INFOCOMM
MEDIA
DEVELOPMENT
AUTHORITY

ADVISORY GUIDELINES ISSUED BY

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

ON

RESILIENCE AND SECURITY OF CLOUD SERVICES

25 FEBRUARY 2025

ADVISORY GUIDELINES FOR RESILIENCE AND SECURITY OF CLOUD SERVICES

1 Introduction

1.1 Digital infrastructure underpins Singapore's Digital Economy by:

a. Enabling seamless connectivity that drives Singapore as a global hub, and accelerates our economic growth through digital industries and businesses[1]; and

b. Powering the digital services in our everyday lives, ranging from digital banking[2] to ride-hailing to e-commerce.

1.2 Digital infrastructure, in particular the compute infrastructure such as Cloud and Data Centres ("DCs"), has become integral to Singapore's economy. Compute infrastructure supports our daily work and lives, and our reliance on it will increase with digitalisation. Resilience and security of the compute infrastructure are important given the systemic impact of failure. While compute infrastructure operators already promote resilience and security as part of their core value proposition, service incidents do occasionally occur, which can lead to significant impact on the economy and undermine user confidence.

1.3 The Advisory Guidelines for Resilience and Security of Cloud Services ("Guidelines") set out guidance on best practices on the resilience and security of Singapore's compute infrastructure, covering how Cloud Service Providers ("CSPs") could manage resilience and security risks of Cloud[3], by planning for business continuity and adopting appropriate and proportionate mitigation measures. While the Guidelines are for voluntary adoption, CSPs are encouraged to adopt the Guidelines, as this will not only uplift their own resilience and security posture, but also distinguish themselves in the competitive market. This will also instil greater confidence in CSPs' users that the digital infrastructure that their businesses rely on is resilient and secured. These Guidelines will be updated regularly to incorporate industry and technological development, learning points from incidents, as well as industry feedback.

2 Measures to address and manage key risks for the resilience and security of Cloud services

2.1 The measures are organised into seven categories. They are in line with existing international standards[4], with a few additional measures to better address risks (e.g., learnings from past incidents), as follows:

[1] Our digital economy is about 17.7% of Singapore's GDP in 2023. Source: Singapore Digital Economy Report 2024 by IMDA.

[2] For example, e-payment transactions in Singapore increased by ~50% from 2017 to 2022, to $127B. Source: MAS Retail Payment Statistics, 2017 and 2022.

[3] For Cloud, the focus of the guidance is on the Infrastructure-as-a-Service ("IaaS") and Platform-as-a-Service ("PaaS") models, due to their role as the underlying infrastructure and their greater impact to services dependent on them.

[4] A non-exhaustive list of referenced standards can be found in the Annex.

Category	What does it cover?
1. Cloud Governance	Measures covering information security management, human resources, risk management, data governance, etc.
2. Cloud Infrastructure Security	Measures pertaining to audit logging and monitoring, secure configuration, security testing, system development and encryption.
3. Cloud Operations Management	Measures regarding operations and change management.
4. Cloud Services Administration	Measures on the management of privileged accounts.
5. Cloud Service Customer Access	Measures pertaining to user access controls.
6. Tenancy and Customer Isolation	Measures pertaining to tenancy and customer isolation.
7. Cloud Resilience	Measures on physical and environmental security, as well as business continuity plan and disaster recovery.

Category 1 – Cloud Governance

2.2 Information security management – CSPs should ensure that information security is managed within the CSP's overall administrative structure. CSPs should:

a. establish information security roles, responsibilities, coordination, and information security policies and standards;

b. ensure Information Security Management System ("ISMS") for cloud computing has been developed, documented, approved and implemented;

c. provide oversight of its information security function such as clear roles and responsibilities, coordination of security activities, etc;

d. ensure its management and board of directors are responsible for the management of information security;

e. establish and document an information security policy and baseline requirements;

f. ensure that the information security policy is reviewed and maintained up to date so that it remains adequate and effective;

g. ensure that auditable entities are established and updated periodically such as reviewing the scope of audit, determining the effectiveness of the audit scope, etc;

h. designate personnel as the primary and backup information security liaisons who minimally, are the points of contact with local authorities, and are contactable by the customers; and

i. establish and document an acceptable use policy for critical and new technologies, services and end-user devices (e.g., wireless technologies, laptops, mobile devices) in accordance with industry standards, and is communicated to all relevant employees and third parties.

2.3 Information human resources – CSPs should ensure that all employees and third parties are suitable for their roles prior to employment or contract and that they understand their responsibilities, employment and contract terms and conditions (including termination) to reduce the risk of theft, fraud or misuse of facilities. CSPs should:

a. perform background checks in accordance with applicable ethics and contractual obligations;
b. evaluate personnel security (including third parties) at least annually;
c. ensure employees and relevant third parties minimally comply with organisation's policies, and re-acknowledgement of acceptance of information security obligations agreement annually and prior to termination of service;
d. establish a formal disciplinary process (which may include termination) for employeesand third parties who have violated the information security policy, standards and procedures;
e. ensure all assets owned by the organisation are duly accounted for and returned by employees and relevant third parties; and
f. establish, implement and review an information security training and awareness programme for employees and relevant third parties upon hire and at least annually.

2.4 Risk management – CSPs should establish and maintain a cloud-specific risk management programme to identify, quantify, prioritise, and mitigate or resolve risks impacting the cloud service operations and information assets. CSPs should:

a. establish and maintain a cloud-specific risk management programme that minimally include the process and methodology, risk identification/ assessment/ treatment/ mitigation plan and address residual risk at least on a quarterly basis;
b. conduct formal risk assessment (including cloud-specific risks) at least annually or when there are significant changes;
c. establish a process to review and monitor risks to the cloud environment including the internal and external networks, hardware, software, applications, systems interfaces, operation and human elements; and
d. develop and maintain a risk register to monitor and report all identified risks.

2.5 Third party – CSPs should ensure that it has an effective control framework over its third-party service providers supporting the cloud environment. CSPs should:

a. establish the framework that include third party service providers due diligence, agreement, delivery management, assurances over their performance and compliance with internal controls;
b. carry out due diligence in fully understanding the related risks prior to subcontracting services to third-party service provider(s) such as subcontracting risks;
c. develop and maintain risk management procedures, overseeing the risks and impact arising from third-party service;
d. ensure that written contractual agreements shall be made with every third-party service provider, which should also include contractual provisions to address relevant third-party risks;

e. ensure that the third-party service provider minimally has implemented all controls, service definitions and delivery levels as agreed in the third-party agreement, etc; and
f. *(additional measure)* ensure open-source components are safe to use, to protect against cyberattacks via software supply chain.

2.6 Legal and compliance – CSPs should ensure that they and their third-party service providers conform to the CSPs' information security and risk management policies, standards, and procedures and contractual obligations. CSPs should:
a. identify, create, maintain and review documentation minimally on compliance, cross-border and transit requirements, contractual requirements;
b. plan and conduct regular reviews to ensure that all information security and risk management procedures are complied with, in accordance with its organisational policies and standards;
c. establish procedures, training or awareness, and relevant policy enforcement actions to deter or prevent employees from unauthorised access, and enforcement of commercial agreements with relevant third parties and end users with acceptable use policies or agreements;
d. use cryptographic controls that are compliant to relevant agreements, applicable laws and regulations, etc.;
e. ensure the third-party service providers providing relevant services demonstrate compliance with the relevant policies, agreements and requirements; and
f. provide a mechanism for customers to perform continuous or real-time compliance monitoring.

2.7 Incident management – CSPs should implement incident management controls to ensure that information security events and weaknesses impacting the information assets and systems in the cloud environment are communicated in a timely manner. CSPs should:
a. implement and maintain an information security incident response plan and procedures to respond to security incidents – procedures shall minimally include roles & responsibilities, root cause and impact analysis, incident monitoring, etc.;
b. ensure that the incident response plan is relevant and effective;
c. establish an information security incident reporting process; and
d. establish clear processes and procedures to handle problems arising from all incidents, including information security and non-information security incidents.

2.8 Data governance – CSPs should ensure that only authorised users have access to the data stored in the cloud environment at all times. CSPs should:
a. establish controls (such as encryption and authentication) to secure data according to its classification and define handling procedures;
b. establish clear ownership of data;
c. ensure data integrity on input/output, transmission or exchange of data and data in storage at all times;
d. establish and implement procedures and controls for data labelling/handling requirements;

e. establish controls and procedures to protect data from loss and destruction by other tenants or by CSP authorised agents;
f. establish data storage and retention policies and procedures, and communicate these procedures to the customers;
g. establish and implement data backup procedures in alignment with the CSP committed services and scope of recovery;
h. establish and implement secure disposal and decommissioning procedures for the hardcopy, media and equipment;
i. establish secure disposal verification procedures for live instances/snapshots, dormant VMs and backups;
j. provide customers with a mechanism to track data; and
k. implement controls to prevent migration of production data to systems that do not have the same (or greater) level of controls.

<u>Category 2 – Cloud Infrastructure Security</u>

2.9 <u>Audit logging and monitoring</u> – CSPs should ensure that activities performed and events occurred in the cloud environment are being tracked and maintained for a period of time to detect any unauthorised activities and to facilitate investigation and resolution in the event of security incidents (e.g., access violations). CSPs should:
a. establish a process to track and monitor all access to network resources and system components including edge nodes;
b. establish a process to review logs;
c. ensure audit trails of all access to network resources and system components are captured and protected;
d. establish a log retention procedure; and
e. ensure integrity and accuracy of the usage logs at all times.

2.10 <u>Secure configuration</u> – CSPs should ensure that the systems in the cloud infrastructure and the supporting networks are designed and configured securely to prevent against unauthorised entry points or malicious activities through weak system configurations. CSPs should:
a. develop configuration standards for all system components and network devices (including virtualised images, snapshots and hypervisor);
b. implement controls (such as anti-malware solutions) to prevent malicious code threats;
c. implement controls to address the risks associated with portable code (code that is executed in a remote location);
d. implement controls (such as disabling unused physical/logical port) for port protection;
e. restrict and tightly control the use of utility programmes;
f. implement controls (such as shutting down inactive session after a defined period of inactivity) to manage inactive sessions;
g. configure system security parameters to prevent misuse of services and protocols;
h. implement controls (such as system configuration reviews) to restrict use of unapproved or unauthorised software; and

i. perform compliance checks to ensure all security configurations are applied according to baseline standards.

2.11 Security testing and monitoring – CSPs should conduct security testing and implement monitoring controls across the cloud infrastructure including services, VMs and physical infrastructure to detect vulnerabilities and malware in a proactive and timely manner. CSPs should:

a. conduct internal and external vulnerability scans when there are significant changes in the infrastructure or at regular intervals;
b. conduct network layer and application layer penetration testing from the Internet, cloud service management network, and CSP internal network when there are significant infrastructure changes, or application upgrades, or modifications, or at regular intervals; and
c. implement a security monitoring process, including implementing appropriate network intrusion detection or prevention systems to detect/deter abnormal network activities.

2.12 System acquisition and development – CSPs should implement system acquisitions and development security controls to ensure that security is an integral part of the information systems as well as the business processes associated with these systems. CSPs should establish policies and procedures for the development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities.

2.13 Encryption – CSPs should implement encryption and secure cryptographic key management to ensure that sensitive information in transmission or in storage electronically is being protected against unauthorised use or disclosure. CSPs should:

a. ensure that encryption policies and procedures including usage of cryptographic controls are established and mechanisms are available to enable encryption where applicable;
b. implement encryption on non-console administrative access, electronic commerce and online transactions (where applicable);
c. establish key management procedures to address all components of the key management life cycle (i.e., generation, distribution, utilisation, storage, archiving, replacement and destruction of the keying material); and
d. ensure that information involved in electronic messaging (i.e., email, instant messaging, audio-video conferencing) shall be appropriately protected.

Category 3 – Cloud Operations Management

2.14 Operations – CSPs should implement operations security controls to ensure that the operations of the cloud are documented, secure, reliable, resilient and recoverable. CSPs should:

a. establish operations management policies and procedures documentation (e.g., administrator and user guides, architecture diagrams) for equipment maintenance and management of its cloud services' operations to ensure continuity and availability of its operations;

b. ensure proper and complete documentation and assessment of the service operations;
c. establish a process to monitor and plan capacity and resource requirements to ensure system and service performance;
d. state the service level and performance including subsequent changes in the contractual agreements or other means of communication acceptable to the customers;
e. establish a process to ensure reliability and resilience of storage systems and edge nodes supporting critical information assets either in a single facility or between multiple facilities;
f. establish a process to ensure recoverability of systems supporting critical information assets; and
g. *(additional measure)* implement processes to deal with reporting of vulnerabilities by researchers.

2.15 Change Management – CSPs should implement change management controls to ensure that changes to the cloud infrastructure are carried out in a planned and authorised manner. CSPs should:
a. implement and maintain a formal change management process to control changes to its production information processing facilities and systems;
b. implement and maintain backup procedures for changes;
c. implement and maintain back-out or rollback procedures;
d. separate development, test, and production environments to reduce the risks of unauthorised access or changes to the operational system; and
e. implement a patch management process.

Category 4 – Cloud Service Administration

2.16 CSPs should implement cloud services administration controls to ensure the enforcement of policies, standards and procedures relating to the creation, maintenance and removal of privileged accounts used for managing cloud services and supporting networks. CSPs should:
a. establish a formal registration and approval process in granting and modifying privileged rights to personnel administering the cloud services;
b. enforce password controls to administrative accounts based on the risk assessments and sensitivity of the system;
c. establish a formal access review and revocation process to review the adequacy of privileges and access levels, and de-provision or remove access in a timely manner;
d. implement a formal process to detect and terminate unauthorised access attempts in a timely manner. Access controls shall be established based on the risk assessments and sensitivity of the system and data;
e. put in place password security controls based on the risk assessments and sensitivity of the system and data;
f. establish procedures for password reset and first login for all accounts with access to the cloud service management network;
g. implement measures (such as role-based access controls) to ensure that the administration of cloud infrastructure is protected from unauthorised changes;

h. implement procedures (such as system configuration review) to log, via native systems or application logs, all administrators' activities;
i. establish controls to manage sessions based on the risk assessments and sensitivity of the system and data;
j. segregate duties and areas of responsibilities to reduce opportunities for unauthorised or unintentional modification or misuse of the information assets;
k. implement appropriate encryption and security protocols for transmitting credentials for non-console administrative access based on the risk assessments and sensitivity of the system and data;
l. implement controls (such as restrict privileged access to vendors on a need-to-have basis) for third party administrative access;
m. implement controls (such as changing service password at least twice annually) for all creation of service and application accounts; and
n. *(additional measure)* include more than one approver[5] for system configuration changes, especially for changes that are significant or sensitive.

Category 5 – Cloud Service Customer Access

2.17 CSPs should implement cloud user access controls to ensure that policies, standards and procedures are established and implemented to govern the creation, maintenance and removal of user accounts to restrict access and safeguard user credentials to prevent unauthorised access to information and information systems. CSPs should:

a. establish a formal user registration process to grant, modify and restrict user access to the cloud services (i.e., applications, systems, edge nodes, databases, and sensitive data and functions);
b. enforce control measures (such as restrict access to logging facilities, default "deny-all" settings, etc) to user access to the cloud environment;
c. implement a formal process to allocate user passwords and require users to follow secure practices in the selection of passwords;
d. implement a formal process to ensure unauthorised access attempts are detected and terminated in a timely manner;
e. establish procedures (such as generate unique password and mandate password change upon first login, verify user identity) for user password reset and first logon change;
f. implement password protection measures (such as transmission of password through encrypted channels, etc) for all user login credentials;
g. implement user session management measures (such as deactivate user session after a period of inactivity, etc);
h. implement measures (such as trigger alert to administrator, etc) to monitor change in cloud user's administrator details;
i. implement measures (such as strict password controls, formal approval process) for the self-service portal that is used for the creation and management of user account;

[5] Approver is to authorise changes before the changes are carried out by a separate team of implementer/maker and checker.

j. provide mechanisms (such as secure distribution of official notifications, etc) for communication with cloud users; and
k. *(additional measure)* ensure strong encryption solutions are in place for software authentication tokens which grant users authorised access to cloud services.

Category 6 – Tenancy and Customer Isolation

2.18 CSPs should implement tenancy and customer isolation controls to restrict user access within the same physical resource and segregate network and system environments such that the customers do not pose a risk to one another in terms of data loss, misuse and privacy violation. CSPs should:

a. implement control measures (such as enforce segregation between VMs, restrict users' access and privileges to its own data environment only, etc) to protect each customers' hosted environment and sensitive data;
b. implement measures to limit sharing of resources between the cloud service delivery network, cloud service management network and CSP's internal network;
c. design, implement and manage secure network architecture to protect the cloud infrastructure (including systems, applications and data), including (i) segregating networks by dividing them into separate network domains and separating them from the public network (i.e., Internet), ii) implementing appropriate access controls between network domains based on business needs and security requirements and iii) implementing appropriate network security controls to permit legitimate traffic and block unauthorised traffic. A test plan shall be formulated to verify and assess the implemented measures, develop compensating controls and ensure the network (both physical and virtual) is protected from unauthorised connections that may breach the access control policy;
d. implement control measures to manage information risks from the deployment of the cloud using virtualisation technology;
e. limit access to data stored on a SAN; and
f. ensure access to data from customers is segregated from one another to prevent data co-mingling.

Category 7 – Cloud Resilience

2.19 Physical and environmental security – CSPs should implement physical and environmental security controls to prevent unauthorised physical access, damage or interference to the cloud environment and infrastructure with the use of appropriate procedures and assessments. CSPs should:

a. implement asset management controls (such as maintain inventory and ownership of assets, disconnect unused hardware devices);
b. implement control measures (such as authorisation before asset transfer) for off-site movement;
c. establish procedures (such as surveillance systems to monitor access, manning of physical security perimeter) for physical security and safety of the cloud information processing facilities;

d. implement procedures to restrict visitor access to the cloud information processing facilities;
e. establish guidelines for environmental threats and equipment power failures to all personnel working in the cloud information processing facilities; and
f. perform review of the physical security controls to identify security and operational weaknesses in the DC.

2.20 Business continuity and disaster recovery ("DR") – CSPs should implement business continuity and DR controls to ensure timely resumption from, and the possible prevention of interruptions to business activities and processes caused by failures of information systems and disasters. CSPs should:

a. develop, maintain and communicate a business continuity framework for the required cloud services;
b. develop and implement business continuity and DR plans;
c. establish a process to test and validate business continuity and DR plans to ensure adequacy and effectiveness of recovery requirements, and personnel's ability to execute emergency and recovery procedures;
d. *(additional measure)* conduct failover tests on cloud environment (minimally a representative environment with the same configurations) for:
    i. all AZs within the Singapore region and any other failover services that CSP offers to customers; and
    ii. global services necessary for the CSP's provision of cloud services to customers in Singapore.

3 Designated Officer

3.1 Uplifting and ensuring the resilience and security of digital infrastructure is an important task, and it requires the collective effort of the organisation led by senior management. CSPs are encouraged to designate a senior representative to take charge of this collective effort.

Annex – Reference to Multi-Tier Cloud Security (MTCS), ISO 27001 and Cloud Security Alliance Cloud Controls Matrix (CCM)

Category		Reference to
1. Cloud governance	a. Information security management	• MTCS • ISO 27001 • CCM
	b. Information human resources	
	c. Risk management	
	d. Third party	
	e. Legal and compliance	
	f. Incident management	
	g. Data governance	
2. Cloud infrastructure security	a. Audit logging and monitoring	
	b. Secure configuration	
	c. Security testing and monitoring	
	d. System acquisition and development	
	e. Encryption	
3. Cloud operations management	a. Operations	
	b. Change management	
4. Cloud service administration		
5. Cloud service customer access		
6. Tenancy and customer isolation		
7. Cloud resilience	a. Physical and environmental security	
	b. Business continuity and DR	

CSPs are strongly encouraged to review the referenced standards in full for a comprehensive understanding of the measures.