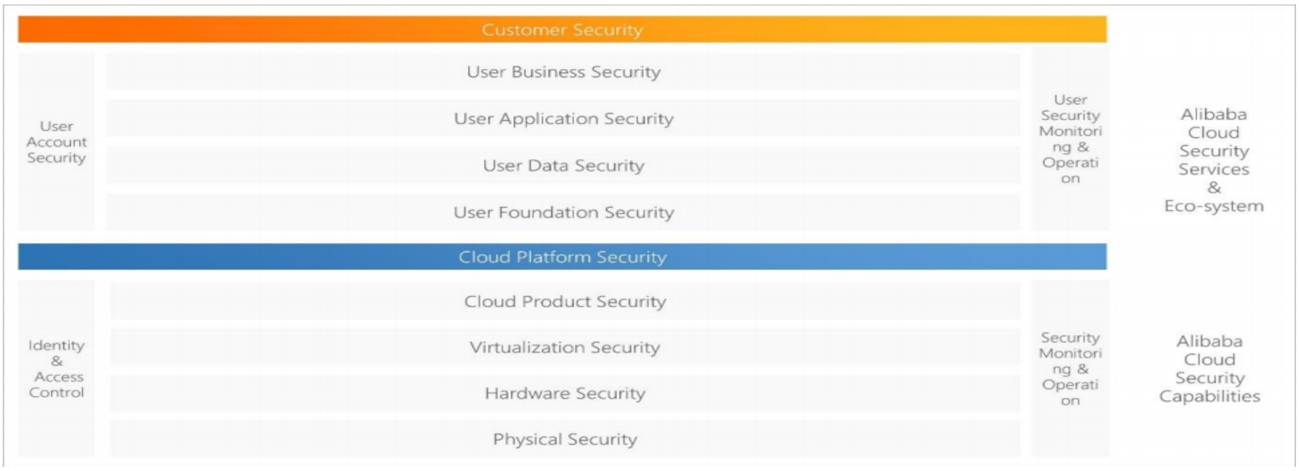
Also, Alibaba Cloud adheres to domestic and international information security standards, as well as industry requirements. We integrate compliance requirements and standards into our internal control framework and implement such requirements and standards into our cloud platform and products by design. Alibaba Cloud is involved in the development of multiple standards for the cloud industry and contributes to industry best practices. We also engage with independent third parties to verify the compliance of Alibaba Cloud according to various requirements. Certified by more than ten standards across the globe, Alibaba Cloud is a cloud service provider with one of the most complete ranges of certifications in Asia.

Benefits of Migrating from On-premises to the Cloud

Alibaba Cloud delivers on-demand computing resources (including servers, databases, storage, platforms, infrastructure, applications, etc.) over the Internet. Alibaba Cloud can be used on a pay-as-you-go basis, which means customers can pay just for what you need. With the rapid development of cloud computing services, migrating existing server systems to Alibaba Cloud easily and quickly is of great significance for you, benefiting from cost-efficiency, data security, scalability and speed, elasticity, unlimited storage space, backup and recovery, and go global in minutes. Besides, Alibaba Cloud provides end-to-end compliance support from Security Compliance Specialist to work with the customers on their security, risk and compliance strategies on the Alibaba Cloud platform. The professionals help the customers to understand how they can integrate Alibaba Cloud security controls into their own control frameworks and provide recommendations in approaches on implementing their controls on Alibaba Cloud.

3.1 Alibaba Cloud Shared Responsibility Model

Alibaba Cloud employs a shared responsibility model, meaning that the security of applications built on Alibaba Cloud is the joint responsibility of Alibaba Cloud and its customers. In general, Alibaba Cloud is responsible for the security of the underlying cloud service platform and providing security services and capabilities to customers, while customers are responsible for the security of applications built based on Alibaba Cloud services. This relieves much of the underlying security burdens while allowing customers to focus more on their core business needs.



Customer Security

User Account Security

User Business Security

User Application Security

User Data Security

User Foundation Security

User Security Monitoring & Operation

Alibaba Cloud Security Services & Eco-system

Cloud Platform Security

Identity & Access Control

Cloud Product Security

Virtualization Security

Hardware Security

Physical Security

Security Monitoring & Operation

Alibaba Cloud Security Capabilities

At Alibaba Cloud, we ensure the security of infrastructure (including but not limited to data centers deployed across regions and zones, and Alibaba backbone networks), physical devices (including computing, storage, and network devices), virtualization solutions, and cloud products running on top of the Apsara distributed cloud OS. Alibaba Cloud is also responsible for identity management and access control, monitoring, and operations of the platform to provide customers with a highly available and secure cloud service platform.

Still, customers retain the responsibility for protecting their own systems by using the security features provided by Alibaba Cloud services, Alibaba Cloud Security, and third-party security products in the Alibaba Cloud security ecosystem. Alibaba Cloud offers Alibaba Cloud Security, which leverages the years of expertise in attack prevention technologies to help customers protect their applications and systems and customers should configure and use cloud products based on security best practices, and build applications on these securely configured cloud products.

3.2 Implementation of Key Areas of Regulation and Guideline with Alibaba Cloud

This part outlines how Alibaba Cloud can help the customers in implementing the key areas of in-scope Regulations and Guidelines listed in **Section 2 — Regulatory Landscape of The Philippines**.

The key areas are as follows:

▪ Domain 1 — Outsourcing

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the outsourcing activities, including Policy and Procedure, Overseas Outsourcing, Due Diligence, Contract Management, Vendor Management.

- 1.1 Policy and Procedure

Key Aspects	Applicability	Consideration
Outsourcing policy	BSFIs - MORB (IT Outsourcing/ Vendor Management)	BSFIs BSFIs are responsible for establishing a comprehensive policy on outsourcing duly approved by the board of directors.

- 1.2 Overseas Outsourcing

Key Aspects	Applicability	Consideration
Data transfer to overseas	BSFIs & Alibaba Cloud - MORB (IT Outsourcing/ Vendor Management)	BSFIs Alibaba Cloud has prepared user guide on regulations of different regions to provide an overview of the regulatory landscape of the host country and the key consideration areas that are covered in the relevant legislation, regulation, and guideline. The user guide is publicly available for customers in Security & Compliance Trust Center. BSFIs can download the relevant user guides to understand and identify what requirements are applicable to them regarding data transfer to overseas.

Key Aspects	Applicability	Consideration
		Alibaba Cloud Alibaba Cloud understands the regulatory requirements imposed on the customers and helps the customers to fulfill such requirements by conducting regular audits following the relevant requirements. For General Control Environment of the Service Provider, please refer to Domain 1.3 — Due Diligence.
Notifications to the authorities	BSFIs - MORB (IT Outsourcing/ Vendor Management)	BSFIs BSFIs are responsible to notify the relevant authorities listed in **Section 2 — Regulatory Landscape of The Philippines** of this Whitepaper about the overseas outsourcing arrangement. Alibaba Cloud provides end-to-end compliance support from Security Compliance Specialist to help customers understand how they can integrate Alibaba Cloud security controls into their own control frameworks and provide recommendations in approaches on implementing their controls on Alibaba Cloud.
Access to outsourced data by local and overseas authorities and auditors	BSFIs & Alibaba Cloud - MORB (IT Outsourcing/ Vendor Management)	BSFI BSFIs are responsible to include a clause which allows for the authority examiners and auditors, i.e. internal and external auditors, to access the data in the outsourcing service agreement. Alibaba Cloud Alibaba Cloud has defined respective responsibilities and obligations of customers and Alibaba Cloud and

Key Aspects	Applicability	Consideration
		the terms and conditions in the service agreement, which includes the rights of Governmental Authorities and Auditors and clauses for overseas outsourcing.
System availability	BSFIs & Alibaba Cloud - MORB (IT Outsourcing/ Vendor Management)	BSFIs BSFIs are responsible to deploy cloud components with sufficient capacity across regions and zones to implement a high availability architecture to meet recovery requirements as set out in their Business Continuity Plans (BCPs). *Block Storage* BSFIs can use Block Storage to automatically replicate data across different servers within a zone and prevents data unavailability due to unexpected hardware failures or affected by a successful cyberattack while ensuring business continuity. *Apsara DB for RDS* BSFIs can use RDS to support remote disaster recovery. Different RDS editions adopt different architectures to ensure RDS is highly available. Users can synchronize data stored in on-premises data center or user-created database on an Elastic Compute Service (ECS) instance to a RDS instance in any region for business continuity and disaster recovery purpose. *Object Storage Service (OSS)* Multi-zone mechanism allows OSS to distribute user data across three zones within the same region so that users' data is still accessible even if one zone becomes unavailable.

Key Aspects	Applicability	Consideration
		Server Load Balancer (SLB) For circumstances where an ECS instance may fail when reaching capacity checkpoints, SLB can synchronize sessions to achieve load balancing in order to protect the ECS instances from single points of failure. *Alibaba Cloud Domain Name System (DNS)* When disaster happens, SLB and ECS instances can operate when users enable resolution and failover setting in Alibaba Cloud DNS so that Alibaba Cloud DNS can route visitors to the nearest application servers i.e., the backup ECS node. Alibaba Cloud Alibaba Cloud offers high available cloud computing infrastructure by setting up cloud data centers across multiple regions and zones globally to ensure cloud products and services are highly available and provide multi-replica data redundancy. Besides, Alibaba Cloud provides different solution to users to enhance their system resilience capability. Critical Alibaba Cloud system components are replicated across multiple Availability Zones to ensure operating processes can be switched to another available zone.
Business continuity management relating to the outsourcing arrangement	BSFIs & Alibaba Cloud - MORB (IT Outsourcing/ Vendor	BSFIs Alibaba Cloud has defined service terms and clauses in the service agreements template, for example, condition for contingency planning where Alibaba

Key Aspects	Applicability	Consideration
	Management)	Cloud acknowledges and agrees that Alibaba Cloud shall maintain and regularly test the contingency plans to ensure business continuity. Alibaba Cloud agrees that customers may rely on the monitoring of the service levels as set out in the SLAs, as well as existing audit reports / certificates covering the relevant policy, procedures, controls, tests and mechanisms of Alibaba Cloud (e.g., International Organization for Standardization (ISO) 22301, Service Organization Control (SOC) 2, etc.). BSFIs can integrate the provider's BCP into its own plan, communicate functions to the appropriate personnel, and maintain and periodically review the combined plan. It should ensure that service provider tests its plan annually and notify the institution of any resulting modifications. Alibaba Cloud Alibaba Cloud maintains an effective BCP in accordance with ISO 22301 with independent audit by third party conducted at least on an annual basis. The certificate of ISO 22301 is available to customer to download publicly from Security & Compliance Centre of Alibaba Cloud. For details about Business Continuity Management, please refer to **Domain 13**.

- 1.3 Due Diligence

Key Aspects	Applicability	Consideration
Outsourcing risk management	BSFIs - MORB (IT Outsourcing/	BSFIs

Key Aspects	Applicability	Consideration
	Vendor Management)	BSFIs are responsible for performing risk assessment prior to the outsourcing arrangement. Alibaba Cloud has prepared user guide with the information of Alibaba Cloud’s financial soundness, reputation, managerial skills, technical capabilities, operational capability and capacity, etc. to facilitate customers’ due diligence process. BSFIs can find the user guide in Security & Compliance Trust Centre. *Financial Soundness* Alibaba Cloud is a fully owned subsidiary of Alibaba Group Holding Limited (NYSE: BABA). Alibaba Cloud’s revenue grows very fast, primarily driven by increased spending from enterprise customers. Alibaba Cloud has been keeping launching new products and features including those related to core cloud offerings, data intelligence, AI applications, security and enterprise solutions. *Reputation* Alibaba Cloud is an industry leading cloud provider in China and it has been officially recognized as one of the only six players in the Gartner magic quadrant for cloud IaaS, worldwide. *Managerial Skills* Alibaba Cloud performs a comprehensive risk assessment considering factors from financial, regulatory, customer service and reputational perspective, at least once a year, and updates the security controls and related policies based on the

Key Aspects	Applicability	Consideration
		assessment results. *Technical Capabilities* Alibaba Cloud provides the technical foundation to the entire Alibaba Group, including the world renowned Taobao Marketplace. From the latest statistics generated internally by Alibaba Cloud in by March 2019, the Alibaba Cloud platform is capable of protecting approximately 40% of websites in China, detecting on a daily basis over 60,000 malicious IPs and defending over 3,600 million attacks and approximately 3,000 distributed denial-of-service (DDoS) attacks every day. *Operational Capability and Capacity* Alibaba Cloud has established an information security management system (ISMS) and certified the ISMS according to ISO/IEC 27001:2013. Alibaba Cloud has also established IT Service Management System (ITSM) policies which are based on ISO/IEC20000. On a yearly basis, Alibaba Cloud performs a management review and documents the review results. If weaknesses are discovered, follow-up action must be taken to ensure continuous improvement on the management system.

- 1.4 Contract Management

Key Aspects	Applicability	Consideration
Service agreement	BSFIs & Alibaba Cloud - MORB (IT Outsourcing/	BSFIs Alibaba Cloud provides a template of an offline

Key Aspects	Applicability	Consideration
	Vendor Management)	Cloud Services Purchase Agreement or Enterprise Agreement. Alibaba Cloud customers have the option to enter into an offline Cloud Services Purchase Agreement or Enterprise Agreement with Alibaba Cloud. The terms and conditions in the offline agreements can be tailored to better meet the customers' needs. Alibaba Cloud Vendors involved in the delivered services are mainly data center service providers. A service agreement is signed between Alibaba Cloud and each data center service provider to define their responsibilities and obligations. In addition, a Service Quality Warranty Letter is attached to the agreement to specify requirements on data center service availability level, business relationship and service scope etc. Alibaba Cloud continuously monitors service level of data center service providers to ensure secure and stable operation of data centers. A monthly service level report must be submitted by service providers to Alibaba Cloud for review, covering services provided during the past month, major incidents, summary of maintenance performed, and any feedback, to ensure all Alibaba Cloud's requirements are appropriately met.

- 1.5 Vendor Management

Key Aspects	Applicability	Consideration
Performance monitoring	BSFIs & Alibaba Cloud -	BSFIs

Key Aspects	Applicability	Consideration
	MORB (IT Outsourcing/ Vendor Management)	BSFIs are responsible for establishing proper measures to monitor their service provider that their performance is in line with relevant service levels and requirements stipulated in the service agreement. Alibaba Cloud Alibaba Cloud evaluates vendors' performance monthly in accordance with the compliance requirements and service levels specified in the contracts. Data center service providers submit monthly service level reports to Alibaba Cloud, covering services provided during the past month and any feedbacks to Alibaba Cloud. Alibaba Cloud's data center managers review the reports in the monthly meetings and record exceptions into the meeting minutes.
Monitoring of control environment	BSFIs & Alibaba Cloud - MORB (IT Outsourcing/ Vendor Management)	BSFIs BSFIs are responsible for performing regular monitoring on service provider's control environment to ensure that the service provide impose similar level of security controls as the BSFIs. Alibaba Cloud Alibaba Cloud acknowledges the customers are required by government authorities to continuously review the effectiveness and adequacy of customers' controls in monitoring the performance of customers' service providers. Alibaba Cloud

Key Aspects	Applicability	Consideration
		therefore supports the audit by the following ways: - Customers providing a questionnaire for Alibaba Cloud to complete; or - A report provided by Alibaba Cloud to customers, addressing any queries that customers may have from time to time; or - A qualified independent third-party audit report; or - An audit to be carried out by the Government Authorities or any agent appointed by the Government Authorities, or an outside firm as mutually agreed by the Parties. Alibaba Cloud will invite independent third party auditors to conduct auditing over the underlying cloud platform. BSFIs can find Alibaba Cloud's most recent certificates and assurance reports via the Security and Compliance Center. For the security incidents with Alibaba Cloud's platform and infrastructure, the security incident response team would follow the incident handling procedures to resolve the incidents identified. A notification will be sent to the impacted customers of the security issue via web console, email and text channel right after the incidents have been identified and resolved.

▪ Domain 2 — Data Security

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the data security, including Policy and Procedure, Data Ownership, Data Protection and Data Disposal and Destruction.

- 2.1 Policy and Procedure

Key Aspects	Applicability	Consideration
Policy and Procedure – Data Classification	BSFIs - Enhance Guidelines on Information Security Management	BSFIs BSFIs are responsible to develop a formal policy on how to handle data based on the classification. Appropriate personnel such as the operation and compliance team should review the classification regularly. BSFIs can make use of Alibaba Cloud Sensitive Data Discovery and Protection (SDDP) which can automatically detect sensitive data stored in data sources. It supports content-based sensitive data detection for files and uses optical character recognition (OCR) technology to extract and detect sensitive information stored in pictures. SDDP also automatically classifies sensitive data that are detected in structured and unstructured data sources and displays the statistics of sensitive data.
Policy and Procedure – Data Security	Alibaba Cloud - Enhance Guidelines on Information Security Management	BSFIs FIs are responsible to institute appropriate set of controls and procedures for information protection in accordance with the information classification scheme. Information should be protected throughout its life cycle from handling, storage or data-at- rest, transmission or data-in-transit, up to the disposal phase. Alibaba Cloud Alibaba Group has established Data Security Guidelines to define different data types, data owners, data classification standards, and protection measures. The policy also governs data security

Key Aspects	Applicability	Consideration
		management lifecycle, including data generation, data storage, data usage, data transmission, data dissemination and data disposal.

- 2.2 Data Ownership

Key Aspects	Applicability	Consideration
Data Ownership	BSFIs - MORB (IT Outsourcing/ Vendor Management)	<u>BSFIs</u> BSFIs have full ownership over the content they stored in the cloud environment. It is stipulated in Alibaba Cloud's Membership Agreement, which is publicly available on Alibaba Cloud official website, that Alibaba Cloud will not access or use customer's content except as necessary to maintain or provide the Alibaba Cloud Services or as necessary to comply with applicable laws or regulations. Alibaba Cloud Operating and Maintenance (O&M) personnel are not able to access undisclosed data of customers without prior consent and authorization of the customers. In addition, production data is kept within the production cluster, and channels for production data to flow out of the production cluster are blocked to prevent O&M personnel from copying data from the production system. BSFIs retain the right to decide where their system and data stored. In case of any relocation of customer conducted by Alibaba Cloud due to data centre relocation, Alibaba Cloud shall notify the affected customers and obtain their consent as stipulated in the Service Purchase Agreement with Financial Institution customers.

Key Aspects	Applicability	Consideration
Data Retrieval	BSFIs & Alibaba Cloud - MORB (IT Outsourcing/ Vendor Management)	BSFIs Prior to termination of a contract, Alibaba Cloud provides customer technical measures to download their data and delete it afterwards from Alibaba Cloud, to ensure no data will be retained in Alibaba Cloud. Besides, there are built-in features of Alibaba Cloud's products that allow customers to download and delete their data prior to termination of a contract to ensure no data will be retained in Alibaba Cloud.

- 2.3 Data Protection

Key Aspects	Applicability	Consideration
Data Encryption in Storage	BSFIs & Alibaba Cloud - Enhance Guidelines on Information Security Management	BSFIs *Key Management Service (KMS)* Alibaba Cloud provides KMS for key management and data encryption capabilities for the encrypted storage of sensitive data on the cloud platform, which supports the Advanced Encryption Standard with 256-bit key length (AES256) for encrypting sensitive data at rest. Such sensitive data include authorization credentials, passwords, and encryption keys. Customers can also use and manage service keys or user-managed keys (Bring Your Own Key ("BYOK") i.e., keys imported from key management infrastructure) as the customer managed keys ("CMK") for data encryption.

Key Aspects	Applicability	Consideration
		OSS OSS can return the CRC64 value of objects uploaded using any of the uploading methods provided. The client can compare the CRC64 value with that calculated locally to verify data integrity. An error-checking code is also generated and used throughout the storage process for fine-grained data integrity protection. Alibaba Cloud Alibaba Cloud uses data encryption to ensure data security, including sensitive data encryption in applications, transparent data encryption in the database, block storage data encryption, object storage system encryption and hardware security modules.
Data Encryption in Transit	BSFIs & Alibaba Cloud - Enhance Guidelines on Information Security Management	BSFIs BSFIs are responsible to develop policies and procedures and implement appropriate safeguards depending on the channel used. The means of protection vary with the network channels used in the data transmission process. For internal communication i.e., data transmission between enterprise sites, VPNs or dedicated lines (Express Connect) should be used to reinforce communication channels. Alibaba Cloud provides VPN Gateway services to help customers build end-to-end data encryption channels to ensure communication security during data transmission between on-premises data centers and Alibaba

Key Aspects	Applicability	Consideration
		Cloud Virtual Private Clouds (VPCs). VPN Gateway establishes IPsec-VPN connection to connect an on-premises data center to a VPC or SSL-VPN connection to connect a remote client to a VPC. Customers should use Secure Sockets Layer (SSL) / Transport Layer Security (TLS) certificates to encrypt transmission channels for requests sent by clients through the Internet. This prevents data from being intercepted by man-in-the-middle attacks during transmission. Alibaba Cloud SSL Certificates Service can issue SSL certificates from well-known third-party certificate authorities (CAs) in the cloud. It helps customers switch from Hypertext Transfer Protocol (HTTP) to Hypertext Transfer Protocol Secure (HTTPS), improve the trustworthiness of their websites, and prevent their websites from being hijacked, tampered with, or spied on. Certificates Service simplifies certificate deployment and allows enterprises to perform unified lifecycle management of their certificates in the cloud, and distribute the certificates to other Alibaba Cloud services with a few clicks. Alibaba Cloud Alibaba Cloud console uses HTTPS encryption for data transmission. Apart from console, Alibaba Cloud products use TLS protocol to ensure data transmission security while users read and upload data. HTTPS is also used to encrypt application programming interface (API) payload data to address the need for protecting transmission of sensitive data via API.

Key Aspects	Applicability	Consideration
Generation, distribution, storage, entry, use and archiving of cryptographic keys	BSFIs & Alibaba Cloud - Enhance Guidelines on Information Security Management	BSFIs BSFIs are responsible to adopt industry-accepted cryptographic solutions and implement sound key management practices to safeguard the associated cryptographic keys. *KMS* KMS provides functions such as secure hosting of keys and cryptographic operations, and implements security practices such as key rotation. KMS can be integrated into other cloud services to encrypt user data managed by these services. KMS's secure and reliable key management is an important prerequisite for data encryption capabilities in cloud services. **Managed Hardware Security Module (HSM)** In addition to the software cryptographic module that hosts CMK in KMS, Alibaba Cloud KMS allows users to manage keys in HSMs and use HSMs for cryptographic and security management operations, providing a higher level of protection for CMKs. **CMK** Each cloud service can manage a default service managed key in KMS for users and use the key to encrypt data. Users can audit the behaviors of cloud services that use KMS to encrypt and decrypt data. Although service managed keys can provide the most basic data protection capabilities, a few shortcomings exist for users who have a clear

Key Aspects	Applicability	Consideration
		requirement for key management. For example, users are not allowed to manage the lifecycle of keys or set automatic rotation, and the service managed keys are only protected in the software cryptographic module of KMS. With the support for CMKs, users can choose to create or upload CMKs into KMS, and choose to use customer managed CMKs through supported cloud services. The users would in turn directly manage the lifecycle of these CMKs. After the authorization through RAM, CMKs can be used for data encryption of cloud services, and can empower users with stronger security capabilities. **Key rotation** KMS integrates automatic key rotation based on the capability of supporting multiple versions of a CMK. With automatic key rotation, KMS automatically generates a new version of a CMK based on the configured schedule. All older versions are used to decrypt historical data. In certain scenarios, users may also re-encrypt historical data to convert the ciphertext generated with an older version of a CMK into the ciphertext encrypted with the new version. Users can also manually rotate CMKs one or more times beyond the automatic rotation schedule when needed.
Off-site back-up and contingency arrangements for cryptographic keys	BSFIs - Guidelines on Information Technology Risk Management	BSFIs BSFIs are responsible to establish the off-site back-up and contingency arrangements for cryptographic keys.

- 2.4 Data Disposal and Destruction

Key Aspects	Applicability	Consideration
Data Disposal and Destruction	Alibaba Cloud - Guidelines on Information Technology Risk Management, Enhance Guidelines on Information Security Management	Alibaba Cloud Alibaba Cloud has established Data Security Guidelines to govern data security management lifecycle, including data disposal. Alibaba Cloud has established a security management system for the full lifecycle of devices, including reception, storage, placement, maintenance, transfer, and reuse or decommissioning. Access control and operation monitoring of devices are managed strictly, and maintenance and stocktaking of devices are conducted on a regular basis. When any device is recycled or decommissioned, Alibaba Cloud takes data erasure measures for the storage media. Prior to disposal of data assets, it is necessary to check whether the media containing sensitive data and genuine licensed software has been overwritten, degaussed, or physically bended and destroyed to make sure that the data cannot be restored. When certain hard copy materials are no longer needed due to business or legal reasons, Alibaba Cloud physically destroys them or obtains proof of destruction from any third-party data processors, to ensure that the data cannot be reconstructed. On terminating services to cloud service customers, Alibaba Cloud deletes the data assets of the customers in a timely manner or returns the data assets according to relevant agreements. Alibaba Cloud uses data erasure techniques that meet industry standards. The erasure operations are

Key Aspects	Applicability	Consideration
		logged to prevent unauthorized access to customer data.

Domain 3 — Access Management

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the access management, including Logical Access, Physical Access, and Privileged Access.

- 3.1 Logical Access

Key Aspects	Applicability	Consideration
Access Provisioning	BSFIs & Alibaba Cloud - Enhance Guidelines on Information Security Management	BSFIs BSFIs are responsible to adopt a sound and systematic access management program following the principles of least privilege and segregation of duties. BSFIs should grant, modify and terminate the access privilege employee access to systems and confidential data based on job responsibilities and the principles of least privilege. The principle of separation of duties should be put in place to restrict employee access to systems and confidential data. *Resource Access Management (RAM)* Customers can use RAM service offered by Alibaba Cloud to manage user identities and resource access permissions by creating a set of processes

Key Aspects	Applicability	Consideration
		to manage user identity changes. RAM enables an Alibaba Cloud account to have multiple independent RAM users. Within RAM, an Alibaba Cloud account owner can create independent RAM user accounts for employees, systems or applications. Also, when an employee leaves the enterprise, the personnel organizational structure changes, or an employee changes the project to which the employee belongs, AIs can change the RAM users, permissions, or the user groups to which the RAM users belong to accurately manage identities and permissions in the cloud. Changes to physical and logical user access, including those that result from voluntary and involuntary terminations, should trigger automated notices, be submitted to and approved by the appropriate personnel. *Single Sign On (SSO)* Every RAM user Administrators can implement SSO or multi-factor authentication (MFA) to authenticate user access. Further, administrators are authenticated using AccessKey (AK) pair when accessing the Alibaba Cloud resources through APIs. Alibaba Cloud Alibaba Cloud assigns permissions based on business needs, and centrally manages permissions by role, user group, department, and user. Each internal user can apply for and use permissions through the permission management system, and the permissions can also be revoked through the system. To strengthen permission management and reduce the risk of using incorrect permissions,

Key Aspects	Applicability	Consideration
		Alibaba Cloud sets different levels of permissions and roles according to risks, and implements different approval processes accordingly at different permission levels. The system automatically freezes permissions that have not been used for a certain period of time. For users who leave Alibaba Cloud, the system automatically freezes their accounts and reclaims their permissions. For users who move to new positions, the system automatically revokes their permission.
Logical Access Review	BSFIs & Alibaba Cloud - Enhance Guidelines on Information Security Management	BSFIs BSFIs are responsible to ensure that user access rights remain appropriate through a periodic user access re-certification process. Obsolete user accounts or inappropriate access rights should be disabled/removed from the systems in a timely manner. *RAM* Alibaba Cloud offers RAM service, which customers can generate and download a RAM user credential report that contains the credential details such as user creation time, user last logon time of the Alibaba Cloud account and RAM users under the Alibaba Cloud account. By reviewing the credential reports, users can detect for the presence of unauthorised users.

Key Aspects	Applicability	Consideration
Segregation of Duties	BSFIs & Alibaba Cloud - Guidelines on Information Technology Risk Management, Enhance Guidelines on Information Security Management	BSFIs BSFIs are responsible to define a system access matrix based on users' roles and responsibilities and assign access right based on the matrix. *RAM* Customers can track RAM operation events performed by using Alibaba Cloud accounts, RAM users, and RAM roles. Hence customers are able to retrieve the detail of all current cloud access to ensure segregation of duties. Alibaba Cloud Alibaba Cloud establishes Alibaba Cloud Access Control Management Policy for logical access management. The policy requires that access be granted following least privilege principle and be granted only upon business needs. The policy defines basic rules of segregation of duties by roles and functions at both managerial level and operational level according to company structure and product teams. Alibaba Cloud has also established Alibaba Cloud Operation Security Management Policy to regulate the segregation of duties mechanism during the design, maintain and grant access to user accounts. Therefore, duties are separated between O&M and audit staff, with the security team being responsible for the audit. Duties are also separated between the database and system administrators.

Key Aspects	Applicability	Consideration
Password Management	BSFIs & Alibaba Cloud - Guidelines on Information Technology Risk Management, Enhance Guidelines on Information Security Management	BSFIs BSFIs are responsible to establish a configuration baseline for password policy to govern the standard of password complexity and password attempts etc. and configure password policy according to the baseline. Customers may create custom password strength policies, including minimum password length, password complexity, and limits to password retries and reuse. *RAM* Administrators can configure password policy for RAM users by specifying password complexity requirements, including the password length, validity period, limitation of password attempts and password history. Alibaba Cloud Alibaba Cloud assigns each user a unique account, and each account has a clear owner. A unified password policy is employed. It requires users to configure a password that meets certain length and complexity requirements and to change the password on a regular basis (further, users are prevented from reusing their previous password). Multiple logon authentication modes are supported, such as account and password logon, one-time password logon, and digital certificate logon. Alibaba Cloud establishes and applies the following password policies: - The new password must be different from previous four passwords;

Key Aspects	Applicability	Consideration
		- Users are forced to change passwords every 90 days. The minimum modification interval is 24 hours; - The maximum number of login attempts is set at five times. If no attempt is successful, the system will be locked for 30 minutes; - The minimum password length is set at eight characters; - Password complexity requirement is defined (i.e., password must contain characters from three or more character categories: uppercase characters, lowercase characters, numbers and special characters); - Users must change their password upon initial login.

- 3.2 Physical Access

Key Aspects	Applicability	Consideration
Access Provisioning	Alibaba Cloud - Enhance Guidelines on Information Security Management	Alibaba Cloud Data center managers must notify data center service providers' personnel of access provisioning, modification and termination for access to the data centers. Only authorized personnel are granted with physical access to data centers.
Physical Access Review	Alibaba Cloud - Enhance Guidelines on Information Security Management	Alibaba Cloud Alibaba Cloud data center managers perform an access review of users with access to the data centers in a regular basis.

Physical Security	Alibaba Cloud - Guidelines on Information Technology Risk Management, Enhance Guidelines on Information Security Management	Alibaba Cloud For each entry to or exit from the data center, such persons must display their ID to check in, and be escorted by the data center's maintenance personnel for the entire duration of the visit. Alibaba Cloud data center consists of equipment rooms, electrical measurement areas, warehouses, and other areas, with each area equipped with an independent access control system. Two-factor authentication (2FA) (such as biometric verification) is employed for sensitive areas, and special areas are physically isolated by metal cages. All Alibaba Cloud data centers and office areas have access control, with visitor areas marked out separately. Visitors are required to carry entry pass and be escorted by Alibaba Cloud staff when visiting Alibaba Cloud premises. The visit is logged. Data centre service providers have installed video surveillance at the entrance of data centres, equipment delivery areas, etc. The video records are required to be stored for at least three months. In addition, the personnel on duty at the monitoring rooms monitors the operation of data centres 24/7.

- 3.3 Privileged Access

Key Aspects	Applicability	Consideration
Remote Access Provisioning	BSFIs & Alibaba Cloud - Guidelines on Information Technology Risk	BSFIs BSFIs are responsible to establish procedures for formal authorization process for granting remote

Key Aspects	Applicability	Consideration
	Management, Enhance Guidelines on Information Security Management	access. *RAM* For remote access, RAM privilege users can enable MFA, and Bationhost offers 2FA service to users. The mechanism protects information from unauthorised use and disclosure by remote access. *Bastionhost* Bastionhost allows customers to include reasons for running privileged commands, which must be approved by administrators before execution. It also provides session playback to facilitate auditing such actions. *VPN Gateway* Customers can use VPN Gateway to protect remote access sessions that the connections are encrypted by Wi-Fi Protected Access 2 (WPA2). All remote accesses would need to pass through the VPN gateway before entering the cloud network. Besides, customers can disconnect the remote access expeditiously in an emergency. Alibaba Cloud All internal resources within the production environment can only be accessed via Alibaba Cloud's Intranet. Authorized personnel must pass 2FA based on domain account name and password plus dynamic digital token received on registered devices to access Alibaba Cloud's Intranet through VPN from the internet.
Emergency Access	BSFIs & Alibaba Cloud -	BSFIs

Key Aspects	Applicability	Consideration
	Guidelines on Information Technology Risk Management, Enhance Guidelines on Information Security Management	BSFIs are responsible to ensure that the use of emergency IDs should be tightly controlled as it gives the user the ability to override system or application controls. Necessary controls may include: Proper safeguard of emergency IDs and passwords; - Change of privileged and emergency IDs' passwords immediately upon return by the requesters Alibaba Cloud Alibaba Cloud's operator may have one-time service permission or service account provisioned to customer’s environment for troubleshooting purpose after obtaining the customer's approval. One-time access key will be granted for the account access and such access will be automatically revoked once the authorization is expired. Alibaba Cloud O&M personnel are not allowed to access customer data without prior consent of the customers. In line with the principle of keeping production data within the production cluster, any channels for production data to flow out of the production cluster are blocked via technical means, thus preventing O&M personnel from copying data from the production system.
Log Monitoring	BSFIs & Alibaba Cloud - Guidelines on Information Technology Risk	BSFIs BSFIs are responsible to monitor activities performed by privileged and emergency IDs.

Key Aspects	Applicability	Consideration
	Management, Enhance Guidelines on Information Security Management	*Bastionhost* Bastionhost also supports session audit, real-time monitoring as well as operating logs review so that administrator can monitor the activities performed by O&M users. Alibaba Cloud Alibaba Cloud defines monitoring rules within the access monitoring system to analyze usage of accounts and access privileges. Automated alerts are generated based on the monitoring results and followed up by security team.

Domain 4 — IT Asset Management

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the IT asset management.

- 4.1 IT Asset Management

Key Aspects	Applicability	Consideration
Technology Inventory	BSFIs & Alibaba Cloud - Guidelines on Information Technology Risk Management	BSFIs BSFIs are responsible to perform and maintain an inventory of all its IT resources, recognize interdependencies of these systems and understand how these systems support the associated business lines. BSFIs should ensure the inventory is updated on an on-going basis to reflect its IT environment at any point in time. Alibaba Cloud Alibaba Cloud has established a Configuration

Key Aspects	Applicability	Consideration
		Management Database (CMDB) for managing the assets related to cloud services. All inventoried assets are assigned to an asset owner, and the assignment of assets to each asset owner is documented in CMDB. In this CMDB, all the history of the changes to the entries in the inventory will be maintained. Alibaba Cloud also establishes Procurement Guideline to regulate equipment acquisition and deployment procedures. The following policies has been established by Alibaba Cloud to govern the procedure of new product development and change management: - Alibaba Cloud System Acquisition, Development, and Maintenance Management Provision; - Alibaba Cloud New Service and Major Service Change Management Provision; - Alibaba Cloud Information Service Change Management Provision; - Public Cloud Change Management Guidelines; and - Alibaba Cloud Management Policy of Information Service Configurations and Assets.
Asset Classification	BSFIs & Alibaba Cloud - Guidelines on Information Technology Risk Management	BSFIs BSFIs are responsible to maintain an inventory of all information assets and identify the information owner who shall be responsible in ensuring confidentiality, integrity and protection of these assets. BSFIs should implement an information classification strategy in accordance with the degree

Key Aspects	Applicability	Consideration
		of sensitivity and criticality of information assets. To ensure consistent protection of information and other critical data throughout the system, BSFIs should develop guidelines and definitions for each classification and define an appropriate set of controls and procedures for information protection in accordance with the classification scheme. *Data Management Service (DMS)* DMS offers centralized platform for customers to manage their database and information assets. Data classification services offered in DMS for customers' data assets can help to identify the security level of data (confidential, sensitive and internal) according to the rule configured by security administrator in DMS. Alibaba Cloud Alibaba Cloud has established Alibaba Cloud Information Assets Security Management Policy to regulate the identification, classification and management of information assets. Alibaba Cloud has established a CMDB for maintaining information assets related to cloud services. Each inventoried information asset is assigned to an asset owner. Changes to the information asset inventory are also tracked in the database in real-time basis.

▪ Domain 5 — Network Management

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the network management.

- 5.1 Network Management

Key Aspects	Applicability	Consideration
Network Design	BSFIs - Guidelines on Information Technology Risk Management	<u>BSFIs</u> BSFIs are responsible to design and maintain detailed network architecture.
Network Isolation	BSFIs & Alibaba Cloud - Guidelines on Information Technology Risk Management, Enhance Guidelines on Information Security Management	<u>BSFIs</u> *<u>VPC</u>* Based on tunneling technology, customers can use VPC instances that are logically isolated from another VPC instance. Users can create multiple VPCs, for example, a VPC for production network and another VPC for non-production network so that production and non-production network are isolated from each other to achieve logical network segmentation. Besides, users can also create VSwitches in a VPC to partition a VPC into multiple subnets for different purpose e.g., testing and development. <u>Alibaba Cloud</u> The network area on Alibaba Cloud is generally divided into three layers from the outside to the inside in a hierarchical manner: - Layer 1: Region and zone - Layer 2: VPC - Layer 3: Subnet and resource perimeter Alibaba Cloud isolates production networks from non-production networks. Direct access from a non-

Key Aspects	Applicability	Consideration
		production network to any servers and network devices in a production network is not allowed. Alibaba Cloud isolates the cloud service network that provides services to external users from the physical networks that supports the underlying cloud service functionalities. Network access control lists (ACLs) are configured to prohibit access from cloud service network to physical network. Alibaba Cloud also takes network control measures to prevent unauthorized devices from connecting to the internal network of the cloud platform and prevent the physical servers of the cloud platform from initiating external connections. Alibaba Cloud deploys Bastion Host on production network boundaries. The O&M personnel in the office network can access the production network for O&M only through Bastion Host. When logging on to Bastion Host, O&M personnel must perform MFA, namely a one-time password is required apart from the regular domain account name and password. Bastion Host uses advanced encryption algorithms to ensure the confidentiality and integrity of data transmitted through O&M channels. To provide network connections for ECS instances, Alibaba Cloud connects the instances to the Alibaba cloud virtual network, which is a logical structure built on top of the physical network structure. All the logical virtual networks are isolated from each other to prevent the network traffic data from being snooped or intercepted by other malicious instances. Alibaba Cloud provides security groups to control access for ECS instances. ECS instances in

Key Aspects	Applicability	Consideration
		different security groups cannot communicate with each other by default, while security group rules can be configured to control network access over ECS instances.
Network Security	BSFIs & Alibaba Cloud - Guidelines on Information Technology Risk Management, Enhance Guidelines on Information Security Management	<u>BSFIs</u> FIs are responsible to evaluate and implement appropriate controls relative to the complexity of its network. <u>Alibaba Cloud</u> *<u>VPC</u>* Alibaba Cloud offers different cloud-based network solutions, for example, customers can create an independent VPC for each network partition. In each VPC, different vSwitches are created to handle different business requirements. VPC instances are logically isolated from another VPC instance. Customers can create a VPC for the production network and another VPC for the non-production network so that they are isolated from each other to achieve logical network segmentation. Different business systems, or different VPCs, can communicate with each other by using Cloud Enterprise Network (CEN). To meet the dedicated requirements of customers, customers can configure custom settings such as route table isolation, route filtering, and routing policies as needed. The following network partitions are commonly used: - Production and testing: The resources in the

Key Aspects	Applicability	Consideration
		production environment and test environment are deployed in two partitions. - Internet facing: This partition is similar to the DMZ in a data center. Internet egress resources, such as elastic IP addresses (EIPs), network address translation (NAT) gateways, SLB instances, and Cloud Firewall, are deployed in this partition. - Business-to-business: The external firewall or other protection devices in the intrusion detection system (IDS) or intrusion prevention system (IPS) in the cloud are deployed in this partition. - Internal O&M: The resources that enterprise employees use to connect to Alibaba Cloud are deployed in this partition. These resources can be jump servers and bastion hosts. - Internet access: The resources that are used to connect to external environments, such as third-party data centers, are deployed in this partition. *ECS* A security group is a virtual firewall provided by Alibaba Cloud for ECS instances. It provides Stateful Packet Inspection (SPI) and packet filtering functions, and can be used to isolate security domains between ECS instances (or container clusters in Container Service) on the cloud. Security groups are logically isolated groups of instances that are located within the same region and share the same security requirements while also being mutually accessible. Security groups are used for

Key Aspects	Applicability	Consideration
		network access control over one or more ECS instances. As an important means of security isolation, security groups logically isolate security domains on the cloud. *Cloud Firewall* Alibaba Cloud Firewall is the industry's first firewall as a service (FWaaS) solution targeted for public clouds. It centrally manages control policies for the access traffic from the Internet to ECS instances (Internet traffic), and provides micro-isolation policies for the access traffic between ECS instances (intranet traffic). This is because in a cloud environment, users not only need to manage boundaries between the Internet and the intranet, but also need to manage network boundaries between cloud products, between VPCs, and even between ECS instances. With Cloud Firewall, users can analyze Internet and intranet traffic, gain full visibility into network-wide traffic such as traffic between security groups and Internet access traffic, and analyze and block external connections. Based on traffic analysis, Cloud Firewall provides isolation and control at all levels of the entire network, including centralized control over public IP addresses, domain name-based access control, VPC-based isolation, and isolation of leased lines between Alibaba Cloud and on-premises data centers. Cloud Firewall also integrates IPS and threat intelligence capabilities for intrusion detection and analysis. By default, Cloud Firewall can also store

Key Aspects	Applicability	Consideration
		network traffic and security event logs and firewall operation logs for six months. *Anti-DDoS* Alibaba Cloud provides an Anti-DDoS solution that can mitigate transport layer DDoS attacks which detects attacks using forged source IP addresses to enter to AIs' internal network continuously and block the attack. Alibaba Cloud secures all data centers with a self-developed Anti-DDoS service that provides protection against all types of DDoS attacks. It uses an AI protection engine to accurately identify attack behaviors and automatically load protection rules, ensuring network stability. Alibaba Cloud Anti-DDoS allows users to monitor risks and protection status in real time through security reports. Alibaba Cloud Anti-DDoS not only supports mitigating DDoS threats for users' business on Alibaba Cloud, but also allows them to use Alibaba Cloud's globally distributed scrubbing centers and AI protection engine for on premise businesses, in order to mitigate high-volume DDoS attacks and provide fine-grained protection against resource exhaustion attacks at the web application layer. *Web Application Firewall (WAF)* WAF filters out a large number of malicious access attempts by defending against common security threats reported by OWASP, such as SQL injection, XSS, common vulnerabilities in Web server plug-ins, Webshell uploads, and unauthorized access to core resources. This prevents website asset leakage, thus safeguarding website security and availability.

Key Aspects	Applicability	Consideration
Virtualization Security	BSFIs & Alibaba Cloud - Enhance Guidelines on Information Security Management	BSFIs are responsible to extend security policies and standards to virtualized servers and environment. BSFIs may adopt the following control measures: - Hypervisor hardening with strict access controls and patch management; - Inspection of intra-host communications and ensuring that security control measures are implemented for confidential/sensitive data stored in virtual machines (VMs); and - VM creation, provisioning, migration, and changes should undergo proper change management procedures and approval processes similar to deployment of physical network/system devices and servers. BSFIs may also consider implementing next generation firewalls that can restrict access more granularly and prevent virtualization-targeted attacks that exploit known VM vulnerabilities and exploits. Alibaba Cloud **Tenant isolation** Based on the hardware virtualization technology, VMM allows VMs on multiple computing nodes to be isolated from each other at the system layer. It prevents unauthorized access to system resources between tenants and guarantees basic computing isolation between computing nodes. The virtualization management layer also provides storage isolation and network isolation. **Security hardening**

Key Aspects	Applicability	Consideration
		Alibaba Cloud uses a lightweight KVM-based hypervisor developed specifically for cloud computing. At the virtualization layer, the hypervisor substitutes a virtual device for its physical equivalent storage device. All the Input/Output (I/O) operations of a VM are intercepted by the hypervisor to ensure that the VM can only access the physical disk space allocated to it, thus implementing security isolation of hard disk space between different VMs. Alibaba Cloud hypervisor limits the number of calls to system-level dynamic libraries without affecting functionality or performance to reduce the potential impact of zero-day vulnerabilities. In summary, Alibaba Cloud minimizes the amount of code that is not related to devices on the cloud at the hypervisor level, therefore reducing the attack surface. In addition, all virtualization software must be compiled and run in a trusted execution environment to ensure that each binary file is not maliciously altered or replaced during runtime. Alibaba Cloud also hardens security at the hypervisor and host operating system (OS)/kernel levels. Alibaba Cloud continues to introduce new security features into the hypervisor and host OS/kernel, including the latest security features developed by Alibaba Cloud and the open source community. **Escape detection** The Alibaba Cloud hypervisor uses advanced VM distribution algorithms to prevent malicious VMs

Key Aspects	Applicability	Consideration
		from running on a targeted physical machine. VMs cannot proactively detect the physical host environment in which they are located. At the hypervisor level, Alibaba Cloud also detects abnormal VM behaviors (i.e. potential attack events) by performing the following operations: analyze and monitor Coredump files in real time, detect suspicious code snippets loaded and executed by the hypervisor in real time, audit VM calls to system functions and abnormal VM Exit behaviors, monitor and analyze possible abnormal behaviors such as irregular process execution and network behaviors of hosts. When an attack is detected, Alibaba Cloud locates and discards the VM that initiated the attack, reconstructs the attack chain in a timely manner, and performs hotfix patching on any discovered vulnerabilities. **Hotfix patching** Alibaba Cloud virtualization platform supports hotfix patching technology, which can fix system defects or vulnerabilities without user intervention, thus keeping any negative effects on user business operations to a minimum.
Security Risk Assessment	BSFIs - Guidelines on Information Technology Risk Management	BSFIs BSFIs are responsible to conduct security risk assessment in a regular basis.

Key Aspects	Applicability	Consideration
Application Whitelisting	BSFIs & Alibaba Cloud - Enhance Guidelines on Information Security Management	BSFIs BSFIs are responsible to adopt advanced security solutions such as application whitelisting to address the more sophisticated forms of malware. Application whitelisting allows only specified programs to run and/or sandboxing technologies which can inspect incoming traffic such as e-mail attachments without compromising the production environment. *Security Center* Security Center also allows users to add applications that run on their servers to an application whitelist. Security Center identifies applications as trusted, suspicious, or malicious based on the application whitelist to prevent unauthorized applications from running. Alibaba Cloud Alibaba Cloud monitors and manages a trusted application whitelist on security critical applications. The trusted computing technology can record and analyze the execution behaviors of an application, such as process startup, file access, and network access, and creates its behavior whitelist and model. When the application is running, the service dynamically measures the collected application behaviors and compares the measurement results with the permissible actions in the whitelist to determine whether the application can be trusted. Based on the verification results, the security O&M personnel can take measures such as reinstalling the correct application version.

Key Aspects	Applicability	Consideration
Training	BSFIs - Guidelines on Information Technology Risk Management, Enhance Guidelines on Information Security Management	BSFIs BSFIs are responsible to provide adequate training to their employees to raise their awareness of attacks.
Configuration Management	BSFIs & Alibaba Cloud - Guidelines on Information Technology Risk Management	BSFIs BSFIs are responsible to ensure that appropriate configuration management processes exist. BSFIs should establish security control requirements based on their risk assessment process evaluating the value of the information at risk and the potential impact of unauthorized access, damage or other threats. *Cloud Config* Cloud Config is an audit service for resources on the cloud. This service provides users with cross-region resource inventory and retrieval capabilities to record historical configuration snapshots of resources and form a configuration timeline. Cloud Config allows users to set compliance rules for the configuration of cloud resources. When a resource configuration change occurs, the compliance assessment is automatically triggered and an alert is issued for any "non-compliant" configuration. Cloud Config allows users to continuously monitor the

Key Aspects	Applicability	Consideration
		compliance of large volumes of resources to address internal and external compliance requirements. Alibaba Cloud Alibaba Cloud has established Alibaba Cloud Management Policy of Information Service Configurations and Assets to govern the configuration management process. All configuration changes must be well planned, assessed, tested and authorized before deployment by following the Alibaba Cloud Information Service Change Management Provision. The change process is standardized and is supported by automatic systems and tools. Any changes need to go through a series of phases from application, evaluation, approval, test and implementation. Change deployment is performed automatic tools in order to prevent unauthorised changes to firewall rules. Nevertheless, Alibaba Cloud deploys an automatic configuration check tool to verify the configurations of infrastructure e.g., firewall after a change in order to detect unauthorized configuration change.

▪ Domain 6 — Change Management

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the change management, including Normal Change and Emergency Change.

- 6.1 Normal Change

Key Aspects	Applicability	Consideration
Policies and Procedures	BSFIs & Alibaba Cloud - Guidelines on Information Technology Risk Management, Enhance Guidelines on Information Security Management	BSFIs BSFIs are responsible to ensure that the change management procedures are formalized, enforced and adequately documented. Authorization and approval are required for all changes and the personnel responsible for program migration should be identified. For the purpose of accountability, proper sign-off should be adequately implemented where formal acknowledgement is obtained from all related parties. Alibaba Cloud Alibaba Cloud establishes a comprehensive change management process based on ISO/IEC 20000, where changes are classified based on the degree of emergency and are managed by category based on their sources and targets. The criteria for judging possible outcomes from various changes are also clearly defined. The whole change process is standardized and is supported by automatic systems and tools. Any changes need to go through a series of phases from application, evaluation, approval, test, implementation, and finally to verification. The responsibilities of various personnel involved in the process are clearly defined. The following policies has been established by Alibaba Cloud to govern the procedure of new product development and change management: - Alibaba Cloud System Acquisition, Development, and Maintenance Management

Key Aspects	Applicability	Consideration
		Provision; - Alibaba Cloud New Service and Major Service Change Management Provision; - Alibaba Cloud Information Service Change Management Provision; - Public Cloud Change Management Guidelines; and - Alibaba Cloud Management Policy of Information Service Configurations and Assets.
Change Implementation	BSFIs & Alibaba Cloud - Guidelines on Information Technology Risk Management	<u>BSFIs</u> BSFIs are responsible to screen requested changes before acceptance to determine alternate methods of making the changes, the cost of changes and time requirements for programming activity. System analysts should assess the impact and validity of the proposed changes and all critical change requests should be set as priority. *<u>Cloud Config</u>* Cloud Config tracks the configuration of supported cloud services. After users activated Log Services (SLS), it allows users to deliver resource configuration changes logs to SLS and perform subsequent security analysis and monitoring. <u>Alibaba Cloud</u> The whole change process is standardized and is supported by automatic systems and tools. A change management system is deployed to ensure all changes are requested with a valid change ticket

Key Aspects	Applicability	Consideration
		and roles and responsibilities has been established in the above policies to ensure only authorized approvers can approve change request, further, there is system setting to prohibit the deployment of unauthorized change thus ensure only the approved code can be deployed to the production environment. Alibaba Cloud adopts a DevOps model to automate and streamline the change management process in order to deliver continuous services at higher velocity. Each of the stages of the change process is tracked via a centralized change management system, with status of each stage recorded and supporting documentation retained.
Change Monitoring	BSFIs & Alibaba Cloud - Guidelines on Information Technology Risk Management	BSFIs BSFIs are responsible to maintain audit trail of all change request. Programmers' activities should be controlled and monitored, and all jobs assigned should also be closely monitored against target completion dates. *ActionTrail* ActionTrail monitors and records the actions performed by Alibaba Cloud and RAM account, including the access to and use of cloud products and services. Users can either view the event records directly on the console of ActionTrail or monitored resource. *Application Configuration Management (ACM)* With ACM client, users can perform query of

Key Aspects	Applicability	Consideration
		historical versions of resource configuration and view the current configuration detail to ensure the configuration setting of end-of-life systems still meet users' security baseline. *Bastionhost* Bastionhost supports session audit, real-time monitoring as well as operating logs review so that administrator can monitor the activities performed by O&M users on the specific hosts. Alibaba Cloud Alibaba Cloud records all the information throughout the change process and deploys an automatic configuration check tool to verify the configurations of infrastructure and information systems after a change in order to detect unauthorized changes to software and hardware. Application submission of configuration change, documentation and approval, are managed and logged in the change management platform.
Segregation of Duties	BSFIs & Alibaba Cloud - Guidelines on Information Technology Risk Management	BSFIs Customers are responsible to ensure that roles and responsibilities of each relevant party, including IT functions and end-user departments, with adequate segregation of duties. This is to ensure that no single person can effect changes to the production environment without the review and approval of other authorized personnel.

Key Aspects	Applicability	Consideration
		Alibaba Cloud Segregation of duties is enforced within the change management process, where responsibilities for requesting, approving and implementing changes to the Alibaba Cloud production environment are segregated among different individuals, to ensure that only tested and approved changes are implemented in production.

- 6.2 Emergency Change

Key Aspects	Applicability	Consideration
Classification of Change	BSFIs & Alibaba Cloud - Guidelines on Information Technology Risk Management	Alibaba Cloud Changes are classified based on the degree of emergency as well as impact of potential system malfunctions and are managed by category based on their sources and targets. Based on the migration time, changes are categorized into normal changes and emergency changes. Normal changes are scheduled to be deployed during the pre-defined routine migration window whereas emergency changes are deployed outside of the routine migration window or during the network block period. Changes to Alibaba Cloud's products, supporting infrastructure, and networks are reviewed and approved by authorized personnel prior to deployment of changes into production. Product team is responsible to obtain approvals by alternative means, report the reason and submit

Key Aspects	Applicability	Consideration
		subsequent change requests in the system in case of emergency.
Emergency Change Implementation	BSFIs & Alibaba Cloud - Guidelines on Information Technology Risk Management	<u>BSFIs</u> BSFIs are responsible to establish formal procedures to manage emergency changes. Emergency changes should be approved by the information owner and other relevant parties at the time of change. If the change needs to be introduced as a matter of urgency and it is impracticable to seek the approval of the information owner, endorsement should be sought from the information owner after the implementation as soon as practicable. <u>Alibaba Cloud</u> Before changes are submitted for approval, they must pass testing with testing results documented. Code scanning is required for source code changes with the scanning results retained. Rollback plans are prepared and documented in case the implementor needs to revert back to the previous state. Prior to deployment of changes into production, a change request must be submitted in the centralized change management system where change type, risk level, risk description, change reason, change plan, rollback plan, and validation method are specified. Changes requests, including emergency change must be approved by authorized personnel before migration into the production environment.

Key Aspects	Applicability	Consideration
Emergency Change Monitoring	BSFIs & Alibaba Cloud - Guidelines on Information Technology Risk Management	Please refer to the above aspect of Change Monitoring in Domain 7.1 – Normal Change.

▪ Domain 7 — Patch Management

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the patch management.

- 7.1 Patch Management

Key Aspects	Applicability	Consideration
Patch Implementation	BSFIs & Alibaba Cloud - Guidelines on Information Technology Risk Management, Enhance Guidelines on Information Security Management	Responsibilities over patch management between Alibaba Cloud and customer have been defined in the Alibaba Cloud Security White Paper, which is publicly available for user entities on Alibaba Cloud official website. Alibaba Cloud detects vulnerabilities from internal and external sources so as to identify necessary patches and security updates in order to maintain secure cloud services and ensure patches and updates are assessed, tested before deploying to the production environment. BSFIs BSFIs are responsible to adopt a patch management process to promptly identify available security patches to technology and software assets, evaluate criticality and risk of patches, and test and deploy patches within an appropriate timeframe.

Key Aspects	Applicability	Consideration
		Security Center Based on the self-developed cross-platform vulnerability scanning and repair engine of Alibaba Cloud, Security Center allows users to scan multiple systems and applications, for example, Windows systems, third-party Linux versions for Alibaba Cloud, and mainstream CMS systems, and detect emergency vulnerabilities in systems or applications without relevant patches. *Cloud Firewall* Users can enable the Virtual Patch function under advanced setting of intrusion prevention feature provided by Cloud Firewall to receive hot patches at the network layer and automatically deploy the patches to protect cloud assets against high-risk vulnerabilities and emergency vulnerabilities that can be remotely exploited. Besides, users can also view the latest information about the updates of security intelligence, virtual patches, and basic IPS policies that posted on Cloud Firewall console to gain an overview for patch management. Cloud Firewall uses a customer engine under the Virtual Patch function to automatically receive hot patches at the network layer and deploy the patches to protect cloud assets against high-risk vulnerabilities and emergency vulnerabilities that can be remotely exploited. Customizations for virtual patch policies are allowed, for example, to manually enable or disable certain patches based on criticality.

Key Aspects	Applicability	Consideration
		Alibaba Cloud ACK ACK offers customers with higher reliability and security clusters in large-scale production environments and thus allowing to deploy patches to simulated environments in advance of official deployment. Alibaba Cloud Alibaba Cloud ensures the security of hardware, software, and network of the cloud platform by means of OS and database patch management, etc. Alibaba Cloud will identify and fix security vulnerabilities through hotfix dynamical patching technology in a timely manner without affecting customers' service availability.

▪ Domain 8 — Log Management

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the log management.

- 8.1 Log Management

Key Aspects	Applicability	Consideration
Log Management	BSFIs & Alibaba Cloud - Enhance Guidelines on Information Security Management	BSFIs BSFIs are responsible to implement processes to protect audit information and audit tools from unauthorized access, modification, and deletion. Audit records contain a set of data elements in order to support necessary analysis requirements. In addition, audit records are available to authorized

Key Aspects	Applicability	Consideration
		users for inspection or analysis on demand, and in response to security-related or business-impacting events. *SLS* Alibaba Cloud provides SLS as an observation and analysis platform that processes multiple types of data such as logs, metrics, and traces. Customers should review logs of physical and/or logical access following events. SLS is able to perform manual and automated correlation analysis. Logging practices and thresholds for security logging should be reviewed periodically to ensure that appropriate log management is in place. This could be done by using Log SLS along with using ActionTrail. *ActionTrail* Alibaba Cloud ActionTrail provides centralized log management for cloud resource operations. The logon and resource access operations performed under each account are recorded. An ActionTrail record includes information such as the operator, operation time, source IP address, resource object, operation name, and operation status. The operation records stored by ActionTrail can be used for security analysis, intrusion detection, resource change tracking, and compliance audit. In a compliance audit, users may need to provide detailed operation records for Alibaba Cloud accounts and RAM users. The operation events recorded by ActionTrail can meet these compliance audit requirements.

Key Aspects	Applicability	Consideration
		OSS Alibaba Cloud offers OSS that provides a secure and high-durability cloud storage service. Logs collected by SLS could ship to OSS for backup. Alibaba Cloud In Alibaba Cloud, all activities performed in production systems through bastion hosts are logged in real time and transferred to a central log management platform. The logs are retained for at least half a year and protected from modification or deletion. Monitoring rules are defined to perform automatic review of activities within the central log management platform. Automated alerts are generated based on the review results and sent to security team for investigation. Alibaba Cloud also utilizes a security incident monitoring platform to analyse the log of activities performed in production systems and identify abnormal user operations and security incidents based on the defined audit rules for violations. Security incidents are reviewed and monitored for resolution by security team.

▪ Domain 9 — Incident Management

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the incident management, including Policy and Procedure and Incident

Management.

- 9.1 Policy and Procedure

Key Aspects	Applicability	Consideration
Policy and Procedure	BSFIs & Alibaba Cloud - Guidelines on Information Technology Risk Management, Enhance Guidelines on Information Security Management	BSFIs BSFIs are responsible to establish incident response and reporting procedures to handle IS-related incidents. Alibaba Cloud - The following policies are established to govern the incident management: Emergency Response Standard of Security Incidents; - Malfunction Management Standard; - Incident response procedures. Alibaba Cloud security team is responsible to initiate the incident response process and follow the standard protocols.

- 9.2 Incident Management

Key Aspects	Applicability	Consideration
Incident Detection	BSFIs & Alibaba Cloud - Guidelines on Information Technology Risk Management	BSFIs BSFIs are responsible to design and implement effective detection controls over its networks, critical systems and applications, access points, and confidential information. Detection controls should provide alerts and notifications for any anomalous activities within its network that can potentially impair the confidentiality, integrity, and availability of information assets.

Key Aspects	Applicability	Consideration
		Alibaba Cloud Alibaba Cloud conducts security monitoring on the cloud platform to promptly discover security incidents in which platform resources such as applications, hosts, and networks are attacked, and then trigger the internal incident response process to properly handle the incidents and eliminate potential impact. Internally, Alibaba Cloud discovers possible security incidents through log collection, anomaly analysis and detection, and alert generation. The external reporting channels include Alibaba Security Response Center (ASRC), Alibaba Cloud Crowdsourced Security Testing Platform, externally reported Common Vulnerabilities and Exposures (CVE) vulnerabilities of open source third-party components, and threat intelligence information from third parties.
Incident Response	BSFIs & Alibaba Cloud - Guidelines on Information Technology Risk Management, Enhance Guidelines on Information Security Management	BSFIs BSFIs are responsible to develop and implement a formal incident response plan to address identified information security incidents in a timely manner. Alibaba Cloud Alibaba Cloud will respond to security incidents and vulnerabilities as soon as they are discovered. The incident response team will first verify the authenticity of the reported vulnerabilities and security incidents. Once the vulnerabilities and

Key Aspects	Applicability	Consideration
		security incidents are confirmed, Alibaba Cloud security team will initiate the incident response process and follow the standard protocols. The security severity level and impact scope of a vulnerability will be confirmed, and the response team will ensure resources are properly allocated so that the vulnerability can be fixed and the affected Alibaba Cloud product can be brought online within the corresponding SLA time. Alibaba Cloud security team will initiate the incident response process and follow the standard protocols. The security severity level and impact scope of a vulnerability will be confirmed, and the response team will follow the steps to handle a security incident including, confirming the impact scope of the incident, eliminating the impact, reviewing the incident, and making subsequent improvements. To ensure the effectiveness of the incident response process, Alibaba Cloud has set up a dedicated team to conduct attack drills from time to time. Alibaba Cloud also regularly invites third-party teams to conduct penetration testing on the Alibaba Cloud platform to verify the effectiveness of the Alibaba Cloud security protection system and the reliability of the incident response process.
Training	BSFIs & Alibaba Cloud - Guidelines on Information Technology Risk Management, Enhance	Alibaba Cloud In Alibaba Cloud, security coordinators in each department are responsible for implementing information security mechanism defined in the guideline, including monitoring security incidents in daily work, coordinating information security

Key Aspects	Applicability	Consideration
	Guidelines on Information Security Management	awareness training, coordinating resources to support information management internal audit, risk assessment and other relevant information security trainings.
Notifications to the Authorities	BSFIs - Enhance Guidelines on Information Security Management, Technology and Cyber-Risk Reporting and Notification Requirement	BSFIs BSFIs are responsible to report the incidents to the Authorities.
Notifications to their Customers	BSFIs & Alibaba Cloud - Enhance Guidelines on Information Security Management	BSFIs BSFIs are responsible to communicate with affected parties, including customers. *Short Message Service (SMS)* SMS, as a communication channels, supports users to deliver their designated messages when incident happens to designated parties by pushing notification through SMS. *Direct Mail* Direct Mail also allows users to inform the relevant parties of the key facts relating to the incidents through batch emails Alibaba Cloud Alibaba Cloud will respond to security incidents and

Key Aspects	Applicability	Consideration
		vulnerabilities as soon as they are discovered. The incident response team will first verify the authenticity of the reported vulnerabilities and security incidents. Once the vulnerabilities and security incidents are confirmed, Alibaba Cloud security team will initiate the incident response process and follow the standard protocols to confirm the security severity level and impact scope of a vulnerability. The response team will ensure resources are properly allocated so that the vulnerability can be fixed, and the affected Alibaba Cloud product can be brought online within the corresponding SLA time. The incident response team will also promptly notify users of security issues through online announcements. Alibaba Cloud has established multi-channel communication methods to announce malfunctions or security incidents that could impact customers. The method includes announcements via Alibaba Cloud official website, station letters, SMS, e-mails and DingTalk messages. Customers can request for detail of incident summary.
Root Cause Analysis	BSFIs & Alibaba Cloud - Guidelines on Information Technology Risk Management, Enhance Guidelines on Information	BSFIs BSFI are responsible to minimize and contain the damage and impact arising from security incidents, immediately restore critical sytems and services, and facilitate investigation to determine root causes. Alibaba Cloud Alibaba Cloud Security Team will investigate

Key Aspects	Applicability	Consideration
	Security Management, Technology and Cyber-Risk Reporting and Notification Requirement	incident root cause through collecting and analyzing information from multiple sources. Incident review is also conducted to propose recommendation so as to prevent the same incident to happen again. Security team organizes monthly team meetings to perform root cause analysis for malfunctions that occurred in the past one month and discuss resolution status with business leadership and project managers.
Forensic Management	BSFIs & Alibaba Cloud - Guidelines on Information Technology Risk Management, Enhance Guidelines on Information Security Management	BSFIs BSFIs are responsible to implement appropriate controls to facilitate forensic investigation of incidents. Policies on system logging should be established covering the types of logs to be maintained and their retention periods. Where a follow-up action against a person or organization after an information security incident involves legal action, evidence shall be collected, preserved, and presented to conform to the relevant rules for evidence. BSFIs should define in the response plan a systematic process for recording and monitoring information security incidents to facilitate investigation and subsequent analysis. Adequate documentation should be maintained for each incident from identification to closure. Facts about the incident, operational impact, estimated cost, investigation findings, and actions taken should be consistently documented. Automated means of reporting and tracking of incidents may be

Key Aspects	Applicability	Consideration
		implemented for analysis and preparation of reports to support decision-making. *SLS* Alibaba Cloud provides SLS as an observation and analysis platform that processes multiple types of data such as logs, metrics, and traces. Customers should review logs of physical and/or logical access following events. SLS is able to perform manual and automated correlation analysis. Logging practices and thresholds for security logging should be reviewed periodically to ensure that appropriate log management is in place. This could be done by using SLS along with using ActionTrail. *ActionTrail* Alibaba Cloud ActionTrail provides centralized log management for cloud resource operations. The logon and resource access operations performed under each account are recorded. An ActionTrail record includes information such as the operator, operation time, source IP address, resource object, operation name, and operation status. The operation records stored by ActionTrail can be used for security analysis, intrusion detection, resource change tracking, and compliance audit. In a compliance audit, users may need to provide detailed operation records for Alibaba Cloud accounts and RAM users. The operation events recorded by ActionTrail can meet these compliance audit requirements. *OSS*

Key Aspects	Applicability	Consideration
		Alibaba Cloud offers OSS that provides a secure and high-durability cloud storage service. Logs collected by SLS could ship to OSS for backup. Alibaba Cloud Alibaba Cloud utilizes a security incident monitoring platform to analyze the log of activities performed in production systems and identify abnormal user operations and security incidents based on the defined audit rules for violations. Security incidents are reviewed and monitored for resolution by security team. Incident response team administers and operates the incident management platform, which consolidate, and track incident discovered via the customer ticketing system, product service monitoring system as well as incident reported by internal employees. All activities performed in production systems through bastion hosts are logged in real time and transferred to a central log management platform. The logs are retained for at least half a year and protected from modification or deletion. Monitoring rules are defined to perform automatic review of activities within the central log management platform. Automated alerts are generated based on the review results and sent to security team for investigation. Alibaba Cloud also utilizes a security incident monitoring platform to analyse the log of activities

Key Aspects	Applicability	Consideration
		performed in production systems and identify abnormal user operations and security incidents based on the defined audit rules for violations. Security incidents are reviewed and monitored for resolution by security team.

▪ Domain 10 — Data Center Management

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the data center management.

- 10.1 Data Center Management

Key Aspects	Applicability	Consideration
Environmental Control	Alibaba Cloud - Guidelines on Information Technology Risk Management, Enhance Guidelines on Information Security Management	Alibaba Cloud Alibaba Cloud implements environmental controls at data centers including heating, ventilation, and air conditioning (HVAC), lightning protection systems, fire detection and suppression systems, and power management systems. **Fire detection and response** For fire detection and response, Alibaba Cloud data centers are equipped with fire detection systems that utilize thermal and smoke sensors. The sensors are fitted to the ceiling and floor and give audible and visual alarms when triggered. Each data center is equipped with an integrated gas extinguishing system and fire extinguishers. Data center personnel also undergo fire detection and response training on a regular basis. **Power** For power supply, to achieve a 24/7 uninterrupted

Key Aspects	Applicability	Consideration
		service, Alibaba Cloud data centers are powered by dual main supplies and redundant power systems. The primary and secondary power supplies and systems have the same power supply capabilities. In case of a power failure, redundant battery packs and diesel generators are enabled to power data center devices, thus allowing the data center to run continuously for a certain period of time. **Temperature and humidity** For temperature and humidity, Alibaba Cloud data centers are fitted with precision air conditioners to ensure constant temperature and humidity levels, which are electronically monitored. In case of any fluctuation in temperature or humidity outside of the normal range, an alarm is triggered and corrective actions are immediately taken. All air conditioning units work in hot standby mode. **Equipment Monitoring System** Nevertheless, an equipment monitoring system is utilized to monitor the environment of data centers and performance of servers. In case of any exception, an alert is triggered automatically by the system and Alibaba Cloud on-site operators will follow up with the data center service providers to resolve the issue. Alibaba Cloud adopts industry standards and best practices to safeguard customer data. Alibaba Cloud has received multiple industry standard certifications, including ISO27001, Service Organization Control (SOC) 1/2/3 and etc. and regularly complete third-party audits.

Key Aspects	Applicability	Consideration
Selection of Location	BSFIs - Guidelines on Information Technology Risk Management	BSFIs BSFIs are responsible to fully consider the environmental threats when selecting the locations of its data centers. Alibaba Cloud is dedicated to providing stable and reliable computing and data processing capabilities and enabling an interconnected world. Alibaba Cloud has 71 availability zones in 25 regions across the globe from the west to east. Customers are suggested to select a region that is the closest to the geographical location of the customers' sites to speed up the cloud access.

Domain 11 — Capacity Management

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the capacity management, including Capacity Planning and Capacity Monitoring.

- 11.1 Capacity Planning

Key Aspects	Applicability	Consideration
Capacity Planning	BSFIs - Guidelines on Information Technology Risk Management	BSFIs BSFIs are responsible to establish capacity planning of the critical online systems and processes.

- 11.2 Capacity Monitoring

Key Aspects	Applicability	Consideration
Capacity	BSFIs & Alibaba	BSFIs

Key Aspects	Applicability	Consideration
Monitoring	Cloud - Guidelines on Information Technology Risk Management	BSFIs are responsible to monitor IT resources for capacity planning including platform processing speed, core storage for each platform's central processing unit, data storage, and voice and data communication bandwidth. *CloudMonitor* Alibaba Cloud provides CloudMonitor to automatically retrieves and monitor cloud service resource under the current Alibaba Cloud account. Users can monitor different server performance metrics in ECS instance, server machines provided by other vendors and different cloud products through CloudMonitor, such as: vCPU utilization, average system loads, in ECS monitoring services or CloudMonitor host monitoring services for capacity forecasting. Users can view the monitoring data in CloudMonitor console, threshold-triggered alert can also be configured in CloudMonitor for users to real-time get notified through email/ IM when certain conditions of the monitoring metric hits. Alibaba Cloud Alibaba Cloud processes and analyzes the logs from different monitoring sources, for example, network monitoring platform through security monitoring algorithms in each computing platform to monitor the performance.

- ## Domain 12 — Business Continuity Management

This section outlines how Alibaba Cloud could offer help to the customers in compliance of the relevant requirements on the business continuity management, including Policy and Procedure, Business Continuity Management and Disaster Recovery.

- 12.1 Policy and Procedure

Key Aspects	Applicability	Consideration
Policy and Procedure	BSFIs & Alibaba Cloud - Guidelines on Business Continuity Management	BSFIs BSFIs are responsible to adopt a cyclical, process-oriented Business Continuity Management framework which should cover each business function and the technology that supports it. Other related policies, standards, and processes should also be integrated in the overall Business Continuity Management framework. Alibaba Cloud Alibaba Cloud has established Alibaba Cloud Business Continuity Management Policy to govern business continuity management. The policy defines roles and responsibilities for relevant parties, Business Continuity Management operation model, Business Continuity Management policies, risk tolerance level, Business Continuity Management objectives, Business Continuity Management evaluation and improvement, and management's responsibilities in resource management and personnel training.

- 12.2 Business Continuity Management

Key Aspects	Applicability	Consideration
Business Impact Analysis (BIA)	BSFIs & Alibaba Cloud - Guidelines on Business	BSFIs BSFIs are responsible to ensure a comprehensive BIA is undertaken to serve as the foundation in the

Key Aspects	Applicability	Consideration
	Continuity Management	development of the plan. <u>Alibaba Cloud</u> Alibaba Cloud's business continuity management team performs BIA and risk assessment on an annual basis, including identification of critical business processes, maximum tolerable period of disruption, recovery time objectives, minimum service levels and time needed to resume services. Results of the BIA and risk assessment are documented in the Alibaba Cloud Business Continuity Management - BIA, Risk Assessment, and Strategy Report. Threats that may cause disruption to Alibaba Cloud's critical business operations are identified and documented, and corresponding strategies are developed for different scenarios of disruptions.
Cyber Risk Assessment	BSFIs - Guidelines on Business Continuity Management	<u>BSFIs</u> BSFIs are responsible to conduct risk assessment incorporating the results of the BIA and evaluating the probability and severity of a wide-range of plausible threat scenarios in order to come up with recovery strategies that are commensurate with the nature, scale, and complexity of its business functions.
Formation of BCP	BSFIs & Alibaba Cloud - Guidelines on Business	<u>Alibaba Cloud</u> Alibaba Cloud's information technology management system working group will form a

Key Aspects	Applicability	Consideration
	Continuity Management	business continuity report based on the BIA and risk assessment results and then submit to the Information Technology Management System leading group for review. BCPs have been established in Alibaba Cloud to document the roles and responsibilities of staff in BCP which covering the scenario of products related and after-sales incident and defined the corresponding recovery time/points objectives. Alibaba Cloud maintains an effective BCP to augment the entity's cyber resilience in accordance with International Organization for Standardization (ISO) 22301 with independent audit by third party conducted at least on an annual basis.
Testing of BCP	BSFIs & Alibaba Cloud - Guidelines on Business Continuity Management	BSFIs BSFIs are responsible to conduct tests periodically, with the nature, scope, and frequency determined by the criticality of the applications, business processes, and support functions. In some cases, plan tests may be warranted due to changes in BSFI's business, responsibilities, systems, software, hardware, personnel, facilities, or the external environment. Alibaba Cloud Alibaba Cloud conducts testing of the BCPs established for Alibaba Cloud critical services and operations at least once a year. Alibaba Cloud also conducts testing of data center

Key Aspects	Applicability	Consideration
		BCPs with data center service providers at least once a year.
Training	BSFIs & Alibaba Cloud - Guidelines on Business Continuity Management	BSFIs BSFIs are responsible to provide annual cybersecurity training includes cyber incident response, current cyber threats, and emerging issues. Alibaba Cloud Alibaba Cloud establishes Alibaba Cloud Security Management Policy of Human Resources to regulate the requirement of information security awareness training for new employees and third-party personnel. Information and data security online training and assessments are required to be completed by all existing employees on an annual basis. Professional training includes skill sharing across teams via an online learning platform; offline training and communication meetings held by internal and external senior experts are available to employees.
Cyber resilience	BSFIs - Guidelines on Business Continuity Management, Enhance Guidelines on Information	BSFIs BSFIs are responsible to ensure the cybersecurity strategy can augment its cyber resilience. BSFIs are responsible to utilize the highly available and multi-replica data redundancy features offered by Alibaba Cloud’s products to ensure vital records

Key Aspects	Applicability	Consideration
	Security Management	are available and accessible in the event of disruption. SLB is a load balancing service that distributes traffic among multiple ECS instances. It improves the service capabilities of applications. Customers can use SLB to prevent single points of failure (SPOFs) and improve the availability of their applications. SLB is designed with full redundancy to avoid SPOFs, and supports zone-disaster recovery. By integrating with Alibaba Cloud DNS, SLB can achieve geo-disaster recovery with an availability of up to 99.95%. SLB supports auto scaling based on application workloads and provides continuous services even when traffic fluctuates. SLB is available in multiple zones in most regions to achieve zone-disaster recovery objectives. If the primary zone becomes unavailable, SLB can switch its service to a secondary zone in as little as 30 seconds and resume provisioning services. After the primary zone recovers, SLB would automatically switch back to the primary zone. The SLB service inspects the health status of ECS instances. If an ECS instance is found in an abnormal state, the service will isolate the instance by not forwarding traffics to it until it recovers. In this way, SLB eliminates SPOFs and improves the service capabilities of applications. Alibaba Cloud provides the layer-4 and layer-7 load balancing services. Layer 4 service uses an

Key Aspects	Applicability	Consideration
		optimized and customized version of the open source software Linux Virtual Server (LVS) and Keepalived to achieve load balancing. Layer 7 service uses Tengine, a web server project based on Nginx, to achieve load balancing. When combined with Alibaba Cloud Security, SLB can defend against DDoS attacks in near real time. Additionally, the Layer 7 load balancing service provides the ability to defend against HTTP/S Flood attacks.
Insurance	BSFIs - Guidelines on Information Technology Risk Management, Guidelines on Business Continuity Management	BSFIs BSFIs are responsible to purchase insurance to cover the potential loss during the service interruption.

- 12.2 Disaster Recovery

Key Aspects	Applicability	Consideration
Alternate recovery site	BSFIs & Alibaba Cloud - Guidelines on Information Technology Risk Management, Guidelines on Business Continuity	BSFIs BSFIs are responsible to make arrangements for alternate and recovery sites for their business functions and technology in the event the business premises, key infrastructure and systems supporting critical business functions become unavailable. A recovery site geographically separate from the primary site must be established to enable the

Key Aspects	Applicability	Consideration
	Management	restoration of critical systems and resumption of business operations should a disruption occur at the primary site. Alibaba Cloud offers high available cloud computing infrastructure by setting up cloud data centers across multiple regions and zones globally to ensure cloud products and services are highly available and provide multi-replica data redundancy. Besides, Alibaba Cloud provides different solution to customers to complement their business continuity and disaster recovery planning. Customer can deploy cloud systems across regions and zones to implement a high availability architecture, such as zone active-active architecture, geo-disaster recovery architecture, active geo-redundancy architecture, and disaster recovery architecture that spans three data centers across two regions. In case of failure in the primary zone, the system immediately switches the workloads to another zone.
Formation of Technology Recovery Plan	BSFIs & Alibaba Cloud - Guidelines on Information Technology Risk Management	BSFIs BSFIs are responsible to specify the technology requirements that are needed during recovery for individual business and support functions when the recovery strategies for the functions are determined. Appropriate personnel should be assigned with the responsibility for technology recovery. Alternate personnel needs to be identified for key technology recovery personnel in case of their unavailability to

Key Aspects	Applicability	Consideration
		perform the recovery process. Alibaba Cloud Alibaba Cloud has established Alibaba Cloud Business Continuity Management Policy to provide guidelines on business continuity management. A Business Continuity Management framework has been established under this policy, which consists of BIA, risk assessment, business continuity management report, as well as maintenance, implementation, testing and continuous improvement of Emergency Response Plan and BCP. BCPs have been documented with purpose, scope, roles and responsibilities, recovery objectives, maintenance of contact lists, emergency response, recovery plan, and incident response plan defined. The BCPs are reviewed on an annual basis and updated as needed.
Disaster Recovery Testing	BSFIs & Alibaba Cloud - Guidelines on Information Technology Risk Management	BSFIs BSFIs are responsible to engage in the design and execution of comprehensive test cases so as to obtain assurance that recovered systems function accordingly. Customers should also participate in disaster recovery tests of systems hosted overseas. Periodic testing and validation of the recovery capability of backup media should be carried out and assessed for adequacy and effectiveness. Alibaba Cloud

Key Aspects	Applicability	Consideration
		Alibaba Cloud conducts testing of data center BCPs with data center service providers at least once a year to verify the effectiveness of Internet Data Centre (IDC) contingency plan.
System Backup	BSFIs & Alibaba Cloud - Guidelines on Information Technology Risk Management	BSFIs BSFIs are responsible to ensure that sufficient number of backup copies of essential business information, software and related hardcopy documentations are available for restoration or critical operations. A copy of these information, documentation and software should also be stored in an off-site premise or backup site and any changes should be done periodically and reflected in all copies. SLB is a load balancing service that distributes traffic among multiple ECS instances. It improves the service capabilities of applications. Customers can use SLB to prevent single points of failure (SPOFs) and improve the availability of their applications. SLB is designed with full redundancy to avoid SPOFs, and supports zone-disaster recovery. By integrating with Alibaba Cloud DNS, SLB can achieve geo-disaster recovery with an availability of up to 99.95%. SLB supports auto scaling based on application workloads and provides continuous services even when traffic fluctuates. SLB is available in multiple zones in most regions to

Key Aspects	Applicability	Consideration
		achieve zone-disaster recovery objectives. If the primary zone becomes unavailable, SLB can switch its service to a secondary zone in as little as 30 seconds and resume provisioning services. After the primary zone recovers, SLB would automatically switch back to the primary zone. The SLB service inspects the health status of your ECS instances. If an ECS instance is found in an abnormal state, the service will isolate the instance by not forwarding traffics to it until it recovers. In this way, SLB eliminates SPOFs and improves the service capabilities of applications. Alibaba Cloud provides the layer-4 and layer-7 load balancing services. Layer 4 service uses an optimized and customized version of the open source software Linux Virtual Server (LVS) and Keepalived to achieve load balancing. Layer 7 service uses Tengine, a web server project based on Nginx, to achieve load balancing. When combined with Alibaba Cloud Security, SLB can defend against DDoS attacks in near real time. Additionally, the Layer 7 load balancing service provides the ability to defend against HTTP/S Flood attacks. Alibaba Cloud Alibaba Cloud offers ECS which allows customers to back up system disk or data disk with snapshot manually or automatically so that customers can roll back a disk to a previous state with a corresponding snapshot when incident happen. Else, customers can also back up image that contains all the data

Key Aspects	Applicability	Consideration
		from one or more disk (a system disk or both system and data disk) so that the image can be used to create an ECS instance with the same operating system and data environment when incident happens. ECS Images can be copied across different regions for remote backup through the image copy function of ECS.
Data Backup	BSFIs & Alibaba Cloud - Guidelines on Information Technology Risk Management	BSFIs BSFIs are responsible to back-up and store its data and program files in a secure off-site location to allow restoration of systems, applications, and associated data in the event normal processing is disrupted by a disaster or other significant event. Alibaba Cloud Alibaba Cloud employs distributed storage. Files are split into multiple data segments and stored on different devices. Each data segment is stored in multiple replicas. Distributed storage improves data reliability and security. Based on product types/tiers and business needs, Alibaba Cloud products also provide multiple protection capabilities such as multi-copy redundancy, system backup, live migration, load balancing, and anti-DDoS to ensure high data availability. Critical Alibaba Cloud system components are backed up at full at least twice a week and are replicated across multiple Availability Zones. Backup restoration procedures are in place. Critical Alibaba Cloud system components are restored on a

Key Aspects	Applicability	Consideration
		monthly basis and reconciliation is performed automatically for data integrity check. Backups of critical Alibaba Cloud system components are monitored by the system. In cases of backup errors or failures, a full backup is automatically triggered until the backup is completed successfully. *ECS* ECS supports full and incremental system disk or data disk backup with snapshot manually or automatically so that users can roll back a disk to a previous state with a corresponding snapshot. ECS also allows to backup image that contains all the data from one or more disk (a system disk or both system and data disk) so that the image can be used to create an ECS instance with the same operating system and data environment when incident happens. *Apsara DB for RDS* RDS supports data and log backup to ensure users can restore their database when incident or disaster happens. RDS supports automatic and manual backup. When users specify automatic backup, RDS will perform full physical backup automatically. RDS also supports manual backup, so that users can specify the following policies: full physical backups, full logical backups, and single-database logical backups. Alibaba Cloud offers Apsara DB for RDS that allows cross-region disaster recovery backup service is

Key Aspects	Applicability	Consideration
		supported by RDS instances for designated High-availability Editions. Besides, Alibaba Cloud offers OSS that allows remote backup for data stored in OSS through the purchase of cross-region data duplication services. *Data Backup Service (DBS)* Also, DBS supports full and incremental for logical and physical backup method. Logical backup is performed by backing up database objects such as tables, indexes, and stored procedures while physical backup is performed by backing up database files on the operating system.

4. Next Steps with Alibaba Cloud

Alibaba Cloud empowers customers to deploy on a trusted and high-performance cloud architecture worldwide. As a globally recognized industry-leading cloud service provider, we have been partners with many banking institutes in their cloud strategy, governance, and adoption processes.

To ensure on-going regulatory compliance and to fulfill their own risk management duty of care, financial institutions must make changes to the existing strategy, governance, policies, operating model, processes when adopting cloud services. The level of necessary change though will be on a sliding scale relative to the architectures deployed and the criticality of workloads hosted in the cloud environment. We provide professional services to assist the planning, design, execution and evaluation processes. (See “Useful Resource – 4. Alibaba Cloud Professional Services”).

While the Alibaba Cloud official website and this user guide facilitate a wealth of information relevant to your considerations, our sales representative should undoubtedly be able to assist you to address your concerns. In case we are not already in touch, please reach us at https://www.alibabacloud.com/contact-sales. We look forward to partnering with your organization to enable your digital transformation and IT modernization journey.

5. Useful Resource

1. Alibaba Cloud Security & Compliance Center
2. Alibaba Cloud Security Whitepaper, Version 2.0
3. Alibaba Cloud Legal Document Center
4. Alibaba Cloud Professional Services

6. Version History

December 2021: First Edition – Version 1.0