Alibaba Cloud User Guide

HKMA Cyber Resilience Assessment Framework (C-RAF) 2.0

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. Overview

Alibaba Cloud provides a comprehensive suite of global cloud computing services to help power and grow customers' business worldwide. Hong Kong, being one of the international financial centers, is strengthening its competitive advantages through promoting FinTech investments. Alibaba Cloud serves the customers from financial industries in Hong Kong to support their rising demands in digital transformation.

The Hong Kong Monetary Authority (HKMA), who is the primary banking regulator in Hong Kong, has published the revised Cyber Resilience Assessment Framework Version 2.0 (C-RAF 2.0), which is one of the three components of Cyber Fortification Initiative (CFI) announced by the HKMA in November 2020 that aims at further strengthening the cyber resilience of authorized institutions (AIs) in Hong Kong. The C-RAF2.0 is a revised structured assessment framework for AIs to assess their inherent risks and the maturity levels of their cybersecurity measures against a set of principles set out in the C-RAF 2.0, called "control principles" (CPs), which AIs governed by HKMA are expected to adhere.

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. We have worked with financial institutions in Hong Kong to integrate cloud computing technologies into their IT governance and business operations; this has helped them to become more flexible, improve operational efficiency and achieve their strategic objectives as well as comply with the applicable CPs set out in C-RAF 2.0.

The Alibaba Cloud User Guide on C-RAF 2.0 (the Whitepaper) aims to serve as a reference guide to introduce the key practices adopted by Alibaba Cloud to fulfill cloud service provider's responsibilities and the cloud computing offering to assist AIs in compliance with the relevant CPs.

2. Introduction

What is C-RAF 2.0?

To further strengthen the cyber resilience of AIs in Hong Kong, the HKMA developed the CFI in December 2016, comprising three pillars, namely:

(i) Cyber Resilience Assessment Framework;

(ii) Cyber Intelligence Sharing Platform; and

(iii) Professional Development Program (PDP).

In particular, C-RAF comprises the following elements:

i. Inherent Risk Assessment;

ii. Maturity Assessment; and

iii. Intelligence-led Cyber Attack Simulation Testing (iCAST).

AIs had largely completed one round of their C-RAF assessments by late 2019 i.e., C-RAF 1.0. In the light of that and recent international developments in cybersecurity, the HKMA conducted a holistic and independent review of the CFI. Industry consultation was conducted in the first half of 2020. The C-RAF has been developed and further enhanced taking into account various overseas practices and regulations, market conditions in Hong Kong, and feedback obtained from the industry consultation in the first half of 2020. As a result, the HKMA launched CFI 2.0 with enhanced C-RAF 2.0 to assist AIs in strengthening overall cyber resilience.

In order to perform assessment with reference to C-RAF 2.0, AIs are required to assess and ascertain its inherent risk rating through performing an Inherent Risk Assessment. The inherent risk rating is then mapped to its respective maturity level of cyber resilience. Based on their maturity level of cyber resilience, AIs should assess and determine the actual maturity level of its cyber resilience by performing the Maturity Assessment. Any gaps identified between the expected level and the actual level of maturity of cyber resilience can be identified from the assessment with CPs set out across 26 components under 7 domains during the maturity assessment. For gaps identified, they should be marked for improvement, so that the AIs can further enhance its cyber resilience to achieve the appropriate level of maturity expected by the HKMA. Nevertheless, for AIs aim to attain the “intermediate” or “advanced” maturity level are required to conduct the

intelligence-led Cyber Attack Simulation Testing ("iCAST"), where AIs are required to apply a risk-based approach to identify the attack scenarios relevant to their institution, and ensure they are tested under the iCAST exercise to simulate real-life attacks conducted by competent adversaries.

Why is it relevant to AI?

The C-RAF is a structured assessment framework by which AIs can assess their inherent risk and the maturity level of their cybersecurity measures against a set of CPs. Through this process, AIs should be able to better understand, assess, strengthen, and continuously improve their cyber resilience. The objective of the CFI is to increase AIs' cyber resilience and the overall banking stability of Hong Kong without sacrificing productivity.

According to the expectation of the HKMA, assessments with reference to C-RAF should be generally conducted on a three-year frequency basis. AIs should also proactively evaluate whether more frequent assessments are needed taking into account factors that could affect its threat profile, such as the inherent risk rating, changes to the AI's business nature or new emerging technology adoption. By using a risk-based approach, AIs rated with high inherent risk should consider assessment with a review cycle of less than 3 years.

Given that the purpose of the Maturity Assessment allows AI to identify gaps and areas for improvement to facilitate continuous improvement process of AI in improving its cyber resilience to an appropriate level. The C-RAF has therefore been established to minimize repetitive and disruptive actions and assists AIs to identify control gaps (if any) and develop remediation and enhancement actions on cyber resilience to reduce cybersecurity risks.

How Alibaba Cloud assist AI in complying with C-RAF 2.0?

Alibaba Cloud has worked with some financial institutions in Hong Kong to help them gain more flexibilities, improve operational efficiencies, achieve strategic objectives by integrating cloud computing technologies into their IT governance and business operations. Alibaba Cloud offers integrated cloud solutions to the financial customers in Hong Kong so that AIs can enjoy various advantages in cloud adoption:

Accelerate resource delivery and increase business agility

If AIs deploy their applications in conventional data centers, resource procurement may take one or more months. When it comes to globalization, data center planning can take a few years. However, the delivery efficiency of resources in the cloud is almost real-time.

Reduce costs

Cloud computing transforms the way in which IT assets are billed from the capital expenditures (CAPEX) model to the operating expenses (OPEX) model. In this case, the upfront investment that enterprises need to make on IT resources is reduced. In addition, Enterprises can purchase the required resources in pay-as-you go mode to reduce costs.

Use the latest cloud technologies

Cloud service providers usually make huge investments in their services and technologies. As a result, the cloud services provided by such cloud service providers are state-of-the-art in the industry. For example, the service providers can provide cloud-native services, such as containers and middleware.

Enhance service security

Cloud service providers usually offer online services at a large scale. In terms of online security, cloud service providers can help customers protect their applications against attacks over the internet.

Alibaba Cloud strives to provide customers with consistent, reliable, secure, and compliant cloud computing services, helping customers to protect the confidentiality, integrity, and availability of their systems and data in turn ensure cybersecurity without compromising security. This Whitepaper is developed to focus on Maturity Assessment of C-RAF 2.0. and illustrate how Alibaba Cloud services can help AIs to meet relevant CPs set out in C-RAF 2.0 Maturity Assessment matrix, as well as highlight the key features of Alibaba Cloud product for its compliance which customers can use, to evaluate, meet, and demonstrate compliance with C-RAF 2.0.

3. Compliance User Guide

Scope of Maturity Assessment

A Maturity Assessment matrix has been developed by the HKMA which sets out the CPs that AIs should comply in order to achieve a particular maturity level for that component. The Maturity Assessment matrix comprises covers 7 domains:

- Governance;
- Identification;
- Protection;
- Detection;
- Response and recovery;
- Situational awareness; and
- Third-party risk management.

These above domains can be further categorized into three levels: governance; the internal environment; and the external environment. Hence, the Maturity Assessment is designed to assist AIs to conduct a comprehensive review of the governance environment and the cyber resiliency in coping internal and external risks and threats.

Shared Security Responsibilities

It is important for customers to note that Alibaba Cloud employs a shared responsibility model, meaning that the security of applications built, and architecture hosted 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.

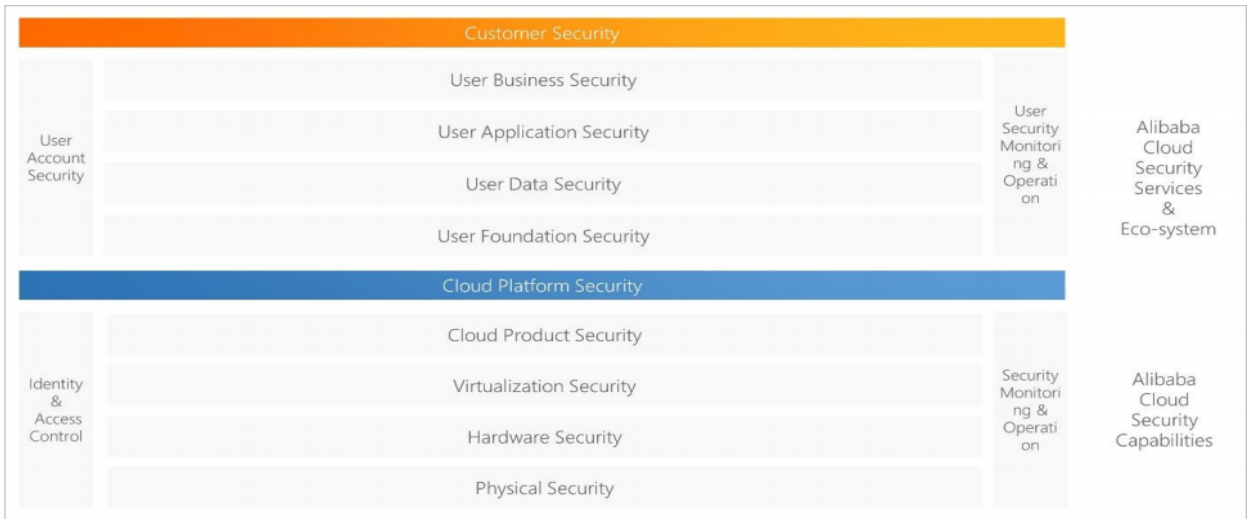


Fig – 1 Overview of the shared responsibility model

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 operating system (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. While Alibaba Cloud offers Alibaba Cloud Security, which leverages the years of expertise in attack prevention technologies to help customers protect their applications and systems, customers should configure and use cloud products based on security best practices and build applications on these securely configured cloud products.

Solution to Compliance with C-RAF 2.0

This part outlines how Alibaba Cloud can help the customers in compliant with C-RAF 2.0. In the following section, baseline level controls are presented using a normal font. In contrast, Intermediate level controls are presented in *italics*. Finally, Advanced level controls are presented in bold italics.

Domain 1: Governance

Domain 1 of C-RAF 2.0 established the expectation on organization governance. In general, it is customers' responsibilities to ensure the Board and Senior Management has provided adequate and sufficient oversight to oversee the overall cybersecurity management and provide support to enhance cybersecurity capabilities of AIs. Domain 1 of C-RAF 2.0 also highlights the importance of AIs to set the tone from the top and cultivates a strong culture of cyber risk management and awareness among all levels of staff.

Key considerations related to governance are listed below for AIs to address Domain 1 requirements:

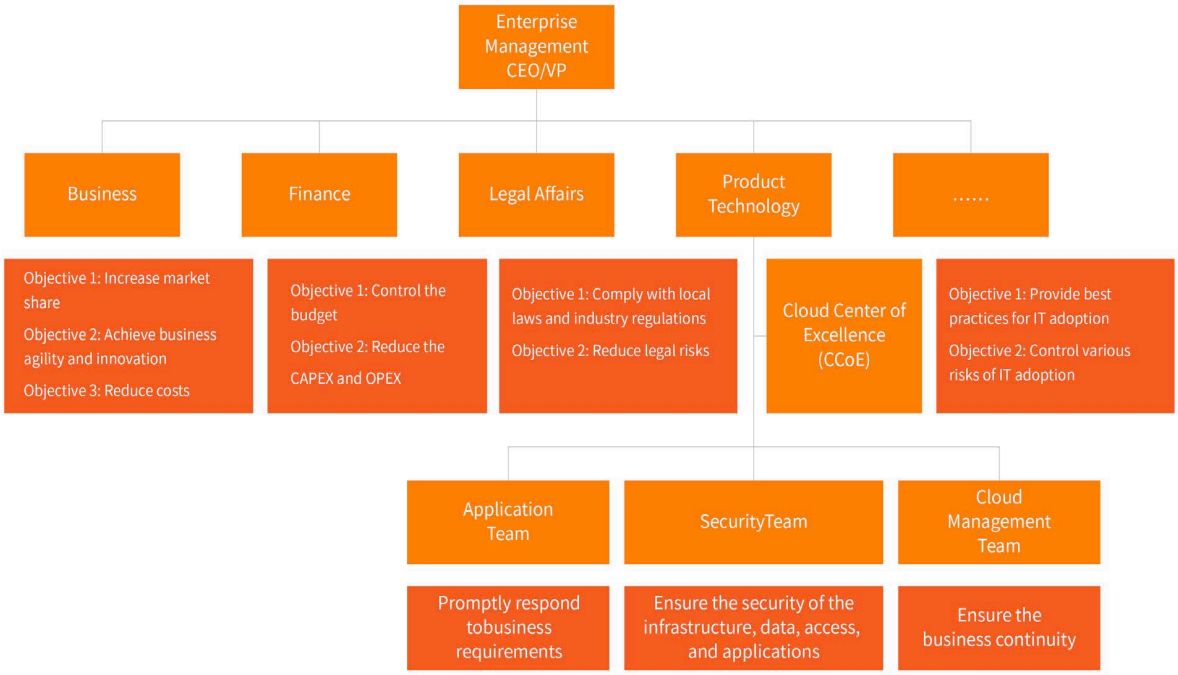
Key Aspects	Applicability	Consideration
Cyber resilience oversight	AIs	AIs are responsible to set the tone from the top and cultivates a strong culture of cyber risk management and awareness among all levels of staff and establishes oversight of cyber risks and tracking of actions to minimize cyber risk exposure.
Strategies and policies		AIs are responsible to establish a top-down action plan to improve the cybersecurity posture and cyber resilience of the institution's systems, processes, and services, and regularly update policies to manage cyber risk and cyber resilience and reflect latest practices across the institution.
Cyber risk management		AIs can establish a top-down plan of action to improve the cybersecurity posture of the entity, allocates adequate resources and expertise to implement and enforce the cyber strategy and implements appropriate governance controls to manage cyber risks consistently and systemically. AIs can build dedicated teams or designate employees to govern risks and the following steps are commonly used for cyber risk governance:

		- Identify and evaluate risks: Identify potential risks that may encounter at each stage, evaluate risk levels by quantifying losses, and make decisions to govern different risk levels. - Formulate governance policies: Transform governance decisions into governance policies. Governance policies are rules that are systematically implemented to restrict specific management operations on IT systems or generate alerts. - Continuously supervise governance: Take technical measures to implement management decisions. Alibaba Cloud is able to provide technical support that helps enterprises reaching their objectives. Systematic governance in the cloud can be divided into two parts: 1. Prevention: Enterprises can use the security services of Alibaba Cloud to actively defend against malicious attacks and use control policies to restrict specific management operations and changes. 2. Detection: Alibaba Cloud's cloud services supplement AI's detection capabilities in detecting insider and external threats.
Audit		AIs' third line of defense should be able to effectively assess the adequacy of policies, procedures, processes, and controls implemented on the basis which commensurate with the AIs' risk profile.
Staffing and training		AIs should establish policies and procedures to govern human resourcing in supporting cybersecurity management. In particular, AIs should ensure cybersecurity staff have the requisite knowledge and skills to effectively perform their duties and discharge their responsibilities. AIs should also provide tailored training program to ensure certain areas of higher risk or priority receive greater attention and investment.

Cloud Center of Excellence (CCoE)

Throughout the lifecycle of cloud adoption, AIs should ensure proper ***governance and steering*** are provided to the deployment process and ongoing management of cloud services in use. AIs may need the support of professional expertise to carry out proper planning, implementation, and continuous optimization for cloud adoption solutions so that AIs can enjoy maximum advantage of the benefits of cloud services thus to promote business development.

Therefore, AIs may set up a cloud management team or a cloud center of excellence (CCoE) under the first line of defense, who are primary responsible for planning the overall cloud adoption plan by identifying the requirements of business teams and implementing the plan in an appropriate manner.



The above figure shows a simplified organizational structure. AIs should note that the Board and Senior Management still retains the ultimate responsibility in managing the cybersecurity risk of the entity associated with cloud adoption. The responsibilities include identify and assess risks in aspects such as security and compliance, and provide guidance to the overall adoption strategy, and prevent, detect, and manage risks at the earliest opportunity throughout the process of cloud adoption and application. The responsible parties may discharge the responsibilities to CCoE.

Domain 2: Identification

Domain 2 of C-RAF 2.0 established the expectation on asset management and cyber risk management. AIs should establish robust process in managing IT assets and manage inherent cybersecurity risks in relation to the internal environment.

AIs should adopt appropriate controls to manage IT assets including software, virtual instances, applications, and data hosted on the cloud environment. Risk management process should be formalized to define and control risks and a dedicated risk governance team or employees should be assigned to manage cybersecurity risks. Key considerations are listed below for AIs to address Domain 2 requirements:

2.1 IT Asset Management

Key Aspects	Applicability	Consideration
IT Asset Management	AIs & Alibaba Cloud	AIs AIs are responsible to maintain an inventory of the IT assets to facilitate assessment of whether appropriate cybersecurity safeguards based on their data classification and business value and are at the level of granularity deemed necessary are in place. AIs should assign accountability and *establish process to update the inventory for installations, removal, and update to IT assets* **as well as track, prioritize and custom reporting of the IT asset inventory. AIs may consider deploying tools to centralize and automatic the maintenance of inventory.** AIs should formulate an asset life-cycle process to limit cybersecurity risk. AIs can use Sensitive Data Discovery and Protection (SDDP) to perform sensitive data detection to facilitate data classification by scanning, classification, and grading on structured and unstructured data. For example, SDDP console displays the storage objects that contain sensitive data, visitors that access data, and anomalous data flows and activities. AIs can control the security risks and optimize relevant security policies based on the information displayed in the SDDP console to protect concerned data. *Monitoring of configuration compliance status* **AIs should deploy tools and implement processes to detect and**

Key Aspects	Applicability	Consideration
		block unauthorized changes to software and hardware, with alerts generated on malicious activities for follow-up. Cloud Config can be used to monitor and continuously evaluate the configuration of Alibaba Cloud resources. AIs can retrieve the configurations of resources and hence track the changes and compliance status of configuration of cloud services. *Shadow IT detection* Controls should be implemented to detect shadow IT or IT applications that are acquired and used without having undergone proper governance and approval procedures. In this case, AIs can configure an application whitelist in Security Center, which only allows authorized software to run to prevent unauthorized and malicious applications (shadow IT) to realize Endpoint Detection and Response (EDR). Alibaba Cloud Alibaba Cloud identifies, inventories, classifies, and manages information assets to ensure an appropriate level of protection over the information assets in the Alibaba Cloud environment that are used to ***render cloud services***. Alibaba Cloud has established Information Assets Security Management policy to regulate the identification, classification and management of information assets. A Configuration Management Database (CMDB) is used for consolidating and maintaining information from different systems on information assets related to cloud services. Each information asset is inventoried and assigned to an asset owner. Identification and classification of information assets are updated as needed to ensure that assets are identified and inventoried accurately, completely, consistently and up to date. All changes to assets maintained in the CMDB are logged. Alibaba Cloud has also established guidelines to regulate procedures for acquiring, deploying, and disposing information assets. For example, acquisition of new assets must be authorized by appropriate personnel. Moreover, before any new asset is deployed to the production environment, testing should be conducted with testing results documented. The formal guidelines are followed to mitigate security risks

Key Aspects	Applicability	Consideration
		throughout the asset life cycle.

2.2 Cyber Risk Identification, Assessment, Treatment, and Monitoring

Key Aspects	Applicability	Consideration
Identification	AIs	<u>AIs</u> AIs are responsible for establishing cybersecurity risk management process and performing regular cyber risk assessment to identify and assess the likelihood and potential damage of foreseeable cyber threats, including the deployment risk of new technologies and services, etc. Such risk assessment should focus on safeguarding all information assets, including internal and customer information, and EOL software and hardware components. Moreover, AIs should consider methodological approaches such as STRIDE and PASTA threat modelling, etc. to identify critical information and systems, high-risk transactions, and associated threats to justify the areas that warrant compensating cybersecurity controls to mitigate risks. **To assist the identification during cyber risk assessment, AIs can utilize the security features provided by different Alibaba Cloud products such as Security Center, Web Application Firewall (WAF), and Cloud Firewall for comprehensive identification of cyber threats and vulnerabilities in various aspects thus assess the risks accordingly. Refer to Domain 4 for more details.** Upon risk identification, risk owners should be assigned to be accountable for implementing and enforcing risk treatment measures, as well as identifying emerging threats to ensure they are reflected in an updated threat model mentioned above. **As the results of risk assessment, AIs should develop risk metrics to highlight assets with the highest risk exposure and evaluate the effectiveness of mitigating controls.**
Assessment		
Treatment		

Domain 3: Protection

Domain 3 of C-RAF 2.0 established the expectation on protection of IT infrastructure. Requirements ranging from access controls, infrastructure design and network protection, data protection, secure development, patch management as well as remediation management have been defined in the domain.

Alibaba Cloud's products provide various levels of access control capabilities. AIs need to configure security features in such products according to business needs. While AIs' applications and business systems on Alibaba Cloud are subjected to protection by Alibaba Cloud Security services and any third-party security products in the Alibaba Cloud security ecosystem. AIs can also use Alibaba Cloud security services to monitor and manage the security of applications and business systems on the cloud.

3.1 User account management

Under the shared responsibility model, AIs are responsible to configure and deploy appropriate controls to access to the cloud platform. Alibaba Cloud has established service agreements on its official website, which defines respective responsibilities and obligations of Customers and Alibaba Cloud. During the Alibaba Cloud account registration or product purchase process, customers must agree to and confirm acceptance of the service agreements. Various solutions are also offered by Alibaba Cloud which provide access control management features to assist AIs to address the requirements of Section 3.1:

Key Aspects	Applicability	Consideration
User account management	AIs & Alibaba Cloud	AIs Alibaba Cloud provides customers with user identity management and resource access control capabilities. Resource Access Management (RAM) is a centralized user identity management and resource access control service provided by Alibaba Cloud which enables customers to securely authorize access to their resources and ensure access to customers' environments is properly restricted. RAM supports user account management in the following ways: - 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,

Key Aspects	Applicability	Consideration
		systems or applications. In order to eliminates security risks arising from sharing of Alibaba Cloud account credentials, a different password or Application Programming Interface (API) Access Key can be assigned to each RAM user. Besides, AIs can create custom password strength policies for RAM accounts. For example, AIs can configure minimum password length, password complexity, and limits to password retries and reuse based on own business need. - Each RAM user can log on to the Alibaba Cloud console or call service APIs to perform operations on cloud resources. By default, a newly created RAM user account does not have any permissions on resources. Customers can assign minimum operation and access permissions to different RAM users following the principle of least privilege to ensure employee access to systems and confidential data is restricted by their granted access. - Further, RAM user can obtain a Security Token Service (STS) token to assume the RAM role and access the defined Alibaba Cloud resources. The Assume Role approach provides AIs the flexibility to grant temporary access to any RAM users. - AIs can implement identification and authentication mechanism based on business requirement. **Multi-factor authentication (MFA) and single sign-on (SSO) services could be enabled for RAM users.** In addition, Alibaba Cloud Identity as a Service (IDaaS) serves as a management platform to centrally manage authentication of RAM users. AIs can use IDaaS to verify authenticity of RAM identifies and hence prevent unauthorized personnel to gain access to the resources. - Changes to logical user access, including those that result from voluntary and involuntary terminations, should trigger automated notices to appropriate personnel. AIs can use EventBridge, a serverless event bus service that can be accessed from other Alibaba Cloud services or custom applications, to build distributed event-driven architectures. RAM events can be set as the event source and Alibaba Cloud Message Queue as the event target. Then, AIs can customize event rules to generate notification and monitor specific types of events such as the change of logical

Key Aspects	Applicability	Consideration
		access by routing events to Message Queue accordingly. The alert service provided by CloudMonitor is integrated with Message Queue that enables AIs to customize alert rules on the monitoring data and receive alert notifications. - RAM operation events, i.e., access provisioning, termination, and modification performed by Alibaba Cloud accounts (administrators) will be logged and allowed tracking. Please refer to Domain 4 of activities monitoring for more details. - AIs can create multiple isolated RAM accounts and set up the organizational structure, with segregation of production and non-production environments to prevent unauthorized access or changes to information assets. For more details, please refer to Section 3.2 Infrastructure Protection Control. Still, adequate internal controls should be implemented by AIs, including but not limited to: - Establish formal access control policy and ensure employee access to systems and confidential data is granted 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. - Although customers can use RAM to manage user identities and access permissions to resources. When an employee leaves the company, or any organizational structure changes resulting change in permissions of RAM users, AIs should establish a set of processes to amend and revoke access to the cloud environment and resources. AIs are responsible to ensure proper accesses and permissions are granted to authorized personnel, and to accurately manage the identities and permissions of the user groups to which the RAM users belong to all the time. In particular, AIs are responsible to ensure logical access is removed immediately upon notification of the involuntary or voluntary departure of an employee. - User information such as active users and roles are available on RAM platform. However, it is AIs' responsibility to perform users access reviews periodically for all access to systems and resources

Key Aspects	Applicability	Consideration
		using risk-based approach. - Proper procedure should be formulated to ensure the creation, amendment, and termination of accesses are submitted and approved by the appropriate personnel. - Change all default passwords and unnecessary default accounts before system implementation and thereafter on a regular basis. - Deploy automatic password checking mechanism to check against a list of commonly-used, expected, or compromised values available online and unique to the commonly used terms within the institution. <u>Alibaba Cloud</u> Alibaba Cloud deployed Identify and Access Management (IAM) measures to ensure access to resources and systems within Alibaba Cloud's environment is properly managed and restricted, following the principle of least privilege and segregation of duties set forth in the Access Control Management Policy, to protect information assets from unauthorized access. *Internal User Management & Permission and Access Management* Alibaba Cloud uses a centralized identity authentication system for the systems and resources within the Alibaba Cloud's environment with SSO enabled. Each employee's Active Directory (AD) account is unique and identifiable to an individual user and cannot be shared. The Human Resource System is synchronized with the identity authentication system and the permission management system, with employee data from the Human Resource System used to facilitate the creation, change, and removal of employees' AD accounts. Alibaba Cloud has established procedures to automatically create new AD accounts for new joiners. For employees who change roles or transfer to different departments, automatic notifications are sent out to the employees' supervisors to review their user access permissions and to return any unnecessary access permissions based on their current job responsibilities. For employee's termination, the employees' AD accounts are disabled within the same day of their last working day based on automated feeds from the Human Resource System.

Key Aspects	Applicability	Consideration
		Alibaba Cloud assigns access permissions of minimum resource to employees based on their positions and roles and business needs. A centralized permission management system is used for access application, access approval, and automatic access provisioning or access removal. An employee can log onto such system to apply for access permissions as needed. Permissions are categorized into different levels based on associated level of risks, and approval mechanisms are implemented with reference to the level of access. Requested permissions are automatically granted to the employee once approvals are provided by authorized personnel. All access requests are required to be approved at least by the user's supervisor, who cannot be the same person as the requestor to ensure segregation of duties. Access to network devices and servers is classified into three types by Alibaba Cloud according to the risk levels, namely normal users, application administrators and system administrators. Approval workflow is pre-set within the permission management system according to the type of access. Approvers in the workflow is determined based on system owner information and application owner information stored in the respective systems. *Password Control* Alibaba Cloud implements stringent password policies, which require users to set up a password that meets the password requirements including password length, password complexity, password age, password history, maximum login attempts, and change of initial password. *Access Review and Monitoring* Audit and monitoring rules have been defined within the access monitoring system to analyze usage of accounts and access permissions, detect potential misuse of access privileges, and generate automated alerts to notify the Security Team of any deviations or exceptions. The Security Team is responsible for following up on the alerts and take appropriate actions. In addition, a schedule job is run to identify access permissions that have not been used by users for a consecutive 90 days and send out automated emails for the associated

Key Aspects	Applicability	Consideration
		users to confirm whether the captured access permissions are still required. Access permissions will be automatically revoked if the access permissions are confirmed to be not needed, or if no confirmation is received within one week.
Privileged user account management	AIs & Alibaba Cloud	<u>AIs</u> It is AIs' responsibility to limit and tightly control elevated privileges of their employees. AIs should ensure administrators should either have two accounts: one for administrative use and one for general purpose, non-administrative tasks, or if they only have one account, then their administrative privileges are granted on a needs-basis. AIs are capable to grant diverse and privileged permissions to a single identity or a group of identities using RAM. AIs can grant the least privilege to prevent execution of privileged commands by non-privileged users such as disable, circumvent, or alter implemented security safeguards or countermeasures implemented on cloud. By using Bastionhost, AIs are capable to configure control policies such as command control, command approval, protocol control, and access control policies so as to manage the access of users to hosts. **AIs can ensure commands are executed with valid reasons and required administrators' prior approvals.** In order to restrict privileged account activities, in particular, to prevent unauthorized downloading or transmission of confidential data from database administrators, AIs can manage the permissions granted to those accounts using Alibaba Cloud Data Management Service (DMS) hence to revoke and reset the database access permission if needed. Stringent authentication controls should be enabled for privileged accounts, such as MFA activated for RAM accounts with privileged/administrative permissions, and privileged access to high-risk

Key Aspects	Applicability	Consideration
		systems as identified in the cyber risk assessment(s) via Bastionhost. To ensure accountability, the operation events performed by RAM users that have the administrator permissions can be tracked and recorded by ActionTrail, such as a creation or deletion of a user group by a RAM user. AIs can also audit the video session recorded by Bastionhost for the purpose of review on execution of privileged functions. Alibaba Cloud Privileged access is strictly controlled by Alibaba Cloud. Root privileges are restricted to authorized personnel only. Password for root accounts is automatically rotated on a monthly basis via a scheduled job. Privileged sudo to root activities are logged and monitored. Moreover, monitoring rules are defined within the access monitoring system to analyze usage of access privileges with automated alerts generated based on the monitoring results and followed up by security team.
Customer access management	AIs	AIs AIs are responsible for implementing adequate customer access controls that are commensurate with the risk for access to internet-based products or services.
Physical access management	Alibaba Cloud	Alibaba Cloud Alibaba Cloud is responsible for the physical security of all its data center facilities. Data centers are configured with strict access control such as access card and fingerprint requirements, equipped with surveillance systems covering all the areas and passages, and staffed with security guards for 24x7 patrol. Moreover, the data center server rooms where the IT equipment and systems are stored, are physically isolated from the office and delivery areas with access controlled via badge readers, biometric identification mechanisms, and/or physical locks. Alibaba Cloud has established policies and procedures around Physical and Environmental Security Management, to regulate access security management and environmental controls. An access card system is used for access management in each data center. Only authorized Alibaba Cloud employees and entitled data

Key Aspects	Applicability	Consideration
		center service providers personnel are granted access to the access card system. At each Alibaba Cloud data center, long-term access permissions are assigned only to corresponding maintenance personnel. If there is a need for any other person to enter the data center, the person must submit application in advance, and is granted temporary permission only upon the approval of the corresponding data center managers. Data center managers are required to notify the data center service providers' personnel of the person's identity. For each entry to or exit from the data center, such person must display his or her ID and be escorted by the data center's maintenance personnel for the entire duration of the visit and their access is logged. On a monthly basis, data center managers perform access reviews to ensure that user access rights in the access card system are appropriate. After an incident e.g., unauthorized access to data center occurs in the data centers, according to the risk level and nature of the incident, data center service providers will submit an Operation Incident Report to Alibaba Cloud, covering the causes, impact and resolution status of the incident.
Remote access management	AIs & Alibaba Cloud	<u>AIs</u> AIs can establish secure and encrypted connections (Secure Sockets Layer - Virtual Private Network (SSL-VPN) or IPsec-VPN) through VPN Gateway to allow remote access by authorized parties. AIs can also integrate IDaaS to enable Two-Factor Authentication (2FA) with an IDaaS instance to add a layer of protection on access. All remote accesses would need to pass through the VPN gateway before entering the cloud network hence all remote access through this centralized managed network access control points to facilitate monitoring and control of remote access sessions and the auditing of user activities. **Besides, AIs can disconnect the remote access expeditiously in an emergency.** Bastionhost supports 2FA which sends a Short Message Service (SMS)

Key Aspects	Applicability	Consideration
		verification code during the logon of users. Such verification adds an extra layer of protection in addition to username and password to authenticate the identity of the user for the second time. This mechanism ensures that users who have not bound their mobile numbers cannot perform Operating and Maintenance (O&M) operations, thus prevents AIs' information from unauthorized use and disclosure by remote access. **For remote access with privileged permission, e.g., execution of privileged commands and access to security-relevant information, AIs are responsible to document the rationale of such assess and regular review to determine if the access is granted on a needed basis.** **To facilitate monitoring, Bastionhost allows AIs to configure control policies for execution of privileged commands and the access to security-relevant information. When control policies are configured, the defined actions must be approved by administrators, and notification will be triggered by Bastionhost before execution. Furthermore, Bastionhost provides session playback which allows AIs to audit activities performed.** **Apart from utilizing Alibaba Cloud's solution to ensure remote access security, AIs should request users to protect information about remote access mechanisms from unauthorised use and disclosure, for example, by attending security training specifically for remote access rights granted, acknowledging access agreement etc.** <u>Alibaba Cloud</u> In order to access Alibaba Cloud's Intranet through VPN from the internet, internal employees must pass 2FA based on domain account name and password plus dynamic digital token received on registered devices.

Key Aspects	Applicability	Consideration
Wireless access management	AIs	AIs AIs should establish wireless network usage restrictions, configuration and connection requirements, and implementation guidance along with protective measures such as implementation of perimeter firewalls and authentication and encryption of wireless access to prevent unauthorized access.
Mobile access management	AIs	AIs AIs should establish usage restrictions, configuration and connection requirement, and implementation guidance mobile access to network. The remote connection should be implemented with proper authorization process and deployed security controls for the confidentiality and integrity of information on mobile devices.
Cryptographic keys management	AIs & Alibaba Cloud	AIs AIs are responsible to establish a cryptographic key management policy and procedures covering key generation, distribution, installation, renewal, revocation, and expiry. To protect cryptographic key in use, Alibaba Cloud's key management infrastructure conforms to the recommendations in National Institute of Standards and Technology (NIST) 800-57 and applies cryptographic algorithms in accordance with relevant compliance requirements. Alibaba Cloud's Hardware Security Module (HSM) has been validated and certified both internationally and domestically. HSMs used outside of mainland China regions are Federal Information Processing Standards (FIPS) 140-2 Level 3 certified. Alibaba Cloud Key Management Service (KMS) provides secure key management and cryptography service including secure hosting of keys, cryptographic operations, and key rotation. AIs can encrypt, decrypt, and host cryptographic keys via KMS and perform other key management operations such as key rotation and renewal. KMS can be also integrated into other cloud services to encrypt user data managed by the cloud services. It is AIs' responsibility to implement controls to prevent unauthorized access to cryptographic keys stored in KMS. Authentication and access to KMS are controlled and managed by

Key Aspects	Applicability	Consideration
		the Alibaba Cloud RAM service. For further detail, refer to 3.3 below. Alibaba Cloud Alibaba Cloud has established Alibaba Cloud Password and Key Management Policy to manage key generation, storage and usage, distribution, backup, replacement, and revocation during the life cycle of cryptographic keys. The policy outlines the requirements on the standard encryption algorithms, key management, and segregation of duties in the management process. For further detail, refer to 3.3 below.

3.2 Infrastructure Protection Control

Alibaba Cloud has implemented infrastructure security measures and virtualization technology to prevents the cloud resources of tenants from unauthorized access and ensures segregation among multiple tenants in a cloud computing environment by means of virtualized computing, storage, and network isolation.

Besides, Alibaba Cloud offers cloud-based network solutions to facilitate network design and protect cloud network. Please refer to below for consideration to address the requirements of Section 3.2:

Key Aspects	Applicability	Consideration
Network protection	AIs & Alibaba Cloud	AIs AIs are responsible for planning and designing cloud-based network architecture which includes configuration of network connection between on premises and cloud network, and segregation of network access in the cloud etc. AIs should ensure own networks are segmented in multiple, separate trust or security zones with defense-in-depth strategies to mitigate the risk of cyber-attacks. **On a regular or as-needed basis, AIs should review and assess the network segmentation approach and enforcement effectiveness to identify gaps in architecture, configurations, processes etc., and formulate a remediation plan that is agreed with Senior Management.**

Key Aspects	Applicability	Consideration
		Network Design and Segmentation Alibaba Cloud offers different cloud-based network solutions, for example, AIs can create an independent Virtual Private Cloud (VPC) for each network partition/segment. Given that VPC instances are logically isolated from another VPC instance, AIs 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 AIs, AIs can configure custom settings such as route table isolation, route filtering, and routing policies as needed. The following are possible network partitions: - Production and testing: The resources in the production environment and test environment are deployed in two partitions. - Internet facing: This partition is similar to the Demilitarized Zone (DMZ) in a data center. Internet egress resources, such as Elastic IP addresses (EIPs), Network Address Translation (NAT) gateways, Server Load Balancer (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. *Traffic Management*

Key Aspects	Applicability	Consideration
		In order to minimize the attack surface and restrict unauthorized network traffic to protect the confidentiality and integrity of AIs' information, network perimeter defense tools such as Virtual Border Router, Virtual Switch (vSwitch), and Cloud Firewall should be properly deployed and configured. **Firewalls should be configured to restrict and monitor traffic between trusted and untrusted zones**. AIs can deploy Cloud Firewall to protect internal network and monitor internal and external traffic. Alibaba Cloud's Cloud Firewall provides firewalls as a service to realize traffic monitoring between internet, VPC and internal network, threat detection and intelligence to deliver protection at the network boundaries including switches. It uses traffic visualization technology to analyze the numbers of total and risky items of open public network IP addresses, open ports, and open applications. It also blocks high-risk IP addresses from connecting to the network. An internet firewall is available at the border between the internet and the internal network, and AIs can configure outbound and inbound access control policies for the internet firewall and monitoring the network flow through Cloud Firewall. Cloud Firewall also has a built-in IPS and synchronizes with Security Center to receive the vulnerability detection results to provide protection against vulnerability and external attacks. Apart from Cloud Firewall, Security Center allows AIs to perform ongoing monitoring of network ports based on a risk-based approach. By integrating Security Center, AIs can gain an overview of asset information such as listening port hence to monitor any high-risk open ports. Besides, the configuration assessment feature enables AIs to perform checking on specific configurations of cloud resources such as port access policies of security groups of Elastic Compute Service (ECS) and unnecessary ports of SLB that are accessible over the internet. AIs are responsible to audit or verify firewall rules on a risk-based approach at least annually and ensure any changes to firewall rules should be reviewed before becoming effective. Cloud Firewall provides security check function to identify if any risky security group rules have been set and provide corresponding recommendation to users, AIs can

Key Aspects	Applicability	Consideration
		manually review and verify Cloud Firewall configuration settings, including the access control setting for internet firewall and VPC firewall. Intelligent policy recommendations are also provided by Cloud Firewall for AIs to view and apply. In addition, AIs can view the statistics on access controls policies including the change in policies from the last seven (7) days. Other than Cloud Firewall, Alibaba Cloud provides WAF for protecting websites and web servers. WAF are configured to defend against common security threats reported by OWASP including SQL injection, cross-site scripting (XSS), common vulnerabilities in web plugins, webshell upload, and unauthorized access to cloud resources. AIs can use WAF to filter out malicious access attempts to prevent leakage of web assets and data and ensure the security and availability of web applications. The Managed Security Service of WAF includes configuration service and protection policy optimization. In particular, it performs adaptability verification after website configuration is completed and assists in modifying the configuration and policies based on the needs of AIs. *Network Access and Connection Security* AIs should implement technical controls to prevent unauthorized connections and unauthorized devices to internal networks including unauthorized addition of new external connections and removal of existing connections. Alibaba Cloud allows AIs to control access to applications by creating a Network Access Control List (NACL) in a VPC network. AIs can customize the rules of a NACL and associate the NACL with a vSwitch to control inbound and outbound traffic of the ECS instance connected to the vSwitch. Besides, AIs can use Security Center to monitor connections on servers and networks. Security Center generates alerts on suspicious connections, such as suspicious connections to external IP addresses and suspicious webshell communications. In addition, Security Center detects suspicious accounts that attempt to log on to AIs' systems based on user behavior analysis to prevent unauthorized

Key Aspects	Applicability	Consideration
		connections and unauthorized actions. *Wireless Access Security* AIs are responsible for ensuring wireless access security through different means, for example, applying strong encryption for authentication and data transmission over wireless network with encryption keys frequently changed, physically segregating guest wireless networks from the internal networks, and deploying perimeter firewalls that are configured to restrict unauthorized traffic. *Remote Access Security* AIs should ensure security controls are implemented for remote access to all administrative consoles, including restricted virtual systems. Refer to other sections of this Whitepaper for authorization and O&M activities audit features provided by Bastionhost. Besides, Alibaba Cloud's VPN Gateway establishes encrypted remote connections. With the use of VPN Gateway, IPSec-VPN connection between AIs and an authorized customer gateway can be formed. For AIs deploying SSL-VPN, they can establish a ClassicLink connection between VPN Gateway and VPC and configure security group rule by entering the private IP address that is allowed to access. 2FA is possible with the integration of VPN Gateway with IDaaS and AD. Hence AIs can use VPN Gateway to ensure only authorized devices are allowed and block access attempts by unauthorized devices such as unregistered devices. **However, AIs are still responsible for deploying tools or establishing processes to detect and block access from unpatched employee-owned devices to internal networks.** *Network Intrusion and Attack Prevention* AIs can deploy Cloud Firewall, which has a built-in IPS. Users can enable the advanced setting for intrusion prevention to receive threat intelligence and intelligence protection offered by Alibaba Cloud. In order to mitigate the risk of any cyber-attacks, Alibaba Cloud provides an Anti-Distributed Denial-of-Service (DDoS) solution that can mitigate transport layer DDoS attacks by detecting and blocking attacks using

Key Aspects	Applicability	Consideration
		forged source IP addresses to enter to AIs' internal network continuously. Anti-spoofing measures is implemented to detect and block forged source IP addresses from connecting to the network: Alibaba Cloud platform solves the IP/Media Access Control (MAC)/Address Resolution Protocol (ARP) spoofing by isolating any anomalous protocol requests initiated on the data link layer of the host and avoiding IP spoofing on the network layer. Alibaba Cloud *Network Isolation* Alibaba Cloud's production and non-production networks are segregated, so that direct access from a non-production network to any servers and network devices in a production network is not allowed. Alibaba Cloud deploys Bastionhost for the production network boundary protection, that the O&M personnel in the office network can access the production network for O&M only through Bastionhost. When logging on to the Bastionhost, O&M personnel must perform MFA with a one-time password (OTP) along with the domain account name and password. Bastionhost uses encryption algorithms to ensure the confidentiality and integrity of data transmitted through O&M channel. Alibaba Cloud also isolates cloud service networks that provide external services from physical networks supporting the underlying cloud services functionalities. NACLs are configured to prevent access from cloud service networks to physical networks. Alibaba Cloud also takes network control measures to prevent unauthorized devices from connecting to the internal network and prevent the physical servers of the cloud platform from connecting to external devices. *Segregation of tenants' content* For the purpose of clearly compartmentalisation and segregation of customers contents stored in different cloud services, based on the hardware virtualization technology, Alibaba Cloud's virtual machine (VM) management practices allow VMs on multiple computing nodes to be isolated from each other at the system layer. It prevents unauthorized

Key Aspects	Applicability	Consideration
		access to system resources between tenants and ensures basic computing isolation between computing nodes. Tenant isolation is achieved in three layers, namely computing, storage and network: *Segregation of tenants' content - Computing isolation* Alibaba Cloud provides a variety of cloud-based computing instances and services that allow automatic scaling to meet application or business needs. The key isolation boundaries are between the management system and VMs and between VMs themselves, provided by the hypervisors. Alibaba Cloud platform uses a virtualized environment where ECS instances run as standalone VMs, and the isolation is enforced by using different permission levels of physical processors to avoid unauthorized access of a user's VM to the host or to another VM. *Segregation of tenants' content - Storage isolation* In the basic design of cloud computing virtualization, Alibaba Cloud separates VM-based computing from storage. This separation allows computing and storage to be scaled independently and makes it easier to provide multi-tenant services. At the virtualization layer, hypervisors use a separate device driver model for input/output (I/O) virtualization. All the 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, implementing security isolation of hard disk space between different VMs. *Segregation of tenants' content - Network isolation* 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 different security groups cannot communicate with each other by default, while security group rules can be configured to control network access over ECS instances.

Key Aspects	Applicability	Consideration
System configuration	AIs & Alibaba Cloud	AIs *System security baseline* AIs should design security configuration baseline and enforce system configurations (for servers, desktops, routers, etc.) in accordance with the baseline to reduce security risk by restricting potential attacks on an ongoing basis. Alibaba Cloud ECS tenants can use an image to create standardized ECS instances. AIs can select images from a marketplace or use their own customized images. The security enhancement of Alibaba Cloud public images contains three (3) parts: image security configuration, image vulnerability fixing, and default security software in an image. In addition, all Alibaba Cloud public images include Alibaba Cloud security software, such as Security Center, to guarantee the security of instances upon startup. For configurations of distributed application, AIs can use Application Configuration Management (ACM) to manage configuration at application level such. Applications should be configured to restrict and prevent unauthorized access attempts; time-out setting can be configured so that system sessions would be locked after a pre-defined period of inactivity and should be terminated if pre-defined conditions are met. AIs can use ACM to configure session timeout policy and automatically push the configuration to all relevant servers and manage the configuration setting of the application continuously. To control the risk of unnecessary open ports and detect if any unnecessary and high-risk ports are enabled, AIs can use Cloud Firewall to conduct network flow analysis to obtain the details of internet access traffic to identify any ports that are no longer needed for business purposes and disable the ports accordingly. *Configuration re-assessment* As an ongoing measures, AIs should verify the compliance with security baseline. Cloud Config can be used to track changes and compliance status after any change of the configuration. Apart from Cloud Config,

Key Aspects	Applicability	Consideration
		AIs can also make use of the configuration assessment feature of the Security Center to check for security risks in the configurations of their cloud services. Configurations will be assessed from different aspects, includes identity authentication and permissions, network access control, data security, etc. For misconfigurations, Security Center hence provides solutions to fix vulnerabilities to reinforces system security. *Authorization control to system configuration* To prevent any unauthorized change to system configuration, proper access controls should be implemented. AIs can use RAM and BastionHost to implement access controls and perform monitoring on the access to configurations of cloud service and operating system (including VMs and hypervisors) to **prevent unauthorized change through the execution of unauthorized code on owned or managed devices and systems components.** Administrators can assign RAM users to manage the configuration of dedicated cloud resources, and Bastionhost supports AIs to whitelist/blacklist command and IP addresses to restrict the activities and access to hosts. Moreover, administrators will receive a notification upon the O&M user runs a command that was configured to be approved for better detection purpose. In addition, AIs are responsible for establishing administrative and technical controls to prevent users without administrative authorization from installing software. Security Center allows AIs to add applications that run on the servers to an application whitelist, hence it identifies applications as trusted, suspicious, or malicious based on the whitelist to prevent unauthorized applications from running. Automatic alerts will be triggered when a process not specified in the whitelist starts on a server. *Vulnerability check* To prevent vulnerabilities resulted from improper system configuration, documented hardening standards should be introduced with reference to industry recognized standards, and a process should be put in place to ensure all devices are hardened in line with these standards. Alibaba Cloud has released the OS Benchmark certified by Cyber Internet Security (CIS). AIs can follow the best practices provided in the CIS

Key Aspects	Applicability	Consideration
		Benchmark to configure cloud services and enhance security. Moreover, AIs should ensure that public-facing servers are routinely checked for integrity to limit the window of time in which a system may be exposed to potential threats. Security Center could be used to detect and generate alerts if unauthorized processes or intrusion attacks to the public-facing servers, such as suspicious and arbitrary command execution or other suspicious processes that may impair the integrity of servers. Nevertheless, AIs should **proactively identify control gaps that may be used as part of a zero-day attack.** Alibaba Cloud *OS and Image Hardening* Alibaba Cloud has established the hardening standards for OS and image hardening. The OS and image adopted for Alibaba Cloud's hosting servers are required to be configured in line with the standards. Alibaba Cloud monitors the vulnerabilities in Alibaba Cloud public image OSs and third-party software in real time to ensure that high-risk vulnerabilities in Alibaba Cloud public images are repaired in a timely manner. After a new high-risk vulnerability is detected, Alibaba Cloud images are updated to integrate patches for known high-risk vulnerabilities to prevent the host from being exposed to high risks.
Virtualization security	AIs & Alibaba Cloud	AIs AIs should ensure that controls are in place to restrict administrative access to the hypervisor and host OS. For that, AIs could manage RAM users and permissions of them to access virtual instances. AIs should also establish policies governing the security, creation, distribution, storage, use, retirement, and destruction of VM images and snapshots. Alibaba Cloud's Container Registry allows AIs to manage and effectively distribute cloud-native artifacts including container images that meet the standards of Open Container Initiative (OCI). AIs can hence store, distribute, perform security scans on VM images with Container Registry. Alibaba Cloud

Key Aspects	Applicability	Consideration
		Any change made to Alibaba Cloud's VM images are required to be requested and approved through a pre-defined approval workflow on change management platform. The verification methodology and results are recorded on the platform. Moreover, the released change is communicated with tenants via Alibaba Cloud official website.
Internet of Things (IoT) Security	AIs	AIs AIs are responsible for maintaining an inventory of all IoT devices with their network connections and physical/logical locations. Based on the IoT inventory, AIs should establish process to assess and implement security controls to mitigate risks arising from the IoT devices, based on the function of and the criticality of data associated with such devices.

3.3 Data Protection

Alibaba Cloud offers data security solutions in various aspects to facilitate data management and security measures. Please refer to below for consideration to address the requirements of Section 3.3:

Key Aspects	Applicability	Consideration
End point data security	AIs & Alibaba Cloud	AIs *Data security associated with cloud services and instances* *Data Loss Prevention Tool* To ensure data security, data loss prevention controls or devices should be applied for outbound communications. In view of this, Alibaba Cloud's SDDP serves as a Data Leakage Prevention (DLP) tool that discovers, categorizes, and protects sensitive data on the cloud. The built-in anomalous activity detection rules can monitor access to sensitive data assets stored in cloud resources and detect high-risk activities. It automatically analyzes sensitive data usage stored by customers and provides early warning for suspicious data access, which helps users prevent data breaches, and meet compliance requirements. For anomalous activity detected, SDDP provides repair recommendations via intelligent algorithms. The sensitive data access control feature helps control access permission to various data storage and data transmission

Key Aspects	Applicability	Consideration
		products in the cloud environment. It also supports the real-time query of data, users, and permissions and alerts AIs of permissions assignments and abnormal permissions usage that do not meet security best practices. Apart from SDDP, Security Center helps AIs to detect and prevent critical data from leakage by using the cloud threat detection feature. Security Center generates alerts on the detection of web page tampering, webshells, mining programs, and other malicious processes to identify potential threats in real time. AIs can quarantine and restore files that contain viruses in the Security Center. It monitors sensitive directories and files to detect suspicious read, write, or delete operations to prevent tampering and removal. It can also detect suspicious command execution in databases and unauthorized system processes. Moreover, AIs can use Security Center to detects risks in the configurations such as to check whether Relational Database Service (RDS) databases are accessible over the internet or whether an access whitelist is configured. On the other hand, AIs has the flexibility to deploy third-party anti-virus and anti-malware solutions in instances which do not support sandboxing architecture. *Data security associated with removable media & mobile devices* It is AIs' responsibility to centrally manage and monitor the use of removable media and mobile devices, that such use should be restricted to authorized personnel to prevent leakage of confidential data. Alibaba Cloud Alibaba Cloud has implemented the following controls in relation to endpoint data security: - Alibaba Group Endpoint Security Management Policy is established to govern software installation and patch updates on Alibaba Cloud's endpoint devices. - DLP software is required to be installed on Alibaba Cloud employees' PCs to detect sensitive operations based on pre-defined rules. - Procedures are in place to restrict the use of removable media

Key Aspects	Applicability	Consideration
		(e.g., USB) on a needed basis with proper authorization. - Alibaba Cloud's O&M personnel could not access customer data and any channels for data to flow out of the production cluster are blocked via technical means.
Data protection	AIs & Alibaba Cloud	<u>AIs</u> Alibaba Cloud provides various products for AIs to ensure data security in the cloud by referencing the Data Security Capability Maturity Mode in respect of non-tamperable hardware-level security, unbreakable encryption capability, secure computing, and precise leak defense. AIs should establish processes and controls for data protection including defining encryption criteria in accordance with the data classification and grading standards based on the industry and business characteristics of AIs and utilize the provided security features to manage the risk of data leakage in transit and at rest. *Cryptography and Key Management* The encryption design varies with Alibaba Cloud services based on product features and business needs. AIs can also utilize KMS for encryption key management. Key hierarchy in Alibaba Cloud consists of at least two layers: the first layer is the Customer Master Key (CMK), and the second layer is Data Encryption Key (DEK). The CMK is used to encrypt or decrypt DEK whereas the DEK is used to encrypt or decrypt customers' data. In general, service managed keys are used as CMKs for encryption of data at rest. Several Alibaba Cloud services also support customer managed keys, including customer supplied keys i.e., Bring-your-own-key (BYOK) and customer generated keys. Given that customer managed CMKs are the asset of AIs. Alibaba Cloud services must obtain authorization from the AIs through RAM before they can use the CMK to encrypt or decrypt data. In addition, the KMS is a secure cryptographic service that provides secure channels and end-to-end authentication to ensure transmission security. All user requests for KMS must use Hypertext Transfer Protocol Secure (HTTPS), that KMS only allows the use of industry standard high security cipher suites in Transport Layer Security (TLS).

Key Aspects	Applicability	Consideration
		Encryption AIs are responsible establish encryption requirement of data in transit, at rest and in-use according to the sensitivity of data and ensure the encryption requirements are strictly followed. *Data in transit* AIs are reminded to perform end-to-end encryption for data in transit, especially for confidential data such as passwords and personal information across internet, **across private connections, and within the trusted zones when required.** The means of protection vary with the network channels used in the data transmission process. AIs should use SSL/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 CAs in the cloud. It helps AIs to switch from Hypertext Transfer Protocol (HTTP) to HTTPS, improving the trustworthiness of AIs' websites and preventing the websites from being hijacked, tampered with, or spied on. It simplifies certificate deployment and allows AIs to perform unified lifecycle management of their certificates in the cloud and distribute the certificates to other Alibaba Cloud services with a few clicks. For data transmission between enterprise sites, VPNs, or dedicated lines (i.e., Express Connect) should be used to reinforce communication channels. For internal communication, Alibaba Cloud provides VPN services to help AIs build end-to-end data encryption channels to ensure communication security during data transmission. Alibaba Cloud gateway products support end-to-end encryption during data transmission. For example, VPN Gateway securely and reliably connects on-premises data centers to Alibaba Cloud VPCs over encrypted channels. It can establish an IPsec-VPN connection to connect an on-premises data center to a VPC. An SSL-VPN connection can also be established to connect a remote client to a VPC.

Key Aspects	Applicability	Consideration
		For external communication, AIs should use the SSL/TLS protocol to encrypt the communication channel. *Data at rest* AIs can use the native encryption capabilities of Alibaba Cloud services or Alibaba Cloud Data Encryption Service for sensitive data encryption e.g., encryption for password in storage. General speaking, Alibaba Cloud allows users to encrypt data stored in Alibaba Cloud services by using keys stored in KMS. Alibaba Cloud supports the Advances Encryption Standard (AES) 256-bit key length for encrypting sensitive data such as password at rest. Data encryption approach varies according to the Alibaba Cloud services. For example, Object Storage Service (OSS) supports both server-side and client-side encryption. For server-side encryption, OSS uses service managed keys and CMKs to encrypt data. For client-side encryption, OSS allows the users to use on-premises self-managed keys or customer managed keys as CMKs generated in Alibaba Cloud KMS to encrypt data on the client side. Multiple versions of ApsaraDB or RDS supports Transparent Data Encryption (TDE) or database instance disk encryption which uses service managed keys and customer managed keys as CMKs to encrypt data. Moreover, AIs are responsible for adopting tools to prevent and detect unauthorized access to or exfiltration of confidential data. AIs can use SDDP as a DLP tool and use the built-in anomalous activity detection rules to monitor and alert on suspicious access to sensitive data. On the other hands, AIs should also have internal controls to restrict the use of removable media to prevent unauthorized personnel from extracting confidential information. Refer to “Endpoint data security” for more detail. *Data in Use* AIs are responsible to ensure the use of customer data in non-production environments (e.g., testing environment) complies with legal, regulatory, and internal policy requirements for concealing or removing sensitive data elements. *Data Destruction*

Key Aspects	Applicability	Consideration
		AIs are responsible for establishing data security policies and procedures to dispose or destroy data within time frames as required by applicable laws and regulatory requirements. Alibaba Cloud does not access or use member content without the customer's consent. On terminating services to cloud service customers, Alibaba Cloud deletes data assets of customers in a timely manner or returns the data assets according to relevant agreements. AIs should retrieve any data stored in cloud in a prompt manner. Alibaba Cloud uses data erasure techniques that meet industry standards. After a user instance is released, its original disk space and memory are reliably scrubbed to ensure user data security. The erasure operations are logged to prevent unauthorized access to customer data. Alibaba Cloud *Cryptography and Key Management* Alibaba Cloud's cryptography and key management ensures the confidentiality, authenticity, and integrity of sensitive data through the effective use of state-of-the-art cryptography. Alibaba Group's Data Security Guidelines is established to outline the protective measures including encryption of sensitive data. Alibaba Cloud has also established Alibaba Cloud Password and Key Management Policy to manage key generation, storage, usage, distribution, backup, replacement, and revocation during the life cycle of cryptographic keys. The policy covers requirements on the standard encryption algorithms, key management, and segregation of duties that are strictly followed in the management process. *Data Protection* Alibaba Cloud 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. *Encrypted Computing*

Key Aspects	Applicability	Consideration
		Alibaba Cloud uses end-to-end encryption to ensure data security and hardware-based encrypted computing service. Alibaba Cloud performs data encryption for user data in the trusted execution environment with Alibaba Cloud cryptographic computing technologies. Alibaba Cloud platform uses Intel® Soft Software Guard Extension (Intel® SGX) to provide a hardware-trusted execution environment. Users can establish a trusted execution environment to protect their sensitive data such as encryption/decryption keys and account credentials. Users can protect their data by writing code that supports that trusted execution environment so that their key data can be accessed and manipulated only through the code that they write. All encrypted information can only be computed and run in a trusted execution environment, providing hardware-based data protection. *Data Encryption* Alibaba Cloud ensure data security by performing encryption to data in transit, data at rest and hardware-based memory encryption. Data is encrypted prior to backup and in transit where applicable. In particular, Alibaba Cloud console uses HTTPS encryption for data transmission and TLS protocol are used for cloud products to ensure data transmission security while users read and upload data. HTTPS is also used to encrypt API payload data to address the need for protecting transmission of sensitive data via API. *Data Destruction* Alibaba cloud has established a security management system for the full lifecycle of devices, including reception, storage, placement, maintenance, transfer, and reuse or decommissioning. Controls are implemented for data destruction, for example: - Data erasure measures for the storage media are implemented for device recycle or decommission. - Prior to disposal of storage medias, procedures are taken to check whether the media containing data has been physically damaged to make sure that the data cannot be restored. - Before any device is recycled or transferred out of data centers,

Key Aspects	Applicability	Consideration
		data is overwritten for multiple times with erasure operations logged. - 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. *Customer Data Erasure and Disposal* Alibaba Cloud has implemented security measures and data erasure techniques that meet industry standards for customer data erasure and disposal. Data erasure is an extension of storage virtualization. After a user instance is released, its original disk space and memory are reliably scrubbed to ensure user data security.

3.4 Secure Development

AIs are responsible for establishing processes and procedures, implementing security measures, and conducting security assessments throughout the development lifecycle to ensure systems are resilient against cyber-attacks. Please refer to below for consideration to address the requirements of Section 3.4:

Key Aspects	Applicability	Consideration
Secure development	AIs & Alibaba Cloud	AIs *System Development Life Cycle (SDLC) Framework* AIs are responsible for establishing own SDLC framework to define the requirements and procedures to be followed during application development. AI should centralize the development process starting from feasibility study to post-implementation phase. It is important for AIs to note that security requirements including access control, authentication, authorization, data integrity, logging, security event tracking, and exception handling should be embedded into every phase or activity of the SDLC. During SDLC, security testing should be conducted by AIs to identify

		security vulnerabilities and remediate those before launching. Alibaba Cloud provides different testing services including penetration testing service, vulnerability scanning features embedded in cloud products. Refer to section “Penetration / Simulation Testing” for details on how Alibaba Cloud supports AIs in testing during development and post implementation stage. Alibaba Cloud *Secure Product Lifecycle (SPLC)* Alibaba Cloud has established SPLC for cloud product development which integrates security into each stage of the product development lifecycle. To ensure that products meet the rigorous requirements for cloud computing, a complete security development mechanism is divided into six (6) different stages, from product initiation, security architecture review, secure development, security validation, product release, to incident response. - In the product initiation stage, the security architect works together with the product team to establish a Function Requirement Document (FRD) and a detailed architecture diagram based on the business requirements and the technical frameworks. The teams also extract the security baseline requirements applicable to a product. Meanwhile, applicable security training courses and exams are arranged for the product team in this stage to prevent security risks in the subsequent phases in the lifecycle. - In the security architecture review stage, the security architect evaluates the security architecture of the product based on the FRD and the architecture description and build threat models for the new product. Based on the security baseline requirements and the security solutions proposed in threat modelling, the security architect then works with the product team to determine all the security requirements for the product. - In the secure development stage, the product team develops the product in accordance with Alibaba Cloud’s secure coding standards and security requirements and implements relevant security features. To ensure rapid and continuous development, release, and deployment of cloud products, the product team carries out self-testing in this stage to ensure that the security requirements have been implemented.

		Corresponding test information such as code implementations and test reports are prepared for security validation. - In the security validation stage, Security Team performs security reviews on the architecture, design, and server environment of the product. The team also performs code review and penetration testing on the product if applicable. Source code builds are scanned for malware prior to production release, any product with issue identified in this stage must be amended. - In the product release stage, only the product that has passed the security validation and acquired the security approval can be deployed to the production environment through a standard deployment system. - In the incidence response stage, the security incident response team constantly monitors the cloud platform to discover possible security problems and identifies security vulnerabilities through internal and external channels as well as self-security scanning. Refer to “Threat & Vulnerability Management” section for details. *Separation of Environments and Segregation of Duties* Alibaba Cloud has implemented access controls around the change management process to ensure that access to productive systems follow the principle of least privilege and segregation of duties. Segregated environments for development, testing and production have been implemented and access to different environments is controlled and restricted to authorized personnel only. 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. *Source Code Management* Alibaba Cloud has developed an internal source code repository to control changes made to the source code to ensure a high level of code security for Alibaba Cloud products. Alibaba Cloud’s source code repositories are used to store source code

		and track changes in source code during development for version control. With the authorization management function, access permissions to the source code are properly managed based on the principle of least privilege. In addition, in the SPLC of cloud products, Alibaba Cloud security experts strictly review and validate the source code security. Alibaba Cloud also constantly performs code security scanning for software in Alibaba Cloud Marketplace to effectively manage security risks.

3.5 Patch and Change Management

AIs should establish formal patching processes and controls to ensure systems are up-to-date and secure against vulnerabilities and operational concerns. Formal change management processes should be also implemented with standardized methods, procedures, and tools to minimize the risk and impact of change-related incidents to ensure operational efficiency. Please refer to below for consideration to address the requirements of Section 3.5:

Key Aspects	Applicability	Consideration
Patch management program	AIs & Alibaba Cloud	High level responsibilities over patch management between Alibaba Cloud and customer have been defined in the Alibaba Cloud Security Whitepaper (See “Useful Resource – 2. Alibaba Cloud Security Whitepaper, Version 2.0”), which is publicly available for user entities on Alibaba Cloud official website. Alibaba Cloud is responsible to secure the cloud platform from several aspects, including but not limited to: • Protecting the security of hardware, software, and network of the cloud platform by means of OS and database patch management; and • Identifying and fixing security vulnerabilities of the cloud platform in a timely manner without affecting customers’ service availability. Meanwhile, AIs who build cloud applications on Alibaba Cloud are responsible for protecting their systems by using the security features provided by Alibaba Cloud services and third-party security products in the Alibaba Cloud security ecosystems. While AIs do not need to
Patch assessment and testing	AIs & Alibaba Cloud	

Key Aspects	Applicability	Consideration
		maintain the underlying computing instances such as keeping the OS updated, hardened, or patched, AIs should harden the OS on their ECS instances and install security patches in a timely manner. AIs AIs are responsible for establishing a patch management program in order to ensure software and firmware patches are applied promptly. Alibaba Cloud's Cloud Firewall is equipped with artificial Intelligence engine which provides virtual patching function so that hot patches can be automatically applied at network layer to protect cloud assets against high-risk vulnerabilities and emergency vulnerabilities that can be remotely exploited. Customizations for virtual patch policies are also allowed, for example, AIs can manually enable or disable certain patches based on criticality. AIs should establish a formal patching process to acquire, test, and deploy software patches based on criticality and a follow-up process to classify and track actions based on priority to ensure timely closure. Systems maintained by AIs should be configured to retrieve patches from the official sources in a pre-defined patch window with patch management reports reviewed for identifying missing security patches across all environments. Before patches are deployed to the production environment, AIs should also ensure the operational impact is evaluated, **and such patches are tested and implemented within aggressive patch frames.** AIs should consider implementing automatic patching mechanism through deploying **patching monitoring software on all servers to facilitate identification of missing patches for OS, middleware, database, and other key software, and the number of day since each patch became available as well as support large scale and rapid patching based on automatic prioritization according to the inherent risk of AIs' systems.** AIs should maintain a backlog of vulnerabilities and conduct regular review on outstanding items, which should be escalated to senior management on a risk-based approach for their endorsement. ACK offers AIs the ability to setup testing environment with the same

Key Aspects	Applicability	Consideration
		configuration setting of production environment thus to perform patch testing for testing the stability of the system in advance of official deployment. Alibaba Cloud Alibaba Cloud is responsible for ensuring the security of hardware, software, and network of the cloud platform by means of OS and database patch management. Alibaba Cloud would identify security vulnerabilities from internal and external sources and fix such vulnerabilities through hotfix dynamical patching technology in a timely manner without affecting service availability. Patches and security updates are assessed and tested before deploying to the production environment.
Change management process	AIs & Alibaba Cloud	AIs AIs are responsible for establishing a change management process for changes to IT system configurations, hardware, software, applications, and security tools and ensuring cybersecurity risk is adequately assessed during the analysis, approval, testing, implementation, and reporting stage of changes. AIs are responsible for implementing internal security controls to manage changes. Any changes to the baseline IT configurations must be subject to formal change requests, documented approvals, and assessment of security implications. The approver should be an authorized individual or committee with appropriate knowledge, authority, and separation of duties. **AIs can use Cloud Config which monitors and continuously evaluates the configurations of Alibaba Cloud resources. It retrieves the configurations of all resources by calling API operations of the corresponding cloud services hence tracks the changes and compliance status of configuration in order to detect and block any unauthorized changes to cloud services.** **In addition, a change management system should be deployed with pre-defined thresholds for determining whether and when a cyber risk assessment of the impact of the change is required.** Alibaba Cloud

Key Aspects	Applicability	Consideration
		Alibaba Cloud has established a standardized change management process to ensure that all changes made to the cloud platform are recorded, evaluated, tested, approved, and where necessary, communicated prior to implementation into production following formal policies and procedures. An independent team has been set up to oversee the change management process, monitor compliance with the change management policies and procedures, and investigate on security incidents or malfunctions caused by uncontrolled changes. All changes that would affect the cloud operation, including changes to data, software and configuration, supporting infrastructure, hardware and network, need to go through a series of phases from application, testing, evaluation, approval, implementation, to verification. 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 the change management system, with status of each stage recorded and supporting documentation retained. Changes are classified by Alibaba Cloud based on the degree of emergency as well as impact of potential system malfunctions. Changes are also managed by category based on their sources and targets, that 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. 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. Subsequent to the testing, 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 must be approved by

Key Aspects	Applicability	Consideration
		authorized personnel before migration into the production environment. During the implementation phase, change scheme, plan, assessment, and implementation are documented. For large scale changes, Alibaba Cloud adopts canary release technique and deploys changes into production by rolling out the tested and approved changes by phases. During the canary release process, product teams closely monitor the status and carry out rollback procedures when needed. After changes are implemented, changes are verified; configuration item is reviewed; and changes results are notified. In addition, where applicable, Alibaba Cloud sends a change notice to AIs who may be affected by the change.

3.6 Remediation Management

AIs should have formal processes and procedures in place to remediate any identified issues in a timely and effective manner, while the remediation expectations and proposed risk mitigation strategies should be established and escalated to senior management for approval. Please refer to below for consideration to address the requirements of Section 3.6:

Key Aspects	Applicability	Customer Consideration
Remediation management	AIs & Alibaba Cloud	<u>AIs</u> Alibaba Cloud offers different solutions to assist AIs in identifying potential and exploitable vulnerabilities associated with cloud services and in performing penetration tests, simulation exercises, etc., please refer to “Vulnerability Detection” section below for further detail. Formal processes should be put in place by AIs to resolve weaknesses and issues identified in the cyber risk assessments and during penetration or simulation testing. Such issues should be prioritized and resolved based on criticality and within time frames defined in the assessment reports. For remediation performed, AIs should conduct a follow-up vulnerability scan and/or repeat simulation testing to confirm the remediation efforts and medium- and high-risk exploitable vulnerabilities are remediated. AIs can use the vulnerability scanning feature of Security Center to re-scan

Key Aspects	Applicability	Customer Consideration
		the repaired systems and applications for confirming that vulnerabilities are remediated. For simulation testing, Alibaba Cloud provides penetration testing service to assist AIs in reperforming simulation testing. Refer to “Penetration / Simulation Testing” section for details. **AIs are responsible for ensuring that maintenance and repair of own organizational assets are performed by authorized individuals with approved and controlled tools, with the process logged and reviewed in a timely manner. Refer to the relevant sections in the Whitepaper for access controls and logging features provided by Alibaba Cloud products to ensure only authorized individuals can maintain and repair organizational assets with the process logged and reviewed.** **AIs should also ensure that all critical and high-risk issues identified in the security testing activities including undesirable testing results are escalated to the Board or an appropriate Board Committee for risk acceptance with adequate mitigating measures if not resolved promptly.** Alibaba Cloud Security incidents, vulnerabilities, and threats identified by Alibaba Cloud will be gathered into the security incident and vulnerability management platform. Alibaba Cloud Security Team reviews incident and vulnerabilities on a daily basis and appoints appropriate personnel for resolution. Moreover, penetration tests are conducted semi-annually by an external third-party with corrective actions taken on identified vulnerabilities.

Domain 4: Detection

Domain 4 of C-RAF 2.0 established the expectation on detection of vulnerabilities, anomalies activities, and cyber incidents and AI’s threat monitoring and analysis.

4.1 Vulnerability Detection

AIs should establish controls and procedures to detect, filter, and block vulnerabilities and technical security weaknesses such as malware. Alibaba Cloud provides various security solutions for AIs to address the requirements of Section 4.1:

Key Aspects	Applicability	Consideration
Antivirus and anti-malware	AIs	AIs AIs should ensure that anti-virus and anti-malware solution and endpoint protection mechanisms are deployed, **centrally managed, and updated automatically (e.g., user behavioral detection rules and signature definitions). User and entity behavioral analytics (UEBA) and EDR solutions should be considered according to AI's inherent risk level.** Alibaba Cloud's Security Center is a cloud-based endpoint protection solution to protect connected endpoints from malware and virus attack. Security Center monitors and analyzes files and processes in the cloud in real time at the server system kernel level through the Security Center agent, effectively bypassing the anti-detection and anti-removal capabilities of trojans and malicious programs. It can also analyze program behaviors, and detect unidentifiable malicious threats in blacklists to actively intercepts them. The virus database in the cloud is updated in real time and integrates advanced technologies such as mainstream anti-virus engines in and outside China, Alibaba Cloud Sandbox, and the machine learning engine. Besides, Security Center also possesses the UEBA capability. It can detect threats based on user behaviors and identify internal and external security threats. With the machine learning and deep learning technologies, over 200 security threat detection models are already available for detecting potential security threats. Apart from endpoint protection, Alibaba Mail protection mechanisms can filter common cyber threats such as attached malware, malicious links, and e-mail viruses, etc. The phishing feature database and the anti-virus engine are maintained and updated by the Alibaba Cloud Security Team. It also provides an anti-spam system to automatically recognize e-mail spam by using the anti-attack and anomaly detection feature, the user behavior and email content inspection feature, and the identity recognition feature. Moreover, AIs can design a whitelist or blacklist to

		filter inbound e-mails.
Penetration / Simulation Testing	AIs & Alibaba Cloud	AIs It is AIs' responsibility to ensure penetration testing is performed on web-based systems or devices before they are launched or undergo significant changes, and *vulnerability scanning is rotated to scan all high-risk systems in the production environment throughout the year and endpoints on a risk-based approach.* *AIs are also responsible to ensure simulation testing is conducted on a regular basis or after significant change that leads to increase of risks and system availability of the services. AIs should define appropriate test scenarios, scopes and cases and engage audit or risk management resources to review the simulation testing scope and results in order to help determine the need for rotating companies based on the quality of the work.* Alibaba Cloud offers penetration testing services that simulate full-scale, in-depth attacks to test AI's system security and identify risks in the business process such as security defects and vulnerabilities. The service process covers from test scope determination, planning of test level with different scenarios, implementation of testing on business systems, web applications, networks, and operating systems, to delivery of test reports that include test process, risk status, vulnerability details, and fix suggestions. According to AIs' risk assessment results, routine penetration testing and vulnerability scanning should be conducted. Apart from penetration testing service, Alibaba Cloud also supports AIs to conduct vulnerability scanning using cloud products such as Security Center and Cloud Security Scanner (CSS). AIs can utilize the services and features to conduct various types of vulnerabilities assessment routinely. For example, AIs can use Security Center to run scan tasks for detecting vulnerabilities on assets and list of which that require immediate fixing. AIs can also schedule task in CSS to perform vulnerability scanning on web applications and obtain recommendations on resolving such vulnerabilities in the CSS console. In addition, Container Registry allows

		AIs to perform security scanning on all Linux-based images to identify vulnerability in four (4) levels, namely high, medium, low, and unknown. AIs can configure an automatic scanning task that permits Container Registry to perform periodic vulnerabilities assessment. Alibaba Cloud Alibaba Cloud has developed plans to conduct attack-and-defense drills on the cloud platform. During a drill, Alibaba Cloud organizes a team of penetration and attacks experts to share their attack technologies and penetration knowledge to identify vulnerable area of the cloud platform by means of periodic attack-defense confrontation. Discovered vulnerabilities are documented and analyzed. In addition, penetration tests are conducted semi-annually by an external third-party engaged with Alibaba Cloud. The identified vulnerabilities are documented and analyzed, and corrective actions are taken as necessary.

4.2 Anomalies Activity Detection & 4.3 Cyber Incident Detection

AIs should establish processes and controls with automated tools implemented for continuous monitoring and detection of malicious security behavior and cyber incidents, such as unauthorized connections and deviations from normal user behavior or patterns. Meanwhile, associated investigations should be conducted on an ongoing manner. Please refer to below for consideration to address the requirements of Section 4.2 and 4.3:

Key Aspects	Applicability	Consideration
Log monitoring and analysis	AIs & Alibaba Cloud	AIs AIs are responsible for establishing process and mechanism in monitoring logical access, particularly privileged access, within own cloud environment and resources deployed on cloud in order to detect any anomalous behavior (including during authentication process) by customers, employees, and third-parties. Logical access logs should be reviewed following events. Therefore, to facilitate monitoring and incident investigation, logs should be available to provide traceability for all system access by individual users. Alibaba Cloud's ActionTrail monitors and records actions performed by Alibaba Cloud accounts and RAM users, including the access to and use of cloud

Key Aspects	Applicability	Consideration
		products and services. AIs can view the event records directly on the ActionTrail console or monitored resource and perform log analysis to detect anomalous operations. In addition, Dbaudit provides AIs to deploy built-in or customized security rules to detect potential threat to database instances, and alert will be generated to users for investigation. AIs can also review access and operation logs for routine monitoring purpose. Log Service supports collection and analysis of user activity and network activity logs from multiple types of Alibaba Cloud services including ActionTrail. With Realtime Compute, log records can be transformed that AIs can export the restructured log records from Log Service to the Security Information and Event Management (SIEM) maintained by AIs. AIs can design scenarios and use cases to analyze and correlate logs from different sources to identify and analyze anomalous behaviors. AIs are also responsible for log management. For example, AIs should ensure devices and logs are synchronized with a centralized and secured time source. In relation to this, Alibaba Cloud provides a Network Time Protocol (NTP) server to achieve synchronization local time of ECS instances thus making timestamp reliable. Furthermore, AIs should ensure that audit log records and other security event logs are retained securely. *Audit logs should be backed up to a centralized log server or media to prevent unauthorized changes, and security logs for key systems and endpoints should be readily available for review with adequate retention period for incident response investigation.* In view of this, logs collected by Alibaba Cloud's Log Service could be shipped to OSS for backup purposes. AIs can configure appropriate bucket policies to achieve the following: - By enabling Write Once Read Many (WORM) settings, no modification could be done to the concerned bucket thus prevent changes to security logs; and - Defining retention period so that critical logs will be retained within the defined retention period to allow future investigation. It is important for AIs to review periodically the logging practices and thresholds for security logging to ensure that appropriate log management is in place.

Key Aspects	Applicability	Consideration
		Alibaba Cloud All activities performed in Alibaba Cloud's 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.
Security information and event management & Event monitoring & Detection and alert	AIs & Alibaba Cloud	AIs With cloud adoption, AIs are responsible for security event monitoring on cloud environment and resources deployed on cloud which include critical assets. *AIs should ensure that effective monitoring mechanism is established, and automated processes including instant alerts to detect incident in real-time should be deployed. Responsibilities of monitoring is assigned to authorized individuals with escalation protocol clearly defined to ensure immediate response by appropriate personnel. The monitoring mechanism should be 24x7 and cover detection, investigation, and root cause analysis of threat activities.* AIs should establish a process to monitor and detect anomalous activities across environments. Although ActionTrail is available to facilitate logging of certain activities and operation events, it is AIs' responsibilities to define the thresholds that determine activity warrant management response and ensure *solutions are deployed to actively monitor security logs* **and actively correlate event information from multiple sources** *for anomalous behavior and provide alerts within established parameters.* Alibaba Cloud offers Log Services which enables AIs to gather logs, configure policies and rules to perform correlation analysis and trigger alerts once the established parameter or pre-defined conditions are met. A process should be put in place to correlate event information from multiple sources including networks, applications, firewalls, and endpoints. Log Services can collect logs from multiple sources. After that, logs can be shipped to Security Center to analyze attack patterns or signatures of anomalous behaviors. Alerts are generated to AIs and suggestions for follow-up actions are provided to AI for reference. The HKMA has defined various scenarios across Domain 4 where AIs

Key Aspects	Applicability	Consideration
		should consider when designing the monitoring mechanism i.e., correlation rules, for example: - Suspicious systems activities, including presence of unauthorized users, devices, connections, and software in logical environments; - *Potential and unusual insider activities that could lead to data theft or destruction;* - *Unauthorized data mining;* - *Discover any infiltration since attackers may traverse across systems, establish a foothold, steal information, or cause damage to data and systems;* - *Multi-faceted attacks (e.g., a simultaneous account takeover and DDoS attack) should be detected by correlating anomalous activities, network and system alerts across business units and the enterprise; and* - **Unauthorized changes to critical system files, firewalls, IPS, IDS, or other security devices.** Apart from Log Service, Alibaba Cloud also offers other solutions to enhance AIs' monitoring capabilities. *Network Traffic Sniffer / Network Monitoring Tool* Cloud Firewall can visualize network traffic, access between businesses, and store network traffic logs generated within the last six (6) months. *AIs should establish a normal network activity baseline* and monitor network activities according to the baseline. **AIs may also utilize network monitoring feature to detect network-based attacks associated with anomalous ingress or egress traffic patterns and/or DDoS attacks and consider deploying defense-in-depth techniques such as Anti-DDoS solutions for timely response.** **Alibaba Cloud provides Anti-DDoS Basic, Anti-DDoS Pro and Anti-DDoS Premium service to prevent AIs' services on the Internet become unavailable due to DDoS attacks. By default, Anti-DDoS provides an anti-DDoS capacity of up to 5 Gbit/s for free. In addition, Alibaba Cloud has launched the Security Credibility plan.**

Key Aspects	Applicability	Consideration
		After becoming a member of Security Credibility, AIs can enjoy additional DDoS mitigation capacity on top of the default offering based on AIs' security credibility score. While Anti-DDoS Pro and Anti-DDoS Premium are designed for AIs who deploy their resources on or off Alibaba Cloud. By using the massive traffic scrubbing center resources of Alibaba Cloud, both products work together with the artificial intelligence protection engine and adopt full-traffic proxy to protect against high-volume traffic attacks and refined web application level resource exhaustion attacks such as HTTP flood attacks. *Data Loss Prevention Tool* Controls or tools (e.g., data loss prevention) should be implemented to detect potential unauthorized or unintentional transmissions of confidential data. SDDP as a measure for monitoring sensitive data or files can be implemented to prevent losses, detect anomalous activity, and monitor access to sensitive data assets. Other than SDDP, Security Center generates alerts for malicious processes and scripts such as inserting mining programs and suspicious network activities including communication activities with mining pools. *Endpoint Detection and Response* *AIs should ensure that endpoint behavioral detection capabilities are available on endpoints* **and all critical systems which include key servers. AIs should also implement a system to monitor and analyze employee behavior (e.g., network use patterns, work hours, and known devices) and provide alerts for anomalous activities.** Security Center can evaluate malicious behavior covering all endpoints including critical systems and servers. Its algorithm consists of machine learning and deep learning as well as large amounts of threat intelligence data to track known threats more effectively. Network monitoring and detection could be done in real-time. *System Performance Monitoring* AIs can use system performance reports as a risk indicator to detect

Key Aspects	Applicability	Consideration
		cyber incidents and set alert parameters to detect cyber incidents that prompt mitigating actions. Application Real-Time Monitoring Service (ARMS) generates 3D topology graphs to identify health status and locate incident indicators such as abnormal services, affected applications, and associated hosts to detect cyber incidents. AIs can also monitor the availability of hosts by installing a CloudMonitor agent on the servers to automatically retrieve cloud service resource under Alibaba Cloud accounts. AIs can locate issues as risk indicators to detect cyber incident based on the monitoring result generated by CloudMonitor. Alibaba Cloud Network Monitoring Alibaba Cloud has installed intrusion detection software on servers to detect potential intrusion behavior. A network monitoring system and tools are utilized to monitor network traffic and user operations in real-time and identify abnormal operations. The security team personnel will follow up on any abnormal operations identified by the network monitoring system and take necessary actions. Event and Incident Monitoring In terms of security events and incidents, Alibaba Cloud's security incident management ensures secure operations and system protection through monitoring and detection of security events, as well as timely execution of proper responses to those events. Alibaba Cloud has established security incident response standards and guidance to regulate classification, escalation, and notification processes for security incidents. Alibaba Cloud conducts security monitoring on the cloud platform to detect security incidents where platform resources are attacked, and the security incident response process will be triggered to properly handle the incidents. Activities performed on the cloud platform are logged and imported into real-time and offline computing platforms. Logs are processed and analyzed through security monitoring algorithms in each

Key Aspects	Applicability	Consideration
		computing platform for anomaly analysis and detection. The Alibaba Cloud security team is established for analyzing, tracking, and coordinating responses to incidents. The team reviews the results on the security incident monitoring platform to verify whether any of the events should be classified as security incidents. Confirmed security incidents will be notified and escalated to the appropriate teams for timely response based on criticality and severity levels of the incident. For security incidents that could impact customers, Alibaba Cloud would establish announcements on the Alibaba Cloud official website. *Physical Security Monitoring* Alibaba Cloud is responsible for the physical security of its data center facilities. For more details, please refer to “Physical access management” in Section 3.1 Access Control.
Customer transaction monitoring	AIs	AIs AIs are responsible for performing customer transaction (e.g., online transaction, external transfer) monitoring and implement *automated alert mechanism to detect anomalous activities such as customer logins within a short time period from physically distant IP locations*. AIs may utilize different solutions offered by Alibaba Cloud to facilitate monitoring, for example: Fraud Detection provides business risk intelligence feature to protect AIs against false information exploited in online fraud such as malicious fraud, cheating, and fraudulent transactions. The large amount of cloud-based big data in Fraud Detection includes accumulated diversified characteristics of fraud and effective anti-fraud policies and algorithms to help AIs defending online fraud. Besides, Alibaba Cloud provides big data processing and computing service with a variety of classic distributed computing models built-in to help AIs tackle large-scale data computing problems such as sophisticated customer transaction monitoring.

4.4 Threat Monitoring and Analysis

AIs should establish procedures and ensure adequate resources are in place to identify threats

throughout the continuous monitoring of threat intelligence to minimize cyber risk exposure. Please refer to below for consideration to address the requirements of Section 4.4:

Key Aspects	Applicability	Consideration
Threat monitoring and analysis	AIs & Alibaba Cloud	AIs To identify emerging threats, AIs are responsible for establishing procedures to monitor and prioritize threat intelligence sources that address all components of the threat profile *and assigning responsibilities in monitoring and analyzing threat intelligence to a specific group or individual.* *AIs should consider establishing a Security Operations Center (SOC) with cyber-surveillance and incident response capability, or other equivalent services, to centralize and coordinate security processes and technologies mentioned in the previous sessions in this Whitepaper so that monitoring systems can operate continuously (i.e., 24x7) to provide adequate support for efficient incident handling.* **AIs should ensure that threat intelligence is constantly gathered and analyzed, the gathered threat intelligence should be viewed within the context of AIs' risk profile and risk appetite. Analyzed threat intelligence can be used to develop threat summary reports which include cyber risk details and specific actions and prioritize for mitigating actions, such as to update IT security architecture and IT configuration standards.** **In relation to threat monitoring and analysis, Alibaba Cloud provides security solutions with intelligence protection feature to support automatic detection and defense against threats. For example:** – **Cloud Firewall utilized a built-in AI engine, which monitors more than five (5) million active malicious IP addresses and domain names. It provides intelligence protection by generating information about threats detected by the Alibaba Cloud Security Team and automatically block malicious network traffic using Cloud Firewall and its built-in IPS; and** – **Besides, Security Center also adopts machine learning,**

Key Aspects	Applicability	Consideration
		deep learning, UEBA, threat intelligence, AV engine, and other security capabilities to build an in-depth three-dimensional threat detection architecture, so that threats can be detected and attacks can be tracked in efficient manner. **Apart from utilizing cloud solutions, AIs should also subscribe multiple sources of threat intelligence and utilize the analysis result of logs across environments, alerts, internal traffic flows, and information about geopolitical events in order to predict potential future attacks and attack trends.** Alibaba Cloud Alibaba Cloud's threat and vulnerability management ensures the security of Alibaba Cloud and its customers' environments by detecting system flaws and unauthorized actions and taking remediation or mitigating actions on a timely basis. Alibaba Cloud has established Alibaba Cloud Security Incident Response System Guideline to regulate security vulnerability management, including classification of security vulnerabilities and response mechanism. Security incidents and vulnerabilities are reported and detected by multiple means, including internal reporting, external reporting, internal vulnerability scanning, and subscription from external vulnerability publishing platforms. The external reporting channels include Alibaba Security Response Center, Alibaba Cloud Crowdsourced Security Testing Platform, and external threat intelligence sources such as RedHat, Microsoft, Cisco, Apache, etc., for externally reported Common Vulnerabilities and Exposures (CVE) vulnerabilities. Security incidents and vulnerabilities collected via the above channels are then gathered into the security incident and vulnerability management platform. The Alibaba Cloud security team reviews the incidents and vulnerabilities on a daily basis to verify the authenticity of the reported incidents and vulnerabilities. Once the security incidents and vulnerabilities are confirmed, the security team will initiate the incident response process and appoints appropriate personnel for resolution. The incident response team will rate the security incidents

Key Aspects	Applicability	Consideration
		and vulnerabilities, determine their priority, and schedule for resolution. Meanwhile, customers shall be promptly notified of security issues through online announcements.

Domain 5: Response and recovery

Domain 5 of C-RAF 2.0 established the expectation on cyber incident response and recovery (CIRR) management ranging from governance across the institutions, preparation of incident response plans and playbooks, collection of cyber forensic evidence, to overall communication and improvement. AIs should establish formal CIRR management framework and formulate the procedures of analysis, mitigation, and restoration to ensure cyber resilience in the event of a cyber incident.

5.1 Governance and Preparation of Incident Response and Recovery

While Alibaba Cloud offers different security solutions to protect asset security and enhance system resilience, AIs should establish a comprehensive framework and processes for CIRR. Please refer to below for consideration to address the requirements of Section 5.1:

Key Aspects	Applicability	Consideration
Governance of incident response and recovery	AIs & Alibaba Cloud	<u>AIs</u> AIs are responsible for establishing an incident response management framework and program with the following objectives and processes: - Define the CIRR objective; - Define roles and responsibilities of each of the parties (both business and IT) and ensure they are aware of their roles in the event of cyber incidents; - Ensure the Board and senior management oversee CIRR management and provide adequate governance; - *Establish direct cooperative or contractual agreements with and perform due diligence on the incident response organization(s) or provider(s) such as technical sources, consultants, or forensic*

		service firms that would be called upon to assist the institution during or following an incident; - *Ensure that management reviews any changes to the processes, systems/applications, or the access of the entitlements necessary for cyber incident management before implementation. Alibaba Cloud provides different solutions to allow AIs to detect authorized changes to systems/applications or access entitlements; please refer to the corresponding sections; and* - **Ensure that methods for responding to and recovering from cyber incidents are tightly woven throughout the business units' disaster recovery, business continuity, and crisis management plans.** <u>Alibaba Cloud</u> Alibaba Cloud's security incident management ensures secure operations and system protection through monitoring and detection of security events, as well as timely execution of proper responses to those events. Alibaba Cloud has established security incident response standards and guidance to regulate classification, escalation and notification processes for security incidents. Besides, Alibaba Cloud has also established malfunction management standards and procedures to regulate malfunctions, including classification, requirements for timely response, as well as escalation and resolution according to risk level, to ensure that problems or malfunctions are identified, evaluated, escalated, and resolved in a timely manner.
Incident response and recovery preparation	AIs & Alibaba Cloud	<u>AIs</u> AIs should document contingency plan to detail processes and procedures for responding and restoring critical functions and systems in the event of a cyber incident. Plans and playbooks should be established to provide well-defined, organized approaches for CIRR services covering different cyber scenarios including severe but plausible cyber scenarios, the criteria for activating the measures and actions to be taken during most critical period. Moreover, business impact analysis, business

		continuity, disaster recover, crisis management plans, and data backup programs should be put in place to recover critical activities and operations following a cyber incident. The recovery objectives (e.g., Recovery Time Objective (RTO), Recovery Point Objective (RPO)), restoration priorities, and metrics should be defined. In addition, AIs may consider engaging qualified third-party service providers (including primary and alternate) to augment resiliency, for example, **to assess from an attacker's perspective, how its assets may be targeted, and validate that there are adequate fail-safes to minimize the impact on interconnectivity and dependencies on third parties in the event of response and recovery**. A retainer agreement should be also established to call upon them as needed to support CIRR activities. To ensure smooth response and recovery, *it is AIs' responsibility to prepare detailed plans (e.g., re-route or substitute critical functions and/or services that may be affected by a successful cyber-attack) for the resumption of essential missions and business functions in accordance with recovery objectives of contingency plan activation.* Apart from maintaining effective plans, several protection measures should be adopted. While Alibaba Cloud provides high available cloud services to AIs. AIs are responsible for building and maintaining resilient architecture by setting geographically diversified backup facilities and ensure isolation through network and system configurations to avoid concentration risks. Alibaba Cloud has three data centers (i.e., Availability Zone) in Hong Kong providing active-active services. AIs could choose the Availability Zone on Alibaba Cloud Console to deploy system and data. **AIs can also implement multiple systems, programs, or processes within a comprehensive cyber resilience program to sustain and recover operations from an array of potentially disruptive and destructive cyber incidents. In regard to this matter, Alibaba Cloud provides various products to facilitate AIs in building a high resilience architecture to ensure high availability of AIs' systems and services:** *Server Load Balancer* SLB is a load balancing service that distributes traffic among multiple ECS instances and improves the service capabilities of applications. AIs

		can use SLB to prevent Single Points of Failure (SPOFs) given that SLB is designed with full redundancy and supports zone-disaster recovery. 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. By integrating with Alibaba Cloud Domain Name System (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. *Elastic Compute Service* By default, the availability of a single ECS instance is 99.975%. The availability of multiple ECS instances across regions is 99.995%. With the integration with SLB service, multiple ECS instances can be clustered to eliminate SPOFs and improve application availability. Data stored in ECS instances also enjoy high resiliency: images and snapshots of ECS instances are stored in triplicate, distributed across physical servers to provide an availability of 99.9999999%. Further, ECS instances are deployed on physical hosts (physical servers) that may fail due to performance anomaly or hardware failures. After detecting a fault on a host, the system will trigger a protective migration to migrate the ECS instances on the host to a normal host automatically to ensure the normal operation and high availability of instances and applications. *Object Storage Service* With the “redundant storage across zones” mechanism, OSS replicates three copies of data to three different zones within the same region. The mechanism ensures data availability when one of the zones is unavailable. With this redundant storage mechanism, OSS achieves 99.9999999999% data durability (designed for) and 99.995% service availability (designed for). The redundant storage mechanism provides OSS with the disaster recovery capability at the data center level, that is, OSS can provide services with strong consistency even if a data center is not available

		because of network disconnection, power outage, or other disaster events. During failover, services are switched without interruption or data loss, ensuring that the failover process is transparent to users. With this disaster recovery capability, OSS can meet the strict requirement that the RTO and RPO must be zero for critical applications and services. *ApsaraDB for RDS* RDS supports multi-zone instances that are also known as zone-disaster recovery instances. These instances provide higher availability than single-zone instances. A multi-zone instance runs on physical servers deployed in different zones. When a failure occurs in a zone, the system immediately switches the workloads to another zone automatically. RDS also supports cross-region data disaster recovery. For example, AIs can asynchronously replicate Instance A' in Region A to Instance B' in Region B by using the Data Transmission Service. Instance B' is a complete and independent RDS instance, and has different connection addresses, accounts, and permissions from Instance A'. *Alibaba Cloud Container Service for Kubernetes* Container Service auto-scales resources according to the scaling rule configured by AIs so that it will scale up the application i.e., create additional nodes and forward traffic to the scaled-up resources when there is excessive amount of inbound traffic that takes up resources to ensure the availability of the application deployed on cloud. Besides, Container Service allows users to create Kubernetes clusters and deploy in-house developed application in the containers using custom image within short period of time to ensure the target recovery time objective can be met. *Block Storage* Block storage uses a three-copy distributed mechanism and provides a data durability of 99.9999999%. Block Storage can automatically replicate data across different servers within a zone and prevents data unavailability due to unexpected hardware failures. Alibaba Cloud Alibaba Cloud has established Alibaba Cloud policies and guidelines of business continuity management to ensure that critical business

		operations could be recovered in a time manner in the event of a disruption. A Business Continuity Management framework has been established consisting of business impact analysis, risk assessment, as well as maintenance, implementation, testing, and continuous improvement of Emergency Response Plan and Business Continuity Plan (BCP). The Business Continuity Management team performs Business Impact Analysis (BIA) and risk assessment on an annual basis, where 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. Based on the BIA and risk assessment result, Alibaba Cloud has developed BCPs to outline business recovery procedures in the event of business disruptions. The BCPs are subject to annual review and are updated as necessary. Alibaba Cloud has also established Alibaba Cloud Emergency Response Plan to define classification of emergencies, roles and responsibilities, response process workflow, and resource management for emergency response. Incident response plans have been established for responding to incidents as related to critical operations and services, network, and Internet Data Centers (IDC) infrastructure.

5.2 Analysis, Mitigation, and Restoration

AIs should have formal processes and strategies in place for incident analysis and resolution to minimize the impact of a cyber incident in a timely, secure, and resilient manner. Please refer to below for consideration to address the requirements of Section 5.2:

Key Aspects	Applicability	Consideration
Analysis	AIs & Alibaba Cloud	AIs AIs may formulate a process to identify cyber security incidents on cloud environment that are internal to AIs. For identified cyber incidents, AIs

Key Aspects	Applicability	Consideration
		should follow an established severity assessment framework and triage process to gauge the severity for incident classification and prioritize incidents accordingly. It is AIs' responsibility to identify cybersecurity incidents detected on cloud internal to the institution and *perform analysis of security incidents in the early stages of an intrusion to minimize the potential impact of the incident on critical business processes. Cloud threat detection of Security Center assists AIs in conducting threat identification, threat analysis, and malicious file quarantine and restoration thus AIs can enable such feature to receive and process security alerts, scan for early attacks, and analyze attacks and possible cyber incident by using the service.* **Moreover, AIs should develop links and correlations between threat intelligence, network operations, and incident response that allow proactive response. AIs can use the threat intelligence library in Security Center to perform correlation analysis on access traffic and logs to detect threat events and possible incidents, including access to malicious domains, malicious download sources, and malicious IP addresses.** Alibaba Cloud In terms of security incident, security on the cloud platform is monitored to discover security incidents where platform resources are attacked and trigger the security incident response process to properly handle the incidents. Logs of activities performed on the cloud platform are imported into real-time and offline computing platforms. Logs are processed and analyzed through security monitoring algorithms in each computing platform for anomaly analysis and detection. The security team is responsible for analyzing, tracking, and coordinating responses to incidents. The security team reviews the results on the security incident monitoring platform to verify whether any of the events should be classified as security incidents. Security incident discovered are notified and escalated to the appropriate teams for timely actions based on security incident's criticality and severity levels. For malfunction, Alibaba Cloud utilizes a malfunction management platform to identify, consolidate, track, and monitor malfunctions

Key Aspects	Applicability	Consideration
		discovered via different channels. Alibaba Cloud Global Operation Center (GOC) is responsible for managing malfunctions till resolution, in accordance with the established malfunction management standards and emergency response procedures. The GOC works with product teams to determine critical systems and events to be monitored on the malfunction management platform. When receiving an alert from the platform, GOC determines whether the alert pertains to malfunctions. When a malfunction is confirmed by GOC, the platform will automatically send an email notification to the impacted teams and initiate tickets for follow-up resolution. In addition to the automatic identification, GOC also collects cases of malfunctions through tickets created by customer service based on customer feedback and takes actions accordingly.
Mitigation	AIs & Alibaba Cloud	<u>AIs</u> In order to prevent unauthorized access to sensitive information and mitigate the potential impact, AIs can implement a process to help contain, control, and eradicate cyber incidents with **automated mechanisms deployed to support the process, where applicable.** *Processes should be established to enable the effective and prompt execution of eradication plans.* *Moreover, AIs are responsible to develop separate containment strategies for different types of major cyberattack, with criteria documented clearly to facilitate decision making,* and establish processes to trigger the incident response program when an incident occurs at a third-party (AIs will be notified by Alibaba Cloud in case of malfunction that may impact to AI's use of cloud services). In relation to high-impact, low-probability cyber incidents, Alibaba Cloud provides various products to facilitate the detection and mitigation process: *Data leakage* AIs can use Security Center to quarantine ransomware, mining programs, and malicious programs, etc. and perform data backup and restoration based on the specified time or file version for ECS instances subjected to ransomware attacks. Alibaba Cloud Data Security Center (DSC) automatically detects sensitive

Key Aspects	Applicability	Consideration
		data stored in data sources. AIs can perform security audits of various data sources in the cloud using DSC service. It provides powerful features in the anti-leakage scenario to help AIs implement threat detection on all data. DSC uses machine learning technologies to establish a security baseline for data access. If a potential data risk occurs, for example, the data of AIs is accessed at an unusual time or from an unusual location, the system promptly sends an alert to the AIs. DSC also provides the AIs with backtracking capabilities and protection suggestions. It turns static detection into dynamic perception to help AIs respond to data security incidents and improve overall response capability. *DDoS attack* Alibaba Cloud's DDoS protection packages are suitable for AIs whose services are deployed on Alibaba Cloud with a large business scale and demanding network quality requirements. Alibaba Cloud Anti-DDoS Premium can protect ECS instances and servers that are not deployed on Alibaba Cloud by routing concerned network traffic to Alibaba Cloud global anti-DDoS network to mitigate various types of attack including malformed packet attack, transport layer DDoS attack, DNS DDoS attack, connection-based DDoS attack, and application-layer attack. AIs can also monitor the protection status in real-time through security reports. Alibaba Cloud Alibaba Cloud has established procedures and implemented security measures to ensure the operation to be recovered with minimal impact to customers in the event of cyber incidents. *Containment and Mitigation Strategies* The BCPs document the roles and responsibilities of staff and recovery objectives in the scenarios of product-related and after-sales incident. Product-specific incident response plans have been established to provide guidance on emergency and incident response of specific product lines. Alibaba Cloud has also established incident response procedures to detail the process workflow in the event of IDC incidents. Contingency plans have been developed to address different scenarios of interruption to IDC, including fire, network interruption, emergency power outage, and natural disasters. After an incident occurs in the data centers, according to the risk

Key Aspects	Applicability	Consideration
		level and the nature of incident, data center service providers will submit Operation Incident Report to Alibaba Cloud, which covers the causes of the incident, scope of the impact, and resolution status. Apart from the documented procedures, Alibaba Cloud has deployed mitigation strategies, supplemented by internal controls and different layers of defense tools, to provide protection for multiple incident scenarios. These strategies include: - Security solutions such as firewall, IPS, SLB (with alternate switches, routers, critical nodes to avoid SPOF and hide the IP addresses of back-end servers), and DDoS protection; and - DLP software to detect sensitive operations performed on the PCs and prevent sensitive data leakage. *Data Redundancy and Replication* Alibaba Cloud has implemented security measures for data replication. Critical Alibaba Cloud system components that support customer services are designed to maintain high availability through redundancy and automatic failover to another instance with minimal disruption to customer services. These system components are replicated across multiple Availability Zones. Moreover, Alibaba Cloud Storage provides data redundancy through distributed storage to improve the availability of customer data. Files are split into multiple data segments and stored on different devices, with each data segment stored in multiple copies.
Restoration and quality assurance testing	AIs & Alibaba Cloud	<u>AIs</u> *Restoration* AIs should formulate restoration strategy to prioritize restoration activities based on business, security and technical requirements with key milestones identified. Related restoration procedures should be established, any deviation should be risk assessed, tested and approved by management before implementation where required. During restoration for incident internal to AIs, AIs are responsible to ensure IT assets damaged by a cyber incident are quarantined, removed, disposed of, and/or replaced with minimal service disruption. *Processes should be put in place to ensure that restored IT assets are appropriately*

Key Aspects	Applicability	Consideration
		reconfigured and thoroughly tested before re-using in operations. AIs can use Cloud Config to track the configuration changes and evaluate configuration compliance in real-time. Cloud Config continuously monitors and records the configuration change details of resources, compares the changes in detail, and organizes the configuration timeline of resources. Apart from that, AIs can specify a remediation template for a rule. Once a rule is triggered, Cloud Config re-evaluates the resource. If a resource is evaluated as non-compliant based on the rule, Cloud Config would remediate the resource in accordance with the settings. Backup program should be established by AIs to facilitate the restoration of data and systems. AIs can also use online backup service to back up and restore files for ECS instances and AIs can utilize Data Backup Service (DBS) to perform full and incremental logical and physical backup to database (note: physical backup is not applicable for RDS databases via DBS). 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. To cover databases that are not hosted on Alibaba Cloud, DBS can be integrated with DMS so that AIs can manage multiple databases regardless of the location they deployed, e.g., on cloud, on-premises hence users can manage the backup copies more efficiently and restore backup data at any time point when cyber incident happens. During the restoration process, AIs should also monitor external services, the network, and systems for abnormal activities. AIs can utilize Cloud Firewall to conduct network traffic monitoring and real-time intrusion defense. After restoration, AI should put in place process to validate that systems are operating as per intended and without the vulnerabilities that led to the initial compromise. AIs could use Security Center to conduct follow-up vulnerability scans on repaired systems and applications and verify whether the vulnerabilities are fixed. While AIs' will be notified by Alibaba Cloud on any incident that may impact to their use of cloud service and provide relevant information to AIs. It is AIs' responsibilities in maintaining proper documentation related to cyber incidents such as preparing incident report and submitting to

Key Aspects	Applicability	Consideration
		appropriate personnel for review and acknowledgement. However, for incidents that are internal to the cloud environment, actions taken from the time the incident was detected to its final resolution should be documented by AIs and timestamped. Tools and artefacts (e.g., scripts, configuration changes, etc.) used by AIs for restoration should be recorded for future use or for the improvement of current process and/or systems. *Furthermore, timely reporting and escalation of issues are critical during restoration phase, hence AIs should track and monitor any cyber incident escalations and resolutions and provide regular updates to AI's management.* *Quality Assurance Testing* In order to develop a comprehensive CIRR program, it is important for AIs to undertake quality assurance activities to ensure the effectiveness of CIRR plans and process and identify any improvement areas in timely manner. Different type of testing can be conducted by AIs with testing objectives properly developed to allow AIs to understand whether the CIRR and BCM controls conform to the defined framework and the ability of AIs to recover critical services/functions within the recovery objectives by following the policies and procedures. **AIs should also ensure critical business functions will participate in the regular exercises to evaluate the effectiveness of incident response and recovery capabilities of critical functions in the event of cyber incidents.** As highlighted in Domain 5 of C-RAF, the following are examples of quality assurance testing and relevant considerations for AIs: – Business continuity and data recovery testing should be conducted at least annually and involves collaboration among critical third-parties where applicable; – Regular testing of system and data integrity and recoverability from multiple copies of data backups should be also conducted to verify if these data are accessible and usable; – *Ability to withstand stresses by AI's critical online systems and processes for extended periods should be assessed. AIs can use Alibaba Cloud Performance Testing Service (PTS), which is a cloud-based stress testing platform that simulates real-world*

Key Aspects	Applicability	Consideration
		business scenarios of a large number of users and tests the performance, capacity, and stability of business sites; – *Resilience testing which includes scenarios based on analysis and identification of realistic and highly likely new and emerging cyber threats should be performed to validate the effectiveness of AIs' BCP and DRP;* – **Stress testing the cyber risk management by simulating cyber incident scenarios involving significant financial loss; and** – **To prevent interruption to business or loss of productivity or data during actual incidents, AIs should conduct testing to ensure the ability to shift business processes or functions between own processing centers or technology systems during cyber incidents.** **There may be problems discovered during the aforementioned cybersecurity resilience testing, AIs should establish process to correct root causes for discovered problem and enhance the CIRR program accordingly.** Alibaba Cloud *Restoration* Backup restoration procedures are in place, and critical Alibaba Cloud system components are restored on a monthly basis with reconciliation performed automatically for data integrity check. In addition, configuration scanning tool has been deployed by Alibaba Cloud to scan configurations of operating systems, database management systems, network devices, and virtual machine images. The scanning results are analyzed by the scanning tool and the analysis results are submitted automatically to the security incident and vulnerability management platform. Deviations from configuration baseline standards are detected and restored to the standard by Alibaba Cloud operation personnel. The detection and restoration results are summarized into a weekly report for rectification. *Quality Assurance Testing*

Key Aspects	Applicability	Consideration
		On an annual basis, Alibaba Cloud conducts a business continuity drill according to the planned procedures for critical Alibaba Cloud products. In addition, Alibaba Cloud conducts testing of data center business continuity plans for the continued operations of critical processes and required resources in the event of a disruption at least once a year.

5.3 Cyber Forensics

AIs should establish formal processes and procedures on forensic evidence collection and preservation to facilitate incident analysis and investigation. Please refer to below for consideration to address the requirements of Section 5.3:

Key Aspects	Applicability	Consideration
Process of collecting evidence	AIs	AIs *AIs are responsible to use generally accepted and appropriate forensic procedures, including chain of custody, to gather and present evidence to support potential legal action.* AIs should follow a formal and documented procedure to properly collect and preserve the integrity of the digital and forensic evidence prior to performing analysis. For example, through capturing and comparing the cryptographic hash of electronic files to determine if the evidence is tempered prior to performing analysis. *It is important to note that the information system should use internal system clocks such as NTP server to generate timestamps for audit records, so that the audit records can be sufficiently granular and synchronized. Refer to Domain 4 for further details.*
Types of evidence to be collected	AIs	AIs AIs are responsible to define the range of digital and forensic evidence to be collected during cyber incidents. It is important for AIs to review and update the range to ensure evidence collected is adequate to support after-the-fact investigations of security incidents.

Key Aspects	Applicability	Consideration
Process of investigating and analyzing evidence	AIs	AIs AIs are responsible to ensure that security investigations, forensic analysis, and remediation are performed by qualified staff or third-parties. Root cause analyses *that are complemented with business impact analyses should be performed to quantify and quality the approximate impact and* to identify the source or perpetrator of a cybersecurity incident. **Security investigations and forensic analysis processes should be also established and applied on a risk-based approach to determine whether to conduct a live response or off-line media analysis.**
Protection of evidence	AIs	AIs AIs should put in place controls to protect digital and forensic evidence, for example: – Encryption to protect the confidentiality of digital and forensic evidence; – Access control to ensure principle of least privilege is applied when granting access to forensic evidence; role-based access controls are enforced to prevent authorized access, modification and deletion of forensic tools; *access to audit configurations and logging records are limited to authorized users. AIs should also real-time alerts can be provided to a defined list of staff when specific security events occur, such as attempted access by unauthorized parties;* – **Automation and orchestration with the information systems to facilitate incident response to alerts; and** – **Cryptographic mechanisms to protect the integrity of forensic evidence and audit tools, where applicable.** AIs may utilize different solutions with relevant features such as access controls, notification, auto-healing, cryptographic management etc., offered by Alibaba Cloud mentioned in this Whitepaper to facilitate the protection of evidence.

Key Aspects	Applicability	Consideration
Evidence retention and storage	AIs & Alibaba Cloud	<u>AIs</u> AIs should ensure the forensic evidence is retained in a proper manner hence AIs should define the retention period for digital and forensic evidence per the AI's own risk appetite and is sufficient to support after-the-fact investigations of security incidents. Alibaba Cloud's OSS supports the Write Once Read Many (WORM) feature. This feature protects objects from being deleted or overwritten for a specified period of time and can be used in cases that are subject to regulations of the U.S. Securities and Exchange Commission (SEC) and Financial Industry Regulatory Authority, Inc. (FINRA). OSS provides compliance policies and AIs can configure time-based compliant retention policies for buckets based on the pre-defined retention period. After a compliant retention policy is locked, AIs can still read objects from or upload objects to buckets, however, no one can delete objects or revoke compliant retention policies within the retention period. Any party can only delete objects after the specified retention period expires. *AIs should establish a list of authorized administrators and ensure warnings are generated to them when allocated storage reaches capacity. Alibaba Cloud's CloudMonitor is available to monitor the usage of Alibaba Cloud resources, including the storage systems used to retain evidence. AIs can configure alert rules based on specific metrics.* *AIs should also regularly backup digital and forensic evidence onto different systems or media. Refer to "Restoration and quality assurance testing" section above for details of backup capabilities offered by Alibaba Cloud products.* <u>Alibaba Cloud</u> For capacity planning, Alibaba Cloud established a baseline to evaluate the resource availability risk due to capacity constraints. Current processing capacity is monitored by system on a real-time basis to forecast capacity demand, which is conducted on a monthly basis by the supply chain team with corresponding capacity plan approved by appropriate personnel. Resource replenishment procedures are

Key Aspects	Applicability	Consideration
		automatically triggered when forecasted demand exceeds the pre-defined capacity thresholds. Follow-up actions are carried out automatically when forecasted usage exceeds capacity tolerances.

5.4 Communication and Improvement

AIs should establish escalation processes for proper communication and notification both internally and externally in the event of a cyber incident. Improvement and mechanisms should be in place to enhance AIs' capabilities in dealing with future incidents. Please refer to below for consideration to address the requirements of Section 5.4:

Key Aspects	Applicability	Consideration
Escalation	AIs & Alibaba Cloud	AIs As suggested in the previous section in this Whitepaper, Alibaba Cloud will notify customers for malfunctions that could impact to their user of cloud services. AIs are responsible to ensure controls are put in place, for example, by utilizing the monitoring and alert mechanism provided by Security Center so that AIs will be notified of any incidents internal to their cloud environment. To ensure identified cyber events can be reported and relevant parties are contacted in a prompt manner, AIs should establish communication and escalation channels that enable employees to report cyber events promptly. *During or following a cyber-attack, AIs' incident response team should be able to coordinate and communicate with both internal and external stakeholders via the established communication and escalation channels*. In order to ensure smooth incident response and communication, AIs should define a list of internal and external stakeholders to be informed depending on identified scenarios and criteria and prioritize and sequence information-sharing activities with internal and external stakeholders upon incident outbreaks. *Internal Escalation* Based on the potential impact and criticality of the risk, AIs are responsible to set criteria for escalating cyber incidents or vulnerabilities

Key Aspects	Applicability	Consideration
		to senior management. *It is important for AIs to ensure the employees who are essential to mitigate the risk (e.g., fraud and business resilience employees) understand their roles in incident escalation and communication so that detected incidents will be timely escalated.* *External Communication* AIs should formulate own procedures and external communication plan with the use of social media and mainstream media for notifying third-parties such as regulators and law enforcement agencies, customers, service providers and media (when applicable) of incidents that may bring impact to them, the communication plan should be regularly review to ensure its effectiveness in notifying relevant parties. Alibaba Cloud Alibaba Cloud will respond to security incidents and vulnerabilities as soon as they are discovered and verified. Once the security incidents and vulnerabilities are confirmed, Alibaba Cloud security team will initiate the incident response process, including notifying relevant personnel for follow-up to minimize the impact of incident. Alibaba Cloud has established multi-channel communication methods to announce malfunctions that could impact customers including announcements via Alibaba Cloud official website, station letters, SMS, e-mails, and DingTalk messages.
Incident reporting	AIs & Alibaba Cloud	AIs AIs are responsible to ensure that all cyber incidents are classified, logged, and tracked. *Quantitative and qualitative metrics for the cyber incident response process should be established by AIs,* and a process to contact personnel who are responsible for analyzing and responding to an incident should exist. Moreover, *tracked cyber incidents should be correlated for trend analysis and reporting. Detailed metrics, dashboards, and/or scorecards outlining cyber incidents and events should be provided to management and are part of the Board meeting package. AIs can use Security Center that provides dashboard to identify and analyze security threats and*

Key Aspects	Applicability	Consideration
		incidents to facilitate reporting. **AIs should consider employing automated mechanisms to assist in the reporting of security incidents to preserve data for investigation, such as user stories defined by AIs as to determine whether there are any suspicious activities. Refer to Domain 4 for more details.** Alibaba Cloud Alibaba Cloud discovers security incidents from internal channels such as through log collection, anomaly analysis and detection, and alert generation. Cyber incidents will be also detected via external channel such as ASRC Alibaba Cloud Crowdsourced Security Testing Platform, CVE vulnerabilities of open-source third-party components, and threat intelligence information from third-parties. Alibaba Cloud will respond to security incidents and vulnerabilities as soon as they are discovered and verified. Once the security incidents and vulnerabilities are confirmed, Alibaba Cloud security team will initiate the incident response process to minimize the impact of incident. Alibaba Cloud's security team organizes monthly team meetings to report malfunctions that occurred in the past month and discuss follow-up status and further enhancements with Alibaba Cloud's business leadership and project managers.
Improvement	AIs & Alibaba Cloud	AIs AIs should formulate a process to continuously improve the incident response plan, for example, incorporating lessons learned from ongoing incident handling activities into the plan and relative trainings and testing. AIs should also ensure the improvement process is an iterative and institution-wide process to improve CIRR program with the objective of *recovering from disruption of services, lost or corrupted data following a cyber incident successfully and ensuring the integrity of recovered data.* *Based on the above, simulation testing exercises should be conducted to evaluate the readiness of incident response and recovery capabilities*

Key Aspects	Applicability	Consideration
		for widely reported events and different scenarios including data corruption and destruction. Refer to Domain 4 for testing service provided by Alibaba Cloud. **Further, AIs should formulate a continuous improvement process so that all security incidents should be regularly referenced when performing trend analysis which aim to identify common factors, determine the effectiveness of controls, and understand the costs and impacts associated with cybersecurity incidents and improve cybersecurity measures and policies. AIs may consider referencing the trend analysis in improvement plan or business cases justifications.** Alibaba Cloud Alibaba Cloud's security team organizes monthly team meetings to discuss follow-up status of malfunctions and enhancements with Alibaba Cloud's business leadership and project managers.

Domain 6: Situational awareness

Threats should be identified and detected via multiple channels, including internal reporting, externally reporting and subscription from external threat intelligence sources. AIs should stay informed of cyber trends, threats, and vulnerabilities by subscribing to threat intelligence feeds and develop threat intelligence sharing processes to facilitate internal and external collaboration. Please refer to below for consideration to address the requirements of Domain 6:

Key Aspects	Applicability	Consideration
Threat Intelligence	AIs & Alibaba Cloud	AIs AI should use threat intelligence to monitor relevant cyber threats and enhance its cyber risk management and control. *AIs are responsible for implementing a formal cyber threat intelligence program, which includes regular evaluation of available external cyber intelligence monitoring services. Such program should also be used to determine if it is applicable to subscribe to those threat feeds and/or supplement with*

		internal sources where appropriate. Protocols for collecting information from industry peers and government should also be established. In order to enhance threat intelligence management, AIs should subscribe to one or more threat intelligence sharing sources that provide information on cyber threats, analysis of tactics, patterns, and risk mitigation recommendations. **The quality of threat intelligence is also important - threat intelligence should include information related to geopolitical events and misinformation related to the institution propagated via cyberspace (e.g., the dark web) that could increase cybersecurity threat levels.** *A centralized read-only repository of cyber threat intelligence should be maintained to protect the integrity of threat intelligence information.* **To ensure rapid response to potential threats can be formulated, AIs should establish a threat analysis system that correlates threat data and then takes risk-based actions while alerting management. In relation to this, AIs can use Security Center which incorporates threat intelligence library developed by Alibaba Cloud to perform correlation analysis on access traffic and logs. AIs can also leverage Cloud Firewall with the built-in IPS that receives simultaneous updates of networkwide threat intelligence and detects and blocks threats from the internet in real time. For detail, please refer to section 4.4 of this Whitepaper.** Alibaba Cloud Refer to Section 4.4 above.
Internal Sharing	AIs	AIs AIs are responsible to establish a formal protocol for sharing cyber threat intelligence and incident information with employees, based on their specific job functions. *AIs should also ensure the management communicates threat intelligence with AIs' business risk contexts and provides specific risk management recommendations to business units.*
External collaboration	AIs	AIs When required or prompted by law enforcement and regulators, it is necessary for AIs to share cyber threat intelligence. Hence AIs are responsible for maintaining and regular updating the contact information

		of law enforcement and regulators to ensure threat intelligence can be shared in timely manner. *Moreover, AIs can establish a formal and secure process to share threat and vulnerability information with other entities (e.g., the industry, law enforcement, regulators, information-sharing forums, public) or via threat intelligence sharing sources, in a manner which does not violate any data privacy laws, regulations, or any internal data protection policies.* **AIs can establish information-sharing agreements to facilitate sharing of cyber threat intelligence with selected groups and associations within the security community and other financial sector organizations or third-parties.** *Nevertheless, AIs should also consider sending a representative to participate in law enforcement or cyber threat intelligence-sharing meetings.*

Domain 7: Third-party risk management

AIs should establish processes and controls to identify and manage external connections and network connected third-parties as well as critical business processes dependent to the external connections. For those identified external parties, AIs are responsible to evaluate and ensure the connected external parties maintain an acceptable level of cybersecurity practice through on-going monitoring and assessments. Please refer to below for consideration to address the requirements of Domain 7:

Key Aspects	Applicability	Consideration
External Connections	AIs & Alibaba Cloud	AIs AIs should establish policies and procedures on third-party risk management and maintain proper record for network connected parties who process, store, or transmit sensitive or critical AI data. AIs should ensure the information of third parties are treated as confidential and managed with access controls. Several security controls are mentioned in Domain 7 of C-RAF with the objective to reduce the risks associated with external connections. **Alibaba Cloud provides various security solutions such as WAF, Cloud Firewall and Security Center to enhance resiliency of connections, protect inbound traffics and safeguard data security**, for example: With the enablement of Cloud Firewall, (1) external connections can be only possible through managed interfaces consisting of boundary protection devices e.g., Cloud Firewall arranged within an AIs' security architecture; *(2) as network traffic will be monitored and controlled in real time, intrusions from external parties can be detected and blocked in timely manner; (3) access control policies can be configured to deny all external communication from external by default, and only allow minimum access by trust and whitelisted parties.* Apart from Cloud Firewall, Security Center also supports AIs in detecting and terminating unauthorized external connection. By default, the features of Security Center Basic are enabled to protect ECS instances. AIs can install Security Center agent on their VMs and servers not deployed on Alibaba Cloud. Security Center can help to analyze network

Key Aspects	Applicability	Consideration
		connections and detect any intrusion attempt, once suspicious connection is detected, Security Center will generate alerts to AIs. **Besides, as AIs may setup ECS instances as proxy servers or install Security Center agent on their proxy servers, Security Center can also act as a centralized console to monitor and manage the proxy servers.** **As sensitive and/or critical data of AIs may be transmitted via the external connection, AIs should work closely with service providers to maintain and improve the security of external and third-party connections. Controls e.g., end-to-end encryption to encrypt network traffic and use of leased lines i.e., Express Connect should be consider for establishing secure connections. AIs may also consider using VPN Gateway to form a remote connection so that the connections will be protected by relevant access control and encrypted by secure encryption algorithm. For further details, refer to Network Protection in Section 3.2.** **In addition to the deployment of security solutions, AIs should adopt boundary protection mechanisms, for example, to segregate internal network into different segments according to the supported business functions and consider isolating external connections in a standalone segment in order to limit the attack surface corresponding to external connections. For detail on network segmentation, refer to relevant sections in Domain 3 of this Whitepaper.** **As critical business functions may be supported by the external connection, AIs should consider establishing an arrangement with third-party service providers to ensure information systems with external connections can failover safely and securely. When AIs migrate to Alibaba Cloud, Alibaba Cloud will ensure the resilience and monitor the availability of supporting infrastructure, physical devices, and strive to provide cloud products and services for protecting cloud applications and data. Alibaba Cloud has established a set of incident response management framework and supporting policies and procedures to ensure systems can failover safely and securely during incidents. In turn, AIs are responsible**

Key Aspects	Applicability	Consideration
		for managing security configurations for cloud products to ensure the security of infrastructure, data, applications, and business systems on the cloud are properly configured and proper procedures are defined for failover so that it can be done in a safe and secure manner in the event of disruption. It is important to monitor if the controls deployed are effective in protecting the connections and AI's internal work, therefore, regular assessment should be performed by AIs to verify the effectiveness of control and follow up if any exception is noted. AIs should also ensure their audit function will assess the management of third party risks to determine if adequate monitoring, escalation and resolution procedures have been established and are operating effectively. *Besides, AIs should also ensure controls adopted for connections are monitored and tested by service providers regularly with outcomes, remediation plan, and remediation status shared with AIs regularly.* <u>Alibaba Cloud</u> 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 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.
Third-party management	AIs & Alibaba Cloud	<u>AIs</u> *Contract Management* AIs should establish formal contracts or service level agreements with third-parties covering specific clauses such as: - Acknowledge the responsibility of the third-party for the security and privacy of the sensitive or critical data over secure connections; - Identify the available recourse to the AI in the case that the third-party fail to meet defined security requirements;

Key Aspects	Applicability	Consideration
		- Establish responsibilities in responding to security incidents; - Specify the security requirements for the return or destruction of AI's sensitive or critical data upon contract termination; and - Document the third-party's responsibility for the notification of cybersecurity incidents and vulnerabilities. Alibaba Cloud has defined service terms and clauses in the service agreements template. AIs have the option to enroll in a tailored service level agreement ("Enterprise Agreement") with Alibaba Cloud to define respective responsibilities and obligations of AIs and Alibaba Cloud in the use of Alibaba Cloud service. Please reach to assigned Cloud Compliance Specialist for arrangement of Enterprise Agreement. *Due Diligence* AIs should perform risk-based due diligence on cybersecurity control for service providers e.g., Alibaba Cloud. In relation to this, AIs can find 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. The user guide is publicly available for customers in Security & Compliance Trust Center. *AIs are also responsible for performing risk-based regular assessments or audits on the controls implemented by Alibaba Cloud in safeguarding data and supporting incident response, disaster recovery, and resiliency. Refer to "Ongoing monitoring of third-party risk" section for monitoring controls available to AIs.* **Besides, AIs should also establish procedures to regular evaluate the cybersecurity posture of subcontractors, particularly for those who support critical functions and services for the service providers. Alibaba Cloud engaged data center service providers to support cloud services. Alibaba Cloud had internal controls to assess the security posture and monitor performance provided by service providers, the internal controls are subjected to external audit on regular basis. For detail, please reach to the assigned Cloud Compliance Specialist.**

Key Aspects	Applicability	Consideration
		A termination/exit strategy should be established for third-parties in case AIs would like to terminate the contract with third parties due to scenario e.g., continuous failed to attain service level agreed, material gaps noted in cybersecurity assessment of the third party. The strategy should be regularly tested and seek endorsement from the management for any high and medium risk items. Alibaba Cloud *Contract Management* In 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, and information security. *Due Diligence* Alibaba Cloud performs background check on vendors as applicable according to the requirements and procedures set forth in the Alibaba Cloud Vendor Management Policy. Alibaba Cloud has stated the rights and obligations, scope of services, confidentiality clauses, compliance requirements, and service levels in the contract, which is required to be signed by vendors before commencement of work. In addition, vendors are required to pass data security tests subsequent to completion of onboarding training for information security awareness.
Ongoing monitoring of third-party risk	AIs & Alibaba Cloud	AIs AIs should regularly review and update the cybersecurity assessments of network-connected third-parties and establish ongoing monitoring practices, including reviewing third-parties' cyber resilience plans. *Such monitoring should be conducted in terms of depth and frequency in accordance with the risk of the third-party.* AIs may rely on CloudMonitor to monitor the performance of cloud products and services. Dashboard is available, and AIs can monitor the

Key Aspects	Applicability	Consideration
		service performance according to the defined metrics on a real-time basis. Besides, to facilitate AIs' continuous monitoring and assessment on outsourced services, attestation reports over the internal controls related to cloud services and industry recognized certifications are available so that AIs can understand Alibaba Cloud's internal control and gain assurance on the effectiveness of those controls. Currently, AIs may download the following attestation reports from Security & Compliance Centre of Alibaba Cloud: SOC 1&2 TYPE II and SOC 3 Reports: The Service Organization Control (SOC) reports are a series of audit reports from independent third-party auditors to indicate the effectiveness of Alibaba Cloud's control objectives and activities. These reports are designed to help AIs and their auditors to get a picture of the control measures behind operation and compliance. Alibaba Cloud SOC reports are categorized into three (3) types: SOC 1 TYPE II: Internal control report on financial reporting SOC 2 TYPE II: Report on trust service criteria including security, availability, and confidentiality SOC 3: Report on security, availability, and confidentiality for general use purpose As a cloud service provider, Alibaba Cloud has established cyber resilience program with respect to business continuity, disaster recovery, incident response, threat monitoring, and infrastructure protection controls. Assessments on the effectiveness of relevant controls are performed by external parties on a regular basis. Assessment results are presented in the aforementioned attestation reports hence AIs can obtain and examine these reports for the purpose of regular review. Alibaba Cloud's services are also certified, and relevant certifications are also available on Security & Compliance Centre to evidence that Alibaba Cloud adheres to international information security standards and is committed to adopt international best practices. For example,

Key Aspects	Applicability	Consideration
		Alibaba Cloud maintains an effective BCP in accordance with International Organization for Standardization (ISO) 22301. BCP program of Alibaba Cloud is audited by third-party conducted at least on an annual basis. The certificate of ISO 22301 is available on Security & Compliance Centre of Alibaba Cloud. Apart from monitoring the cybersecurity posture of service providers, AIs should assign responsibilities to monitor the access of third-parties **and track the third-party employee's access to own sensitive or critical data based on the principles of least privilege, irrespective of systems hosted by either party. External and temporary accesses to Alibaba Cloud resources may be granted by AIs to Alibaba Cloud employees via ticket service in the management console. Such access is restricted by AIs' configured authorization setting and can be tracked by AIs. For other external access granted by AIs to cloud resources, AIs can use ActionTrail to monitor and record actions which include access to cloud products and services storing critical and sensitive data by third-party employees.** Alibaba Cloud Alibaba Cloud has established Alibaba Cloud Vendor Information Security Management Policy and Vendor Management Policy to regulate management over vendors and third-party employees. Vendors' (including data center service providers) performance is reviewed and evaluated monthly by Alibaba Cloud in accordance with the compliance requirements and service levels specified in the contracts.

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

January 2022: First Edition – Version 1.0