OIC-CERT Cloud Security Framework

Version 1.0

OICCERT-5-GUI-02-CLOUD-V1

Document Date: 30 Oct 2023

Standards Office Name: OIC-CERT Permanent Secretariat, CyberSecurity Malaysia
Address: Level 4, Tower 1, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya, Selangor, Malaysia
Phone: +603-8008 7999
Email: secretariat@oic-cert.org
Website: www.oic-cert.org

Published in the www.oic-cert.org

Contents

Audience

This framework is mainly intended for regulatory authorities of member states, with the purpose of assisting them in making policies on cloud service vendors and relevant service providers.

1 Introduction

1.1 Global Cloud Service Market Continues Growing

1.1.1 Digital Economy and Industry Digital Transformation Promote the Rapid Popularization of Cloud Computing

Cloud services refer to obtaining required services through the network in an on-demand and easy-to-scalable manner. This service can be related to IT and software, the Internet, or other services. The cloud service can store the software, hardware, and documents required by enterprises on the network, so that data access and computing can be performed anytime and anywhere through connected IT devices. Currently, common cloud services include public cloud, private cloud, and hybrid cloud. Public cloud can be further classified into infrastructure as a service (IaaS), software as a service (SaaS), and platform as a service (PaaS).

With the advancement of scientific and technological revolutions and industry transformations, the digital economy is booming. As a mainstream advanced computing model and critical infrastructure, cloud computing provides basic support for the development of emerging technologies such as big data, artificial intelligence, and 5G. Cloud computing is also an indispensable means for industry digital transformation and important support for improving informatization development and building new momentum for the digital economy. Cloud computing is one of the hottest topics in IT today, allowing scalable and elastic IT-enabled capabilities to be delivered as services using Internet technologies. Many related technologies use cloud computing for integration and upgrades, while a variety of industries rely on it for business model innovation. Cloud services enable enterprises to quickly respond to changing market requirements and attract more customers through innovative applications and services. More business operations are implemented through cloud computing and delivered through cloud services. Many organizations around the globe are radically changing the way they deliver their services, both internally and externally. The past decade has seen an explosive growth in data volume. The development of mobile applications and the Internet of Things (IoT) has greatly increased the computing requirements of enterprises and individuals, and they also want instant access to data anywhere they are. These trends have been pivotal in promoting cloud computing as the infrastructure of choice in the digital economy.

1.1.2 Steady Growth of Cloud Computing Despite Global Economic Downturn

According to multiple industry organizations, the cloud service market will continue to grow rapidly in the next two or three years. Gartner forecasts that by 2023, 40% of all enterprise workloads will be deployed in cloud infrastructure and platform services, up from 20% in 2020[1]. At the same time, a survey by CyberSecurity Insider commissioned by Fortinet indicates that 39% of organizations are already running more than 50% of their workloads in the cloud, a number projected to grow to 58% in the next 12 to 18 months.[2]

Since 2020, the COVID-19 pandemic has also spurred on the industry's growth; the global cloud computing technologies, industries, and applications are developing towards a new trend. Internet applications such as telecommuting, online education, and online games have become more mainstream, and the computing volume increases sharply. As a result, enterprises are looking to go digital faster, bring services online, and migrate to the cloud in the near future. Businesses are looking to cloud to revitalize their business to pre-pandemic levels.

In the meanwhile, the pandemic has forced many countries and regions to enact travel bans and prohibit mass gatherings. In this context, the majority of companies have encouraged telecommuting, which has promoted innovation in service collaboration. People began to realize that remote corporate access is inconvenient with legacy VPNs. Instead, cloud-device collaboration enables the massive use of office applications, which is both efficient and convenient.

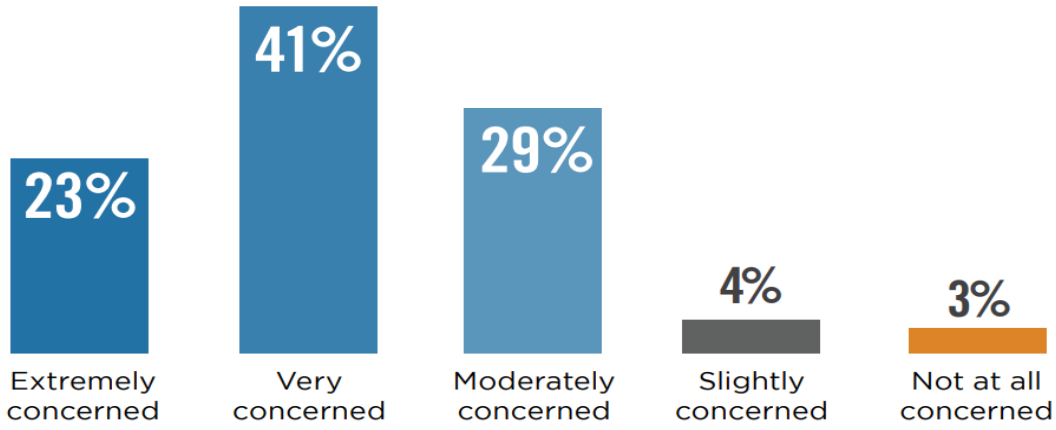
[1] Gartner Cloud Market View, 2021-2022

[2] Fortinet Cloud Security Report 2022

1.2 Enterprises Moving to Cloud Are Primarily Concerned About Security Threats to Cloud Services

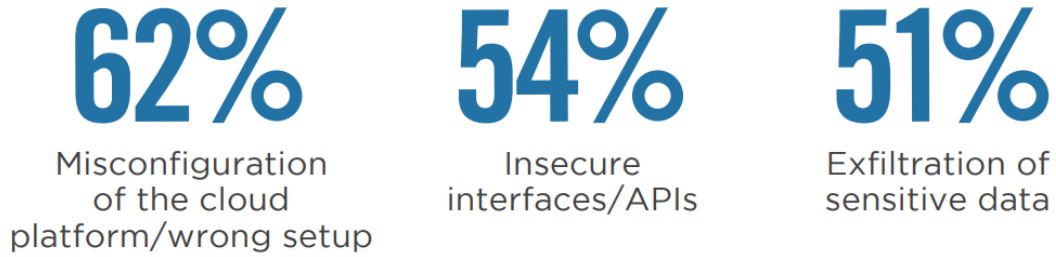
1.2.1 Cloud Service Customers (CSCs) Are Concerned About Cloud Security

As is the case for other emerging technologies, the security of cloud services is a major concern. As the technology develops, new security and compliance issues arise, posing challenges to the wide deployment and development of cloud services. The 2022 Cloud Security Report sponsored by (ISC)² also shows that 93% of companies surveyed are concerned about public cloud security, among which 29% are moderately concerned, 41% very concerned, and 23% extremely concerned.



Source: 2022 Cloud Security Report sponsored by (ISC)²

The top 3 cloud security challenges for organizations are misconfiguration of the cloud platform/wrong setup, insecure interfaces/APIs, and exfiltration of sensitive data.



Source: 2022 Cloud Security Report sponsored by (ISC)²

1.2.2 Major Threats and Challenges Facing Cloud Services

When providing services, cloud service providers (CSPs) may face both internal and external security threats. For example:

- Internal threats: lack of trusted professionals in key positions of cloud services; unknown or uncontrolled assets and devices; data center (DC) damage during extreme natural disasters; cloud service products vulnerable in design; and data leakage, malicious use of data, and abuse of access permissions due to invalid access control.
- External threats: hacker attacks, defective products from third-party suppliers, and business processes with vulnerabilities that may be exploited for fraud.

The Cloud Security Alliance (CSA) released 11 top threats to cloud computing, including:

- Insufficient identity, credential, access, and key management: the most concerned threat that could lead to negative business performance and loss of trust in the market.
- Insecure interfaces and APIs: unintended exposure of sensitive or private data due to the wide use of interfaces and APIs in the cloud environment for access operations and data interaction.

Misconfiguration and inadequate change control: may affect the confidentiality and integrity of data, system operation, or company reputation and stock price.

- Lack of cloud security architecture and strategy: limits the viability for effective and efficient enterprise and infrastructure security architecture to be implemented, resulting in fines and breaches or a high cost of implementing workarounds.

- Insecure software development: leads to (1) loss of customer confidence of the product or solution; (2) damage to brand reputation due to a data breach; (3) legal and financial impact due to lawsuits.

- Unsecure third-party resources: Since key business processes depend on the supply chain system, issues in the system may cause a loss of business data accessed by external parties. The efficiency of issue resolution depends on the supplier's response speed. Service providers can periodically review third-party resources to identify and track third-party resources in use.

- System vulnerabilities: a major cause of data breaches, which will affect the company's business and damage customers' trust in the company's brand and services. Regular vulnerability detection, patch deployment, and strict Identity and Access Management (IAM) can effectively reduce security risks caused by system vulnerabilities.

- Accidental cloud data disclosure: The cloud computing database can contain sensitive customer data, employee information, product data, and more. Accidental disclosure will incur compensation. The service provider should periodically check the storage and computing workload of the database. Access risks can be reduced by ensuring that the IAM is implemented with the principles of minimum authorization in the database.

- Misconfiguration and exploitation of serverless and container workloads: Applications implemented with serverless technology without the necessary expertise and due diligence can result in major breaches, data loss, and financial exhaustion. Therefore, traditional infrastructure teams that manage local environments must acquire related knowledge.

- Organized crime, hackers & APT: The advanced persistent threat (APT) is used to describe an attack campaign in which an intruder, or team of intruders, establishes an illicit, long-term presence on a network to mine highly sensitive data. Service providers must pay attention to the possible impact of APTs on organization services.

- Cloud storage data exfiltration: results in (1) loss of intellectual property, affecting the product development progress; (2) loss of the trust from customers, stakeholders, partners, and employees, weakening other organizations' desire in cooperation; (3) loss of employees' trust in the organization's ability to protect their data.

Compared with the 11 threats released in 2020, CSA noted that legacy cloud security issues ranked lower than before thanks to CSP efforts. Other concerns that are no longer on the list or rank quite low are issues such as insider threats, account hijacking, metastructure and applistructure failures, and limited cloud usage visibility. This shows that legacy security issues that CSPs take responsibility for seem to have been effectively mitigated.

1.2.3 CSPs and CSCs Should Collaborate to Improve Cloud Security Capabilities

1.2.3.1 CSPs Should Improve Security Management to Build Customers' Trust

One of the top issues for CSP service provision is promptly enhancing CSCs' trust by resolving the cloud service security issues and challenges CSPs themselves face. CSPs need to find better ways to cope with potential security risks related to public cloud services, internal and external security threats of organizations, and cloud security compliance risks. They also need to enhance the understanding of the shared security responsibility model. For this, CSPs must take appropriate management and technical measures to gradually improve their cloud security and privacy management capabilities. For example, CSPs should:

- Integrate the security services provided by third-party security suppliers for their cloud platforms to quickly incorporate more up-to-date security products and capabilities.
- Strengthen access management, log review, security training, and other measures for internal personnel to mitigate internal security risks.
- Strengthen vulnerability management, in-depth protection, and more measures to defend against external threats.
- Gain in-depth understanding of compliance requirements, improve compliance capabilities, and avoid penalties, lawsuits, and reputational damage caused by violations. Strengthen communication and guide customers to clearly understand their security responsibilities.

CSPs need to take several actions to address the above challenges and security management requirements. They need to establish a cloud security management system that covers all cloud computing service processes, implement security control requirements for each business domain by function, and help business departments better understand cloud security management requirements. Ultimately, these actions can help CSPs provide customers with secure and compliant cloud computing services to build and enhance customers' trust.

1.2.3.2 CSCs Can Draw on Security Services and Products Provided by CSPs

CSPs and CSCs share cloud computing security responsibilities, meaning that CSCs also need to consider how to manage security in the cloud computing environment. CSCs may not have comprehensive cloud security management knowledge, or their original security management methods do not apply to the cloud. Therefore, CSCs can use service products provided by CSPs to improve their cloud security management capabilities.

- **Visibly advanced security protection capabilities**

CSCs can use security protection services and products provided by CSPs for timely and effective security assurance. At the same time, CSPs can provide visualized security monitoring and protection capabilities specific to cloud computing environments to help CSCs detect and block security vulnerabilities, detect suspicious behavior, and promptly respond to possible intrusion attacks; these security capabilities include infrastructure protection, data protection, intrusion detection and analysis, identity authentication and management, and firewall hosting.

- **Security solutions adaptable to multiple scenarios**

During digital transformation, CSCs may apply many new technologies and develop new business scenarios. The application of new technologies and business process transformation brings new security risks, which may cause trouble to CSCs and arouse their concerns about the application of new technologies. Digital transformation of an enterprise cannot go anywhere without cloud services. CSPs can leverage their innovation capabilities to integrate mature products and up-to-date technologies to design cyber security solutions for various business scenarios, safeguarding CSCs' digital transformation and empowering CSCs to be assured to invest more in new technological changes. For example, some CSPs provide content moderation service for CSCs to automatically detect non-compliant content, helping CSCs reduce service violation risks.

- **Rich cloud security ecosystem**

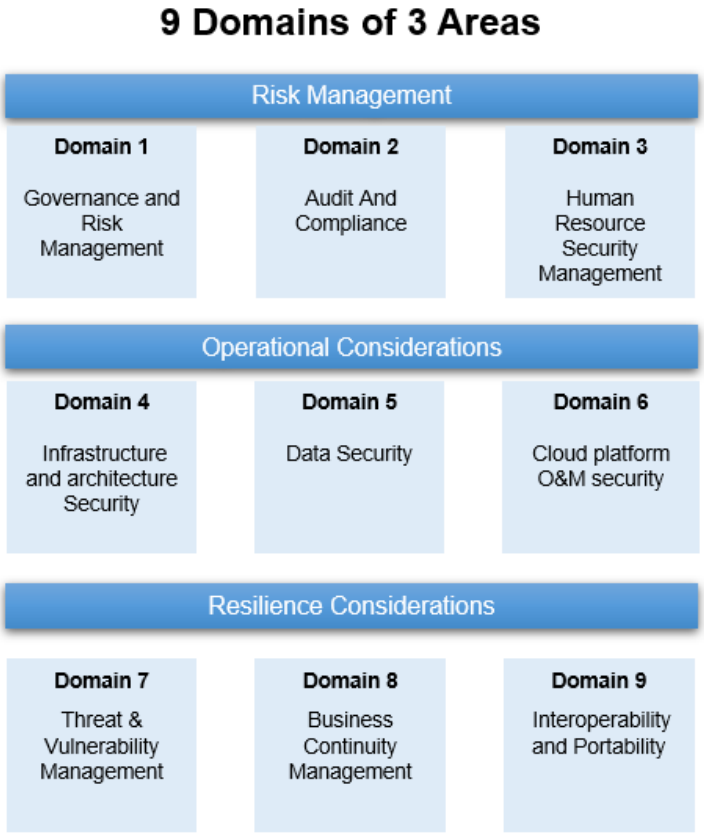
The rich cloud security ecosystem greatly expands the categories of cloud security services, enabling CSCs to choose the right products and services for their specific contexts. This helps CSCs improve their IT system security.

- **Other cloud security services**

CSPs can also provide CSCs with security and compliance consulting, security hosting, and other services, so that CSCs can quickly obtain a high level of security management capabilities by drawing on the capabilities and experience of CSPs. With the help of high-level CSPs, CSCs can improve their multi-cloud security management capabilities with less efforts and higher efficiency, especially in multi-cloud environments.

2 Baseline security technical specification

Security control requirements given by this document are divided are divided into three areas: Risk Management, Operational Considerations, and Resilience Considerations, covering 9 domains, as shown in the following diagram.



OIC CERT Cloud Security Controls Overview

2.1.1 Area 1 Risk management

This area introduces how the organization is managed and operated, and what are the policies, procedures and the internal controls put in place.

2.1.1.1 Domain 1 Governance and Risk Management

2.1.1.1.1 Formalise Responsibilities and Accountability

a) The responsibility and accountability for each party shall be formally documented in a cloud service contract or agreement, clearly stating the roles and responsibilities between the Cloud Service Provider (CSP) and the end user organisation.
b) Roles and responsibilities shall be clearly defined and formalised to develop, operationalise and enhance governance programs.
c) All relevant policies, regulations, contractual agreements shall be identified and documented.
d) All policies and procedures shall be reviewed at least on an annual basis or as and when there are significant changes to these documents.
e) Any deviations shall go through a formal approval process and documented.
f)

2.1.1.1.2 Training

a) Both the CSP and Cloud Service Customer (CSC) shall undergo relevant training on governance and risk management in order to better understand the scope and depth to which they shall be addressing risks. An example would be the ISO31000:2018 Risk Management standard, or equivalent.
b) Both the CSP and CSC shall consider joining relevant international governance and risk management communities and associations for information sharing and to further their knowledge.

2.1.1.1.3 Establish a Formalised Risk Management Framework

Risk Management Programme

a) A risk management framework shall be established to manage technology risks. Processes shall be established to identify, prioritise and put in place risk mitigation strategies to address the risks identified.

b) Relevant roles and responsibilities with clear reporting structures shall also be defined for all organisation functions.
c) The risk management framework shall also incorporate requirements such as risk identification, risk assessment, risk treatment and putting in place mitigation plans to manage and accept risk up to an acceptable level agreed with the risk owners.

Risk Identification

a) Risk management procedures for CSPs shall be developed and approved by management.
b) Organization-wide assets shall be identified, and associated risks shall be determined based on the criticality of the assets and the impact and probability of threats.
c) Risks shall be identified based on their associated risks to the Confidentiality, Integrity, and Availability of the systems.
d) Contracts and agreements made with CSPs shall cover the following:
    i. The identified risks
    ii. The scope and amount of control that the CSC has over the CSP
    iii. The service level agreements to be adhered to
    iv. The roles and responsibilities of the CSP
    v. Any legal recourse, penalties, and compensation should any issues occur
e) Risk management procedures shall be aligned with industry best practices to check for completeness.
f) The CSP or an independent third party shall conduct regular threat and vulnerability assessments on the CSP's data centre.
g) The CSP shall develop a remediation plan that addresses the identified risks within a reasonable timeframe.

Risk Assessment

a) Risk assessments shall be conducted regularly, at least on an annual basis, or when there is a significant change to the system, to understand the probability of security incidents, its impact on the organisation, and the corresponding security controls that shall be implemented.
b) Risk assessments shall include threat and vulnerability assessments, and impact assessments.
c) Both qualitative and quantitative methods shall be utilised to assess the probability and the impact of all inherent and residual risks.
d) Data protection topics shall be covered to address data protection concerns.
e) Risk assessments shall be aligned to industry best practices and standards.
f) A regular review of all users' entitlements to network, systems, applications and data, shall be performed to ensure that all entitlements are appropriately based on principles of separation of duties and least privilege, and commensurate with the risk level and information classification of the data being accessed.
g) Authorised users who need access to network, systems, applications, and data from geographically remote sites shall be subjected to appropriate terms and conditions, applicable policies and procedures, and necessary approvals from the relevant OIC CERT authorities.

Risk Management

a) Risk mitigation plans shall be put in place to address the risks related to the cloud services and agreed between the CSP and the risk owners.
b) The risk mitigation plans shall also be communicated to the relevant personnel.
c) All material risks shall be evaluated and prioritised.
d) All risks are to be re-evaluated regularly, at least on an annual basis.
e) Remediation plans shall be developed to address and mitigate the risks identified.
f) In the event of an incident, the risk assessment shall be reviewed to check if it has been addressed or needs to be revised.

Risk Register

a) A risk register shall be developed, maintained, and monitored to report all identified risks.
b) The risk register shall be updated regularly, at least on an annual basis.
c) Risk remediation and controls shall be developed for each of the identified risks.
d) The following criteria shall be covered by the risk register:
    - Risk criteria

- Risk appetite
- Risk priority level
- Risk remediation plan
- Risk resolution duration
- Management approvals for each risk
- Where appropriate, management shall be including the findings, especially the high priority ones, from the risk register into the organisational security roadmap. Relevant resources such as manpower and budget shall also be provided to appropriately address the identified risks.

e) There shall be engagement and regular communication with the relevant cloud related industry groups to keep up to date with the latest best practices.

Risk Treatment

a) Risks shall be handled and tracked according to the risk treatment plan to reduce residual risks to an acceptable level.
b) Risk, risk indicators, and treatment measures shall be audited at least quarterly.

2.1.1.1.4 Security Incident Management, e-Discovery and Cloud Forensics

a) The CSP shall institute capabilities in Security Incident Management, e-Discovery and Cloud Forensic and establish the corresponding policies and processes to ensure the consistent and continuously improved effectiveness of the respective capabilities.
b) The CSP should deploy personnel that are qualified, but not limited to, below or equivalent to support the respective capabilities:
   - Global Information Assurance Certification (GIAC) Certified Incident Handler (GCIH)
   - CREST Certified Incident Manager (CCIM)
   - Association of Certified E-Discovery Specialists (ACEDS) Certified E-Discovery Specialist (CEDS)
   - GIAC Law of Data Security & Investigations (GLEG)
   - GIAC Certified Forensic Examiner (GCFE)
c) The CSP Security Incident Management capability shall coordinate with the CSC Security Incident Management team, if any, particularly to support software and applications where the Cloud Service Model deployed is IaaS or PaaS. If there are no CSC Security Incident Management team, the CSP shall ensure that it is capable to respond to incidents that occur on the components (e.g virtual machines, applications) provided by the CSC.
d) The CSP e-Discovery capability should support software and applications where the Cloud Service Model deployed is IaaS or PaaS. The CSP should also support 3rd-party e-Discovery contractors authorised by the CSC.
e) The CSP Cloud Forensic capability should support software and applications where the Cloud Service Model deployed is IaaS or PaaS. The CSP should also support 3rd-party Cloud Forensic contractors authorised by the CSC.
f) The CSC should also consider obtaining capabilities in Security Incident Management, e-Discovery or Forensic independent of the respective CSP capabilities, either through development of such capabilities within the CSC or via contracting a 3rd party, to augment the effectiveness in these areas when required.

2.1.1.1.5 Establish Security Incident Management Plan

a) The CSP shall institute a Security Incident Management team complete with the following details:
   i. Resources (i.e. people, budget, processes) that are necessary for the effective and ongoing operation of the Security Incident Management capability.
   ii. Standard Operating Procedures to facilitate ready triaging of security incidents and appropriate responses and parties to notify and update. This should also include procedures that described co-ordination with external Security Incident Management team such as from the regulator or appointed by the CSC.
   iii. Documentations of policies, procedures, guidelines and reports to be properly managed and disseminated to relevant parties.
b) The CSP shall regularly conduct drill exercise of the Security Incident Management team in order to ensure effectiveness of the Security Incident Management capability.

c) The CSP shall institute performance and incident metrics for the purpose of assessing the effectiveness of the Security Incident Management team in order to direct the continuous improvement of the Security Incident Management capability in order to meet statutory, regulatory and contractual requirements.

2.1.1.1.6 E-Discovery

a) The CSP shall put in place policies, processes and resources to support e-Discovery requests and efforts authorised by the CSC via parties that are approved by the CSC.

2.1.1.1.7 Cloud Forensics

a) The CSP shall put in place policies, processes and resources to support forensic requests and efforts authorised by the CSC via parties that are approved by the CSC.
b) CSP shall inform CSP of any impact to the Service Level due to the forensic investigation.

2.1.1.2 Domain 2 Audit and Compliance

2.1.1.2.1 Comprehensive and Formalised Plan for Audit Management Systems and Compliance Activities

Audit Committee
An audit committee shall be established to make decisions on audit matters.

Audit Plans
Audit plans shall be developed, approved, and communicated to ensure that audit and compliance activities are maintained.

Audit Scope
The audit scope shall include audit strategies, timelines, roles and responsibilities, internal audit programs with CSPs, and external audit programs with independent third-party providers.
Regular Review and Updates

Audit programs shall be reviewed and updated on a regular basis, at least annually.
Compliance with Relevant Best Practices

Audit and compliance activities shall be in compliance with relevant international best practices, standards, and regulations.

Audit Trails
Audit trails shall contain information such as user identifiable information, event types, date and time stamp, affected data or system.

Protection of Audit Trails
a) Audit trails shall be stored on a centralised storage system.
b) The centralised storage system shall be located in an internal network and protected by at least a firewall.
c) Access to audit trails shall be protected by both physical and logical access controls.
d) Audit trails shall be protected from being tampered with.
e) Audit logs shall be protected from unauthorised edits or deletion.
f) Events sent to the log server shall be categorised, prioritised and easily identifiable.
g) A network time protocol (NTP) server shall be set up and configured to ensure that all systems are synchronised and updated with the correct network time to enable accurate investigations and analysis where necessary.

Backups
a) Log retention procedures shall be formalised and reviewed regularly, at least on an annual basis.
b) Logs shall be backed up regularly and only be accessible by authorised personnel.

Regular Review
Audit programs shall be reviewed regularly, at least once a year, or in the event of significant changes to the systems.

Data Residency
For SENSITIVE and SECRET environments, there must be local data residency so that all data remains in-country and is not transmitted or stored out of country.

Staff Residency
a) All personnel operating these classified and highly classified environments must also be based locally and not be based remotely.
b) A regular review of all users' accesses made to network, systems, applications, and data shall be performed to ensure that all accesses made are authorised.
c) A regular review of all users' entitlements to network, systems, applications and data, shall be performed to ensure that all entitlements are appropriately based on principles of separation of duties and least privilege, and commensurate with the risk level and information classification of the data being accessed.

2.1.1.2.2 Engage with International Audit Community

There shall be regular engagement and communication with the international audit community to keep updated on latest best practices.

2.1.1.2.3 Deploy Automated Systems and Appropriately Trained Personnel

Audit Tools
Audit tools should be used where feasible to enable audit logs to be automatically collected and protected from unauthorised access.

Use of Automated Systems
Automated systems should be used where feasible to collect, inform the relevant parties, and track the audit findings until closure.

Personnel
Personnel in charge of audit and compliance functions should be appropriately trained and professionally certified in relevant international best practices. Examples of professional certifications are as follows:
a) Certified Information Systems Auditor (CISA) from Information Systems Audit and Control Association (ISACA)
b) Certified Information Systems Security Professional (CISSP) from International Information Systems Security Certification Consortium (ISC)2
c) Certificate of Cloud Auditing Knowledge (CCAK) from Cloud Security Alliance
d) Any other relevant internationally recognised professional certifications
e) Any other local OIC CERT licencing schemes available

2.1.1.3 Domain 3 Human Resource Security Management

2.1.1.3.1 Employment and Contracting

Job Descriptions
a) For every role that is required in the organisation, there shall be a job description that clearly specifies the job requirements, duties, responsibilities, and the skills required to perform in that role.
b) The documented roles and responsibilities in these job descriptions shall be communicated to all relevant parties within the organisation so that there is clarity during the hiring process, and employment or contracting period.

Background Checks and Screenings
a) All potential employees and 3rd parties shall be subjected to a relevant background check and screening prior to employment or contracting in accordance with applicable laws, regulations, ethics, requisite professional security qualifications, and contractual obligations.

b) The comprehensiveness of the background checks and screenings shall be directly proportionate to the level of criticality of the role, level of responsibilities of the role, as well as the level of access to sensitive networks, systems, applications, and/or data.
c) Background checks and screenings shall also be performed on a regular basis of existing employees and 3rd parties, or when there is a change in role and responsibilities of an employee or 3rd party, that is commensurate with the risks of that role and responsibilities.

Employment Agreements and 3rd Party Contracts

a) The organisation shall include the role and responsibilities of the job, the provisions and/or terms for adherence to established information governance and security policies, as well as the termination rights by all parties within the employment agreements and 3rd party contracts.
b) Agreements containing compliance with cyber security rules and regulations shall be signed with internal personnel, external service providers, and authorized visitors, and they shall understand and agree to the terms and conditions.
c) Depending on the role and responsibilities of a job, an additional non-disclosure agreement (NDA) may be required and should be considered between the organisation and the employee or 3rd party as part of the employment agreement or 3rd party contract.
d) The content of the NDA shall be reviewed at least once a year, and stakeholders should be notified to reconfirm promptly.
e) Potential employees and 3rd parties shall be made aware of the consequences and disciplinary actions that might be taken in the event of a violation of security policies, standards, and/or procedures.

Personnel Change

a) When personnel change positions, stakeholders shall be informed of the transfer information, and their logical and physical access permissions shall be evaluated and updated. The transfer shall be completed within the specified time.
b) When personnel terminate employment, stakeholders shall be informed of their departure information, conduct exit interviews, promptly remove their access permissions, and require the employee to return the CSPs' assets if any.

Disciplinary Actions

a) The organisation shall establish (or include within existing) policies and procedures of a formal disciplinary process (which may include termination) for employees and 3rd parties who have violated the information security policies, standards, and procedures.
b) Employees and third parties shall be made aware of the consequences and disciplinary actions that might be taken in the event of a violation as specified in the policies, standards and/or procedures.
c) When discovering violations by internal or external employees, the violation shall be confirmed again, and the severity and impact of the violation shall be assessed.
d) The disciplinary process shall be documented, and relevant personnel should be informed of the handling measures and the reasons.

2.1.1.3.2 Relevant Security-related Policies and Procedures

Access to Organisation

a) The organisation shall establish (or include within existing) employee onboarding checklists that all access to the organisation's networks, systems, applications, and/or data should only be granted after the employee or 3rd party has signed off on all employment or contract documents, including but not limited to acknowledging the organisation's information security policies, and has officially joined the organisation.

Acceptable Use of Technology

a) The organisation shall establish (or include within existing) policies and procedures for defining allowances and conditions on the acceptable use of the organisation-owned or managed technology assets.
b) Due to the ever-changing technology landscape, the policies and procedures shall be regularly reviewed for continued relevance and updated accordingly when necessary.

Clean Desk

a) The organisation shall establish (or include within existing) policies and procedures for on-premise workspaces when left unattended to be maintained appropriately by employees and 3rd parties to not have openly visible data or information that may be sensitive.
b) Due to the ever-changing technology landscape, the policies and procedures shall be regularly reviewed for continued relevance and updated accordingly when necessary.

Remote Work and Work-From-Home

a) The organisation shall establish (or include within existing) policies and procedures to protect data and information that are remotely accessed, processed, and/or stored at off-premise workspaces.
b) Due to the ever-changing technology landscape, the policies and procedures shall be regularly reviewed for continued relevance and updated accordingly when necessary.

Asset Return

a) The organisation shall establish (or include within existing) policies and procedures for the proper return of organisation-owned technology assets by leaving employees and 3rd parties.
b) The policies and procedures shall also include the proper seizure of organisation-owned technology assets from employees or 3rd parties terminated under acrimonious circumstances or due to disciplinary actions.

2.1.1.3.3 Employee Training Programs

Security Awareness Programs

a) The organisation shall develop and implement an information security awareness program that is applicable to all employees and 3rd parties on the information security policies, standards and/or procedures of the organisation.
b) This program shall be implemented on a regular basis to ensure that employees and 3rd parties are constantly reminded on:
    - the importance of information security in their area of work;
    - the need to report immediately to management on any potential security breaches or events that they may see or encounter;
    - the applicable legal and regulatory requirements; and
    - the potential consequences of non-compliance that are applicable to the organisation as well as to their employment or contract.
c) Regular security awareness training shall be provided to internal and external employees, including:
    - Before on-boarding
    - At least once a year
d) Records of security awareness training activities shall be kept, and measurement and evaluation should be carried out to enhance the training.

Scenario-based Security Training

a) The organisation shall develop and implement a scenario-based training program that can be applicable to all employees and 3rd parties (e.g. email phishing exercises, ransomware attacks, etc.) as well as trainings that are only applicable to specific groups of employees and 3rd parties (e.g. email spear-phishing exercises, management table-top exercises for security incident management, etc.).
b) These trainings, which are more targeted, shall be performed on a more regular basis compared to the security awareness program so that employees and 3rd parties stay vigilant and maintains the security posture of the organisation.

Industry Recognised Security Certifications

a) The organisation shall encourage and support employees in achieving industry and/or OIC CERT recognised security certifications that are relevant and applicable to their roles.
b) Industry and/or OIC CERT recognised security certifications may be found at, but not limited to the following:
    - Cloud Security Alliance
    - ISACA
    - (ISC)2

- SANS Institute

2.1.2 Area 2 Operational Considerations

This area introduces three important domains related to cloud operation and maintenance.

2.1.2.1 Domain 4 Infrastructure and architecture Security

2.1.2.1.1 Introduction

Infrastructure security encompasses the lowest layers of security, from the physical facilities to the end-user configuration and implementation of infrastructure components, and is the foundation for operating securely in the cloud environment.

2.1.2.1.2 Network

Documentation

a) Policies, guidelines, and procedures related to infrastructure and virtualisation security shall be formalised and communicated with all relevant parties. As well, all documentation shall be reviewed regularly to maintain relevance to changes in internal processes and latest industry standards.
b) Production and non-production environments shall be clearly identified and documented.
c) Critical network infrastructure, network architecture diagrams, data flow diagrams, and system configurations shall be clearly identified and documented, especially for areas that may be subjected to regulatory requirements.
d) Security baseline standards used for network devices, servers, hypervisors, and operating systems, as well as any approved deviations from baseline standards, shall be clearly documented.
e) Virtualised IT systems and services are clearly identified and documented, including the potential security risks and vulnerabilities, and appropriate risk assessments and treatments have been performed for these virtualised IT systems and services.

Segregation and Segmentation

a) Infrastructures and virtualisations shall be designed, developed, deployed and configured such that all user access by the CSP is appropriately segregated and segmented, and monitored for enforced restrictions.
b) In multi-tenanted environments, segregation between virtual machines belonging to different CSCs shall be strictly enforced.
c) Segregation of production and non-production cloud environments shall be strictly enforced.
d) Software-defined networks (SDNs) shall be a preferred option for microsegmentation implementations due to its additional benefits to network security.

Access Controls

a) Network communications between environments shall be monitored, encrypted and restricted to only authenticated and authorised connections. These connections shall be regularly reviewed to ensure continued relevance and documented justification of allowed services, protocols, ports and compensating controls.
b) Remote management of hosts and hypervisors shall be disabled for enhanced security.
c) Access to hosts and hypervisors shall be restricted and limited to authorised administrators on a need basis only.
d) Multi-factor authentication methods shall be implemented for all user access, including remote access.

Monitoring, Detection, and Response

a) The overall cloud network shall be monitored to ensure that no unknown virtual devices join the cloud network.
b) All network devices and virtual machines shall be monitored for their operational status, resource usage, network traffic and performance, application and service executions, etc.
c) Relevant personnel shall be alerted immediately upon detection of any anomalies in the monitored parameters.
d) There shall be relevant logs generated from the monitoring activities, and all log data shall be maintained for a sufficient period of time for the purposes of investigation.

Resource Planning

a) The availability, quality, and capacity of resources required in provisioning the necessary system performance shall be monitored on a continuous basis, and that plans are in place for immediate deployment if necessary, and for future growth and/or expansion when necessary.

2.1.2.1.3 Compute (Workload)

Isolation

a) Internal processes and technical security controls shall be implemented to prevent administrator or non-tenant access to running virtual machines or volatile memory.
b) Specific hardware pools or general locations shall be a preferred option to support workload isolation, availability, and compliance requirements.
c) Immutable workloads shall be a preferred option for workload isolation due to its significant security benefits.

2.1.2.1.4 Storage

Encryption

a) All physical storage devices shall be encrypted to reduce the risks of data exposure during drive replacements.
b) Encryption functions shall be isolated from data management functions to prevent unauthorised access to data.

2.1.2.1.5 Data Centre

Geographic Location

a) The specific location of the data centre shall not be public knowledge, and shall be limited to a need-to-know basis only.

Environment

a) The chosen location and the design of the data centre shall be sufficiently safe from environmental risks, such as, floods, earthquakes, fires, extreme temperatures, extreme weather events, etc.

Work Safety and Security Standards

a) The data centre, that includes the offices, rooms, facilities, etc., shall adhere to industry standards and local regulatory requirements for a safe and secure working environment for all on-site personnel.

Documentation

a) All subsequent policies, guidelines, and procedures related to data centre security that follows this policy document shall be formalised and communicated with all relevant parties. As well, all documentation shall be reviewed regularly to maintain relevance to changes in internal processes and latest industry standards.

2.1.2.1.6 Physical Security Management

Access

a) List of personnel with physical access permissions to DCs is specified and approved.
b) Access to data centre is limited to authorised personnel on a need to basis only, and access to the data centre is revoked immediately upon employment termination or expiry.
c) Mechanism capable of automatically shall be provided to revoke and delete physical access permissions.
d) Lost or damaged access credentials shall be promptly update.
e) The personnel list for accessing DC facilities shall be reviewed at least every month or when significant changes occur.
f) Physical access controls shall be in place to effectively restrict access to data centre to only authorised personnel, and attempts to enter the data centre by unauthorised personnel are responded to immediately.
g) All visitors to the data centre shall be security cleared and approved by the appropriate management and security personnel, and shall be escorted by authorised personnel at all times.
h) A detailed logbook of all visitors to the data centre shall be maintained and regularly reviewed for potential discrepancies.

i) All personnel and visitors in the data centre must be easily differentiated by visual inspection and identification.

Surveillance

a) Surveillance systems are in place to monitor access going into, within, and exiting the data centre.
b) Surveillance systems shall encompass all areas of the data centre with no blind spots with regulatory requirements and restrictions taken into consideration.
c) Surveillance systems shall have the capability to record and store on-site for a sufficient period of time for the purposes of investigation.
d) Surveillance recordings shall be backed-up and maintained off-site for a sufficient period of time for the purposes of investigation.
e) Surveillance recordings shall be sufficiently detailed for easy identification of areas and persons monitored.

Security Personnel

a) There shall be sufficient security personnel on duty within and outside the data centre at all times.
b) Security personnel shall be background checked and security cleared prior to employment.
c) Security personnel shall be subjected to regular scenario-based incident response exercises to ensure familiarity with standard operating procedures.
d) All personnel operating these classified and highly classified environments must also be based locally and not be based remotely.

Security Incident Response

a) Security personnel shall be able to respond immediately to any security incident detected or reported within or at the vicinity of the data centre.
b) All security incidents shall be escalated to the appropriate management personnel immediately for attention, further investigation, and/or resolution.

2.1.2.1.7 Asset Management

Inventory

a) All assets within the data centre shall be catalogued, classified, tracked, and records kept of all asset movements.
b) All assets entering and exiting the data centre shall be authorised by the appropriate management personnel, closely monitored, and tracked with handover and takeover procedures.

Physical Access and Connectivity

a) Physical access to assets (e.g., physical ports, network jacks, wireless access points, gateways, handheld devices, information systems, communications hardware, telecommunications lines, etc.) shall be restricted to authorised personnel only.
b) Connecting assets to each other shall be performed only with authorisation, and by authorised personnel only.
c) Personnel shall adopt a clear desk and clear screen policy to ensure privileged information is not inadvertently leaked.

Redundancies

a) There shall be considerations for redundant or parallel power lines provisioned for the data centre, and/or for power supply to be supplied from two different power stations.
b) Emergency power systems or standby generators shall be put in place to protect life and property in the data centre from the consequences of losing primary electric power supply.
c) Uninterruptible Power Supply (UPS) systems shall be put in place to protect computer and telecommunication hardware where an unexpected power disruption could cause injuries, fatalities, serious business disruption, and/or data loss.
d) There shall be considerations for additional physical and environmental resources in anticipation for the probability of rapid infrastructure expansion.

Decommissioning and Disposal

a) Assets being decommissioned shall be disconnected physically from the network, and no longer be connected to the production environment.
b) All decommissioned and/or end-of-life assets shall be disposed appropriately based on industry standards and regulatory requirements, such as:

- Degaussing of magnetic memory devices
- Physical destruction of magnetic/solid state memory devices
- Environmentally friendly disposal of potentially toxic substances contained within the assets.

2.1.2.1.8 Environmental Controls

Protection

a) Physical structure of the data centre shall be sufficiently robust to withstand any break-in attempts to allow for responding security personnel to arrive on-site.
b) Communication cables shall be laid in a concealed and secure location to protect them from potential damage.
c) Lightning protection measures shall be implemented to securely ground facilities and protect data centre equipment.
d) Fire prevention measures shall be implemented to protect the data centre, equipment, and personnel.
e) Water prevention and protection measures shall be implemented to protect the data centre and equipment.
f) Anti-static prevention and protection measures shall be implemented to protect the data centre and equipment.
g) Electro-magnetic protection measures shall be implemented to protect key areas, communication cables, and critical equipment.
h) Temperature and humidity control measures shall be implemented to ensure that the temperature and humidity are within the allowed range for the equipment to operate.
i) Emergency control measures/mechanisms shall be implemented, such as cutting off power and water supplies and providing emergency lighting.

Monitoring, Detection, and Response

a) The environmental parameters of the data center shall be monitored in real-time.
b) Relevant personnel shall be alerted immediately upon detection of any anomalies in the environmental parameters.
c) Pertinent alerts and confirmed environmental events shall be escalated to the appropriate management personnel immediately for attention, further investigation, and/or resolution.
d) There shall be emergency controls and processes available to address each environmental parameter being monitored, and shall be made available to the relevant personnel responding to the environmental parameter alert.

2.1.2.1.9 Disaster Recovery Plans

Documented Plans

a) There shall be a documented Disaster Recovery Plan (DRP) for the data centre with various identified scenarios that has taken into consideration the potential risks (probability vs. impact) from identified threat surface, threats, and threat vectors.

Practical Drills

a) Drills of various scenarios shall be conducted on a regular basis (at least once a year) to ensure data centre personnel preparedness and familiarity with DRP procedures in the event of a real incident occurring, such as:
    - Power failure
    - Fire incident

Table-top Exercises

a) Table-top exercises shall be conducted on a regular basis, in addition to the practical drills, where certain scenarios may not just be an environmental incident, and still have the potential to disrupt data centre availability, such as:
    - Terrorist attack on the data centre
    - Cyber-attack on the network infrastructure

2.1.2.1.10 Data Centre Personnel

Security Clearance and Background Checks

a) All personnel that are going to be working at the data centre shall be background checked and security cleared before deployment.
b) Additional security clearances and/or background checks shall be performed for personnel being deployed into more sensitive and/or highly classified environments within the data centre.
c) Access that are assigned to personnel shall be revoked immediately upon their termination or transfer.

2.1.2.1.11 DC O&M

a) Limit the scope of personnel who know the physical locations of DCs.
b) DC equipment shall be properly installed and protected, and obvious and irremovable labels shall be set.
c) The environmental parameters of the data center shall be monitored, and real-time alarms shall be generated and relevant responsible persons notified when abnormalities are detected.
d) Unauthorized physical access shall be monitored, respond to intrusion alarm system triggers, and retain monitoring videos for at least 3 months.
e) Facilities and protective equipment shall be maintained regularly, and the effectiveness and redundancy of the facilities and devices shall be checked at least once a year or when major changes occur.
f) Emergency exercises for the DC's uninterruptible power supply and emergency power supply system of the data center shall be conducted at least once a year.

2.1.2.2 Domain 5 Data Security

2.1.2.2.1 Introduction

Data security stipulates the considerations on the importance of the tenant's oversight in accurately determining the classification of the data that is to be hosted and operated on the cloud platform through a risk assessment approach.

2.1.2.2.2 Data Classification Policy

a) The CSC shall classify data that the CSC owns according to the OIC CERT Data Standards as follows prior to moving the data to the CSP:

- **Open Data**: Data that may be disseminated without restrictions or with relevant minimum restrictions prescribed
- **Confidential Data**: Data whose disclosure to the public or 3rd parties may cause limited damage to the public interest or persons.
- **Sensitive Data**: Data whose disclosure to the public or exchanged by Government entities on other than a "need-to-know" basis may cause significant damage to the public interest or persons.
- **Secret Data**: Data whose disclosure to the public or exchanged by Government entities on other than a "need-to-know" basis may cause very serious damage to the public interest, to national security or to persons.

b) Both CSP and CSC shall ensure proper and thorough risk assessment is performed as stipulated in the Governance and Risk Management policy in order to determine the appropriate security classification for the data.
c) For data that are not owned by the CSC, the CSC shall seek the consent of the individuals or private entities to use, store, process and exchange the data with other government entities in the course of providing the cloud service.
d) The CSC shall ensure there processes in place to protect the personal data or the intellectual property rights of relevant parties.
e) The CSC shall ensure that CSP cloud infrastructure can support the security requirements of the data to be processed in terms of security measures and particularly when exclusive use of the servers and network equipment are required. Highly sensitive data shall be protected via hardware solutions such as air-gap security measures.

2.1.2.2.3 Data Residency and Operator Access

a) The CSC shall ensure there is sufficient number of personnel adequately accredited to access data required for operations in the data centre.

2.1.2.2.4 Appropriate Security for Data Lifecycle

Data Lifecycle Security Measures
The CSP shall ensure that effective data protection policies, procedures and measures are instituted to secure the data throughout the data lifecycle:

- Create. Creation is the generation of new digital content, or the alteration/updating/modifying of existing content.
- Use. Data is viewed, processed, or otherwise used in some sort of activity, not including modification.
- Share. Information is made accessible to others, such as between users, to customers, and to partners.
- Store. Storing is the act of committing the digital data to some sort of storage repository and typically occurs nearly simultaneously with creation.
- Destruction. Data is permanently destroyed using physical or digital means via encryption

Security Measures for Data Creation
a) All data are to be owned by a designated owner and data creation and/or collection shall be authorised by the data owner
b) Data collected shall be classified and subjected to the corresponding security requirements

Security Measures for Data Usage
a) The purpose of use for the data shall be authorised by the data owner
b) Corresponding authentication requirements shall be required for access to the data depending on the classification of the data

Security Measures for Data Share
a) The purpose of sharing of the data and the parties to share the data with shall be authorised by the data owner
b) Corresponding security requirements shall be required for sharing of the data depending on the classification of the data
c) Encryption of the transmission of the data shall be used where it is required by the classification of the data to ascertain the confidentiality of the data and the authenticity of the receiving party.
d) Cross border transmission of data shall be conducted only when it is in compliance with the policies and local laws. Such transmission shall be recorded for future reference.

Security Measures for Data Storage
a) The storage medium shall be assessed for trustworthiness appropriate for the classification of the data
b) Technical measures shall be in place to provide appropriate protection in the confidentiality and integrity of the data stored that commensurate with the classification of the data

Security Measures for Data Destruction
a) Data that exceeds its designated retention period shall be regularly identified and deleted.
b) Data shall be safely destroyed throughout the cloud environment through secure erasure means such that it is not recoverable

Regular Review
a) The CSP shall regularly review the security measures for the data lifecycle for continuous improvement purposes.

2.1.2.2.5 Appropriate Security for Shared Security Responsibility

a) The CSC shall be cognisant of its security responsibility of the cloud application.

b) The CSC shall ensure that it has the resource, manpower and capabilities to implement the required security measures commensurable to the classification of the data processed in the areas of cloud computing that are responsible by the CSC particularly for the IaaS and PaaS cloud service model.
c) The CSC shall ensure that data classification and appropriate use of data are properly performed when using the SaaS cloud service model.
d) The CSP shall ensure that data is only processed in its designated servers and network and connections to new servers and/or networks shall be authorised.

2.1.2.2.6 Encryption Certificate and Key Management

Encryption Algorithm

a) The CSC shall stipulate the encryption algorithm and key length to be used to protect the data at a commensurable level required of the data's classification. The encryption algorithm should be recognised as an international standard.

Encryption Hardware

a) The CSC shall stipulate the encryption hardware accreditation standard, if any, to be used to protect the data at a commensurable level required of the data's classification.

Qualified Personnel

a) The CSP shall deploy trained and qualified personnel to manage the encryption keys and certificates. The CSC shall assess the requirement for the CSC to manage keys or certificates and correspondingly ensure the availability of qualified CSC personnel for this purpose.

Key Management

The CSP shall centrally manage the keys used for encryption to ensure that the lifecycle of encryption keys (i.e. generation, storage, distribution, use, rotation, backup, recovery, suspension, destruction) are properly managed, accounted and authorised.

a) The CSP shall generate encryption keys via Hardware Security Module (HSM) for the protection of data when requested by the CSC or as required by the security classification of the data.
b) The encryption keys shall be distributed in a secure manner to ensure the confidentiality and integrity of the keys to the intended recipients.
c) The CSP shall ensure that recipients of the encryption keys are informed on the proper use and storage of the keys to ensure operational security. The recipients shall report any compromise or loss of the encryption keys as soon as possible.
d) The encryption keys shall be stored securely in an HSM or if Key Encryption Keys (KEK) are used, they shall be at least as strong as the keys that are being protected. KEKs shall not be kept together with the keys that are being protected and techniques such as key splitting can be used to enhance the protection of encryption keys.
e) The encryption keys shall be rotated securely on a regular basis.
f) The CSP should archive old encryption keys securely and use it for only decrypting purposes where necessary.
g) The CSP shall assess and plan for the risks arising from the loss, leakage, corruption and destruction of encryption keys and implement measures to recover from such incidents.

Certificate Management

The CSP shall centrally manage the certificates such that the purpose, validity and the responsibilities of the certificate users are properly accounted for and authorised.

a) The CSP shall ensure a secured environment to generate the certificate to be issued by an authorised Certificate Authority (CA).
b) The CSP shall ensure a secured environment to store the certificate.
c) The CSP shall ensure a secured environment to destroy the certificates that are expired or corrupted.
d) The CSP shall assess and plan for the risks arising from the lost, leakage, corruption and destruction of certificates and implement measures to recover from such incidents.

Regular Review

The CSP shall regularly review the key and certificate management policies and processes to ensure the sufficiency of the security measures and identify new measures to enhance the operational effectiveness of the processes.

2.1.2.3 Domain 6 Cloud platform O&M security

2.1.2.3.1 Introduction

stipulates the requirements for the tenant to ensure that while the CSP managing a multitude of change requests to a wide range of components within its cloud infrastructure, all such changes are mediated through a controlled manner to record their origin, authority, purpose and impact assessment.

2.1.2.3.2 Identity and Access Management

User Account Management

a) Unique account names shall be assigned to their users, set validity periods, and identify cross-organization accounts.
b) Accounts that fail authentication attempts up to 6 times shall be locked, with a lockout duration of at least 30 minutes.
c) Accounts that have not been used for more than 60 days shall be automatically locked and will be deleted after 90 days of being locked

Privileged Account Management

a) The use and access of privileged accounts shall be restricted through management tools such as bastion hosts.
b) The use of local administrator accounts shall be prohibited. If such accounts need to be used, explicit approval shall be obtained and such accounts shall not be used for daily business activities.
c) Third parties can use privileged accounts only under the direct supervision of CSPs and shall terminate the access immediately after the use.

Service Account Management

a) When creating accounts, CSPs shall specify their purposes and ensure that the creation is approved by their management personnel. In addition, they shall allocate one-time or time-limited passwords, or implement dual control.
b) Interactive login shall be prohibited when using the account, and simultaneous logins shall be restricted. The password shall be changed at least twice a year or when an administrator quits.

Permission Management

a) Permission management shall follow the principles of on-demand allocation, minimum authorization, and separation of duties (SOD).
b) Role-based control (RBAC) or attribute-based access control (ABAC) mechanisms shall be adopted.
c) Approval from the management personnel shall be obtained for granting permissions to access a cloud service management network and tenant network.
d) Users shall be provided with self-service authorization requests, with identity verification and approval obtained before authorization.
e) When the responsibilities of internal or external personnel change, relevant account and permission shall be changed within 24 hours.

Password Management

a) The password policies shall comply with industry standards. Common or shared passwords or those that are the same as accounts must not be used.
b) Random initial passwords shall be assigned, with an expiration period of no more than 14 days. The initial passwords shall be changed upon the first login.
c) User identity shall be verified before resetting passwords, and the quality of the reset password ensured.
d) Password transmission shall be protected, and plaintext protocols shall be prohibited.

e) Passwords shall be encrypted for storage, The static authentication credentials that are not encrypted must not be included in applications or access scripts.

Multi-Factor Authentication

a) Multi-factor authentication (MFA) shall be implemented for all remote and privileged account access.
b) At least one cryptographic technique of MFA shall use password technology to implement, or in an out-of-band manner. The password shall be reset if multi-factor devices are lost.
c) MFA shall be bound to a unique account, and MFA factors must not be shared among different accounts. The minimum and maximum validity periods and reuse conditions must be specified. When the role or attribute changes, the MFA factors must be updated accordingly.

Session Management

a) Notification messages or banners shall be displayed to users who attempt to access the system.
b) The session shall be terminated if it is idle for more than 15 minutes, and the user shall be required to perform authentication again.
c) Multiple concurrent sessions are not allowed for the same account.

Periodic Review

a) All accounts and permissions shall be reviewed at least once every 30 days, and rectification shall be completed within seven days if any deviation is found.

2.1.2.3.3 Certificate and Key Management

Cryptographic Algorithm and Key Management

a) Cryptographic algorithms that comply with international and industry standards shall be used.
b) The use of cryptographic technology and products, as well as key management, shall comply with local laws and regulations.
c) A key usage and protection strategy shall be developed and implemented throughout its entire lifecycle.

Key Generation and Distribution

a) Hardware cryptographic modules shall be used to implement cryptographic operations and key management, and authentication mechanisms shall be set up for operators.
b) Secure random number generators shall be used to generate keys, and the key strength must be greater than or equal to the cryptographic algorithm.
c) Private keys used for device authentication shall be generated separately on each device, and exporting private keys from devices shall be prohibited.
d) Secure channels shall be used for key distribution to ensure the confidentiality and integrity of the keys.

Key Storage

a) Keys shall be stored in a secure and controlled location.
b) Root keys and encryption keys for personal sensitive data shall be stored on tamper-resistant devices, encrypted and stored separately, or stored using key components that are not less than their length.

Key Rotation and Destruction

a) Key rotation cycles shall be defined based on industry standards, laws, and regulatory requirements.
b) countermeasures shall be developed for the loss, leakage, damage or destruction of keys or key components, taking into account the risk of data leakage.
c) Unused keys shall be destroyed, and expired data encryption keys shall be archived.

Centralized Certificate Management

a) Certificates shall be uniformly and securely managed, with clear purposes, custodians, and expiration dates for each certificate.

b) Certificates shall be issued by trusted Certificate Authority (CA) and the validity period shall not be longer than that of the CA certificate.
c) When certificates are about to expire, private keys are leaked, or the algorithms are non-compliant, the certificates shall be replaced.

Periodic Review

a) Audits shall be conducted at least once a year and in the event of significant changes or security incidents, including:

Control policies related to certificate and key management
Strength of keys and cryptographic algorithms

2.1.2.3.4 Security Configuration Management

Security Configuration Baseline

a) A security configuration management plan shall be developed.
b) A security configuration baseline that complies with industry standards shall be established.
c) Software and hardware assets shall be strengthened according to the security configuration baseline.

Configuration Monitoring

a) Automated check tools shall be provided to centrally manage the security configuration baseline.
b) Deviations from the security configuration baseline shall be analyzed, reported, and rectified.

Periodic Review

a) The security configuration baseline, including important configurations such as antivirus database, intrusion detection rule libraries, firewall rule libraries, and vulnerability libraries, shall be audited at least once a year or in the event of significant changes.

2.1.2.3.5 Change Management

Change Application and Authorization

a) Changes shall be documented, risk assessment and classification shall be assessed.
b) Risk assessment information shall be provided to CSCs for high-risk changes or as contractually required.
c) Change and rollback solutions shall be developed, reviewed and approved before implementation, and technical measures shall be implemented to prevent unauthorized changes.
d) Change and rollback plans shall be tested based on risk impact analysis.

Change Notification and Implementation

a) Stakeholders shall be notified of the impact of the changes, including the change scenario, time, type, scope, and impact.
b) Backups shall be made before the implementation of changes to ensure that rollback can be performed in case of failure, and remedial measures shall be provided in case of rollback failure.
c) Records shall be kept during the change process to ensure traceability of change operations.
d) The effectiveness of changes shall be verified and the configuration library shall be updated synchronously after the implementation of changes.

2.1.2.3.6 Capacity Management

Capacity Management Planning

a) Capacity demand shall be assessed at least once a year, and a capacity baseline shall be established.
b) Future trends in capacity demand shall be predicted, appropriate measures shall be taken, and requirements from cloud customers shall continue to be met in the event of capacity bottlenecks.

c) The utilization rate of key resources shall be continuously monitored, resource capacity alarm rules shall be set up, deviations from resource and capacity baselines shall be analyzed and reported, and corrective actions shall be taken.

2.1.2.3.7 Logging and Monitoring

Enabling Logging

a) The system types for startup logs shall include physical access control systems, network devices, hosts, virtualization platforms, application software.
b) Logs shall be recorded for access control, O&M operations, sensitive data access, system events.

Log Management

a) A log management system shall be used to collect and analyze logs in a centralized manner.
b) Sensitive data in logs shall be anonymized during collection and processing.
c) Logs shall be periodically backed up, and protective measures shall be taken for both logs and their backups.
d) Security audit logs for the past 6 months shall be available for online querying, and offline archives shall be kept for at least 1 year.

Periodic Review

a) The log collection and management strategy shall be reviewed at least once a year or when significant changes occur.

2.1.2.3.8 Backup and Restoration

Backup and Restoration Management

a) Data and systems that require regular backups shall be identified, and regular backups shall be implemented.
b) Corresponding backup and recovery strategies shall be formulated based on service contracts and business continuity requirements.
c) The execution of data backups shall be monitored, and relevant responsible parties shall be notified and corrective actions taken when anomalies are detected.
d) Backups shall be protected, including but not limited to implementing offline backups, encrypted storage and transmission, access control, as well as physical and environmental security measures.
e) Backup recovery testing shall be conducted at least once a year.

2.1.3 Area 3 Resilience Considerations

This area introduces anti-attack capability of the cloud platform, business continuity management, effective and efficient use of cloud services.

2.1.3.1 Domain 7 Threat & Vulnerability Management

2.1.3.1.1 Introduction

Effective CSPs institute a comprehensive threat and vulnerability management regime to proactively minimize its attack surface area. Regular vulnerability scanning and penetration testing exercises should also be scheduled to surface vulnerable pathways for remediation.

2.1.3.1.2 Threat and Vulnerability Programme

a) The CSP shall institute a Threat and Vulnerability Programme that established the corresponding policies and processes to ensure the consistent and continuously improved outcome of the programme.
b) The Threat and Vulnerability Programme should deploy personnel that are qualified for the area of threat and vulnerability management listed, but not limited to, below or equivalent:
   - Global Information Assurance Certification (GIAC) Penetration Tester (GPEN)
   - GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
   - GIAC Enterprise Vulnerability Assessor (GEVA)

c) The Threat and Vulnerability Programme shall cover the software and applications that are used by the CSC and not directly supplied by the CSP particularly where the Cloud Service Model deployed is IaaS or PaaS. The CSP shall propose arrangements that will support the software/applications provided by the CSC such that potential exposures due to corresponding threats and vulnerabilities are similarly managed.

2.1.3.1.3 Malware Protection Use of Anti-Malware solutions

a) The cloud infrastructure shall install centrally-managed anti-malware solution to ensure prevention, detection and eradication of malicious software.
b) The cloud infrastructure should also deploy network access control technologies such as firewall and Intrusion Detection Systems (IDSs) at critical network segments and servers.
c) Anti-malware solutions shall be capable of continuous monitoring the protected server/computer and raise alerts when necessary.
d) Anti-malware solutions shall be capable of regular scanning
e) Anti-malware solutions shall be capable of self-checking to prevent being compromised by malicious software before operation.
f) Anti-malware solutions shall be capable of updating itself daily or when new updates are made available by the vendor.
g) Anti-malware solutions shall have daily update of its malware database.
h) Anti-malware solutions shall be capable of rollback to earlier versions of itself to recover from a corrupted version update.

2.1.3.1.4 Vulnerability Management Vulnerability Awareness

a) The CSP shall conduct regular Vulnerability Scanning and Analysis Exercise (VSAE)
b) The VSAE shall be conducted using automated tools and by qualified personnel.
c) The VSAE shall be conducted in a manner that does not disrupt or minimise its impact on the cloud applications. The CSP shall duly notify the CSC in advance on upcoming VSAE particularly if the IaaS or PaaS model is used.
d) The VSAE shall utilised the latest vulnerability database of good quality and detect insecure configurations of the scanned system.
e) The VSAE shall be conducted on CSP's production servers as well as computing resources that are accessible to the public (e.g public APIs)
f) The VSAE shall be conducted monthly, when there is a major change in the CSP's cloud infrastructure and when an emergency notification on a high-impact vulnerability.
g) The VSAE shall rate the discovered vulnerabilities against the Common Vulnerability Scoring System (CVSS) framework to ascertain the severity of the vulnerabilities and its associated exposure.
h) The result of the VSAE scanning shall be collated and analysed on a regular basis to determine the progress and effectiveness of the exposure mitigation process.

Vulnerability Mitigation

a) Identified vulnerabilities shall be mitigated within a specific timeframe that commensurate with the corresponding exposure. The CVSS rating for the vulnerability shall be used to determine the timeframe. Specifically, the CSP shall be capable of mitigating vulnerabilities that are rated severe (CVSS 9 to 10), or are determined otherwise, within 24hrs upon request.
b) Vulnerability mitigation shall be documented and processed for automated patching where feasible.
c) Testing of the patches used for vulnerability mitigation shall be tested prior to installation.
d) Vulnerabilities that cannot be mitigated within the specific timeframe shall be formally assessed for ongoing monitoring of the resulting exposure until the case is closed.

Vulnerability Disclosure

a) The CSP should share, with affected customers, relevant information of vulnerabilities, its status of mitigation and whether there are follow-ups actionable by the customers.
b) Disclosure of vulnerabilities to external parties that are not customers or operators of the CSP shall be authorised.

2.1.3.1.5 Security Testing

a) Security Testing such as Penetration Testing shall be conducted on the CSP cloud infrastructure regularly. This should include systems that are accessible from the Internet as well as critical systems.
b) Security Testing shall be conducted while minimising impact to the operation of the target system. Customers who are affected by the testing shall be duly notified in advance.
c) Penetration Testing shall be conducted by qualified personnel using industry standards to ensure effectiveness and minimal impact to the operation of the cloud infrastructure.
d) Each Penetration Testing shall be authorised with a plan that identifies the objectives, target of test and specifics of the test such as test window and how the test is to be conducted.
e) Penetration Testing that are conducted on systems that are critical shall be conducted by a team of at least 2 operators to minimise human error.
f) A report shall be prepared to collate the discovery of the Penetration Test for assessment on the risk mitigation.
g) A verification test shall be conducted upon the rectification of the vulnerabilities and exposures discovered by the Penetration Test.

2.1.3.1.6 Security Monitoring

a) Logs that are indicative of security incidents shall be centrally collected and collated for automated monitoring and alerts.
b) Manual investigation of potential incidents shall be triggered by the security monitoring process so that relevant technical expertise can be brought to attend to anomalous events and incident response procedure can be initiated where necessary.

2.1.3.2 Domain 8 Business Continuity Management

2.1.3.2.1 Introduction

A business continuity management (BCM) programmed helps ensure that business continuity (BC) and disaster recovery (DR) plans are put in place to address contingencies such as disasters and crisis so as to continue providing an acceptable level of service to its customers.

2.1.3.2.2 Business Continuity Management (BCM), Business Continuity Plans (BCP), and Disaster Recovery Plans (DRP) Should Be Formalised

Formalised Plans

a) BCM, BCP and DRP documents shall be developed, approved, formalised, and communicated to all relevant parties.
b) A risk-based approach shall be taken when developing these documents.
c) Plans and documents shall be developed according to international best practice. An example would be the ISO 22301:2019, Business Continuity Management Systems (BCMS), which specifies the requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise. The ISO 22301:2019 BCMS is intended to be applicable to all organizations, or parts thereof, regardless of type, size and nature of the organization.
d) A physically separate alternate recovery site shall be provided for.

Contents of Formalised Plans

The key requirements to be covered by the plans are, but not limited to, as follows:

a) Identified critical systems that support the services provided
b) Identified supporting systems to these critical systems
c) Impact analysis for identified disruptions
d) Identifying the Maximum Tolerable Period of Disruption (MTPD)
e) Identifying the Recovery Time Objective (RTO) of each identified system
f) Identifying the Recovery Point Objective (RPO) of each identified system

g) System restoration prioritisation based on the criticality of the identified system
h) RTO and RPO shall include failover to a geographically locations in other countries

Access Control

a) A regular review of all users' accesses made to network, systems, applications, and data shall be performed to ensure that all accesses made are authorised.
b) A regular review of all users' entitlements to network, systems, applications and data, shall be performed to ensure that all entitlements are appropriately based on principles of separation of duties and least privilege, and commensurate with the risk level and information classification of the data being accessed.
c) Strong authentication and multi-factor authentication controls shall be deployed, especially for privileged accounts
d) Strong authentication and multi-factor authentication controls shall be deployed for all cloud accounts.

2.1.3.2.3 Consider Redundancy and High Systems Availability from the Beginning

a) Redundancy and high availability capabilities shall be considered for all critical systems as well as the supporting infrastructure and systems.
b) Relevant resources such as manpower and budgets to operate and maintain these critical systems shall also be planned for these critical systems.

2.1.3.2.4 Roles and Responsibilities Should be Clearly Defined

a) Roles and responsibilities shall be formalised for each of the BCM, BCP, and DRP documentation.
b) Roles and responsibilities shall be maintained and communicated to all relevant personnel.
c) All relevant personnel shall be familiarised with their respective roles and responsibilities in the event of a disruption event.

2.1.3.2.5 Ensure Risk Assessment and Business Impact Analysis

Risk Assessments

a) Ascertain if there are any previous risk assessments performed to address identified disruption scenarios.
b) A key asset inventory/register shall be maintained to identify all the key systems and processes that are required for maintaining business operations.
c) Risk assessments shall be conducted to ascertain critical systems as well as the events that can cause disruptions to the business operations.
d) Risk assessments shall help to identify whether BCP and DRP shall be formalised for the identified critical systems.
e) The CSC shall also consider the possibility of a CSP experiencing either the entire CSP or a major portion of the CSP infrastructure not being available. The CSC may consider accepting the risk or consider alternative plans to continue business operations in such a disruption. Examples would be to consider alternative business continuity locations or alternative CSPs.

Business Impact Analysis

a) A Business Impact Analysis (BIA) shall be performed, based on the information provided from the Risk Assessment.
b) All key business processes and systems shall be identified and prioritised based on criticality and impact to the organisation.
c) The Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) shall be defined.

2.1.3.2.6 BCM, BCP and DR Plans are Regularly Reviewed and Tested

Regular Documentation Review

BCM, BCP and DRP documents shall be regularly reviewed, at least annually.

Regular Testing

a) BCM, BCP, and DRP testing for identified scenarios shall be conducted regularly, at least annually.

b) Testing may be performed, either in part, for individual teams or departments/ functions, or as an overall plan for an entire organisation.
c) After the completion of each testing, a post-mortem shall be conducted and remediation or improvement points shall be implemented and updated in the relevant documentation.

Practical Drills
Drills of various scenarios shall be conducted on a regular basis, at least annually, to ensure data centre personnel preparedness and familiarity with DRP procedures in the event of a real incident occurring, such as:

- Power failure
- Fire
- Infectious biological virus outbreak (eg. SARS, COVID19)

Table-Top Exercises
Table-top exercises shall be conducted on a regular basis, at least annually, in addition to the practical drills, where certain scenarios may not just be an environmental incident, and still have the potential to disrupt data centre availability, such as:

- Terrorist attack on the data centre
- Terrorist attack on supply chain providers (eg. utility providers)
- Cyber-attack on the network infrastructure
- Cyber-attack on the systems such as servers and endpoints

2.1.3.2.7 Backups are Regularly Performed

a) Backup media shall be located off site from the primary location.
b) Backup media shall be regularly tested to ensure that they are still operational.
c) Backup media shall be encrypted to ensure that any data is protected.

2.1.3.3 Domain 9 Interoperability and Portability

2.1.3.3.1 Introduction

Interoperability and portability are essential to the effective and efficient use of cloud services. Interoperability enables the interaction between cloud services, as well as between cloud and non-cloud services, while portability enables cloud service customers (CSCs) to move their data and/or applications effectively and efficiently between non-cloud and cloud services, and between cloud services.

2.1.3.3.2 Implementation Planning

Interoperability Considerations
a) Due consideration shall be given to identifying a suitable CSP that has the capability to work well with the CSC, as well as other CSPs that the CSC may depend on, and has the properties needed to facilitate successful interactions between both parties' ICT facilities.
b) Interoperability requirements tend to be an issue of implementation costs, as such, a cost-benefit analysis shall be performed to determine whether the resources needed to assure exchange of information in the prescribed method while obtaining predictable results is worth the effort, time, and costs.

Portability Considerations
a) Due consideration shall be given to identifying CSPs that have the capabilities to allow for CSCs to migrate or move their data easily and adapt their applications suitably between the systems of the CSCs and CSPs.
b) Portability requirements tend to be an issue of implementation costs or "switching costs", as such, a cost-benefit analysis shall be performed to determine whether the ability to porting applications and/or data is worth the effort, time, and costs.

Documentation

a) There shall be a comprehensive and formalised interoperability and portability implementation plan that is approved by senior management for the cost-benefit analyses and the acceptable risk level of the interoperability and portability capabilities provided to the organisation by the CSPs.
b) Policies, guidelines, and procedures related to interoperability and portability shall be formalised and communicated with all relevant parties. As well, all documentation shall be reviewed regularly to maintain relevance to changes in internal processes and latest industry standards.

2.1.3.3.3 Interoperability and Portability SaaS Model

a) Insist on standard APIs, protocols, and data formats whenever possible.
b) Compatibility of on-premise applications and the cloud services shall be considered.
c) Compatibility of cloud services provided by different CSPs shall be considered.

PaaS Model

a) The application environment (web server, database server, etc.) supported by the CSPs shall be compatible with the on-premise application environment for application migration purposes.
b) The application environment shall be based on open technologies to ensure portability between CSPs, if a change in provider is warranted.

IaaS Model

a) CSPs shall support key open technologies, accepts standard or widely accepted application packaging formats (OVF, Docker, etc.), and any interfaces and APIs are open and/or standard.

Application Programming Interfaces (APIs)

a) On-premise applications shall leverage Service-Oriented Architecture (SOA) design principles to ensure the ability to utilise and expose APIs to enable interoperability with remote cloud services.
b) Where cloud services require access to on-premise APIs or data, suitable API Management capabilities shall be put in place to prevent unauthorised access.
c) Where using multiple CSPs, security technologies shall be supported and usable between the CSPs.

2.1.3.3.4 Legal

2.1.3.3.4.1 Due Diligence

a) Contracts and/or agreements between the organisation and CSPs shall be subjected to comprehensive review and due diligence to ensure that terms and conditions are not detrimental to the organisation.
b) The CSP shall be assessed comprehensively in their capability to ensure data residency security requirements for critical and/or sensitive data.
c) The employees of the CSP that will be directly or indirectly involved in the service provisioning shall be assessed comprehensively to ensure that they are based locally and have been subjected to appropriate security clearance.

2.1.3.3.4.2 Contractual Obligations

a) The contracts and/or agreements between the organisation and CSPs shall not subject the organisation to an unnecessary lock-in duration, nor include a complicated termination process.
b) The contracts and/or agreements between the organisation and CSPs shall include data portability provisions, where upon termination, will indicate the length of time the data will continue to be stored by the CSP, the scope of data retained and made available by the CSP, and the data deletion process of the CSP.

3 Bibliography

The OIC CERT Cloud Security Framework references the following international cloud security standards:

(1) ISO/IEC 27001 Information Security Management Systems (ISMS)
(2) Multi-Tiered Cloud Security (MTCS) Singapore Standard SS584
(3) Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) v4.0
(4) ISO/IEC 31000:2018 Risk Management
(5) ISO/IEC 22301:2019 Security and Resilience - Business Continuity Management Systems
(6) ISO/IEC 27701 Privacy Information Management
(7) ISO/IEC 27017 Code of Practice for Information Security Controls
(8) ISO/IEC 27018 Code of Practice for Protection of Personally Identifiable Information
(9) Cloud Computing Compliance Criteria Catalog (C5)
(10) CSA CoC for GDPR Compliance
(11) Payment Card Industry Data Security Standard (PCI DSS)
(12) AICPA Trust Service Criteria（SOC2）
(13) The NIST Cybersecurity Framework 2.0
(14) COBIT 2019 for Information Security
(15) Baseline for Classified Protection of Cybersecurity (GB/T 22239-2019)
(16) Information security technology—Security capability requirements for cloud computing services (GB/T 31168-2020)

