CCM v4.0 Implementation Guidelines

CSA cloud security alliance®

Acknowledgments

Lead Authors:

John Britton
Bobbie-Lynn Burton
Daniele Catteddu
Aradhna Chetal
Peter Dickman
Angell Duran
Rajeev Gupta
Shawn Harris
Roberto Hernandez
Matthew Hoerig
Erik Johnson
Harry Lu
Claus Matzke
Vani Murthy
Johan Olivier
Bala Kaundinya
Nancy Kramer
Surinder Singh Rait
Michael Roza
Agnidipta Sarkar
Lefteris Skoutaris
Ashish Vashishtha

Contributors:

Sandra Ackland
Geoff Bird
Madhav Chablani
Ramon Codina
Mamane Ibrahim
Joel John
Giovanni Massard
Jean-Sebastien Mine
Chirag Sheth

CCM Leadership:

Daniele Catteddu (CSA)
Sean Cordero
Sean Estrada
Shawn Harris
Harry Lu
Lefteris Skoutaris (CSA)

CSA GLobal Staff:

Claire Lehnert (Design)
Stephen Lumpe (Cover)

About the CCM WG

The Cloud Control Matrix (CCM) Working Group (WG) comprises cloud industry professionals, such as cloud security professionals, auditors, operators and a great number of organizations, representing both providers and consumers of the cloud, as well as consulting/auditing firms.

The *CCM v4.0* and its implementation guidelines stem from collective work built on group experience and feedback. As a result, it provides the community with one of its best vendor-neutral cloud security and privacy control frameworks.

Co-chairs supervise the WG activities. These individuals are highly experienced professionals representing three roles in the cloud industry: cloud service providers (CSPs), cloud service consumers (CSCs), and cloud auditors.

All contributions are personal and shall not constitute a commitment or opinion by the contributor or the contributor's organization.

The permanent and official location for Software Defined Perimeter Working Group is https://cloudsecurityalliance.org/research/working-groups/software-defined-perimeter/

Table of Contents

Table of Figures

Executive Summary

The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) provides fundamental security principles, controls, and controls criteria to guide cloud service providers (CSPs) and cloud service customers (CSCs) seeking secure implementation, assessment, and management of cloud services security risks. The CSA CCM provides a detailed controls framework aligned with CSA's Security Guidance[1], which states that "the most important security consideration is knowing exactly who is responsible for what in any given cloud project". The CCM now includes a comprehensive structure for delineation and proactive management of the cloud shared security responsibility model (SSRM), with transparency and accountability across the entire supply chain to operationalize this crucial concept.

The *Cloud Security Alliance's Cloud Controls Matrix Version 4 (CCM v4.0),* published in 2021, includes core security and privacy controls and additional components. These include CCM Implementation Guidelines (included in this document), the Consensus Assessment Initiative Questionnaire (CAIQ), and the CCM Controls Auditing Guidelines[2]. The *CCM v4.0* also includes useful supporting information for CCM controls. This information includes typical SSRM control ownership assignments and control scope and applicability information, such as: architectural relevance and mappings to other industry-accepted security frameworks (e.g., ISO/IEC, AICPA, NIST, FedRAMP). These works are regularly reviewed and enhanced by the CSA team.

The CCM Implementation Guidelines constitute a new addition to *CCM v4.0*. These guidelines strive to support the application of CCM controls and provide further guidance and recommendations related to CCM control specifications. This document also provides structured guidance for navigating the CCM (spreadsheet format) framework and interpreting and implementing CCM control specifications to use the CCM effectively.

However, this document is not meant to be a "how-to" manual for the CCM controls implementation. Given the nature of CCM controls, their operationalization will largely depend on the IT/service architecture, the type of technology used, risks faced, applicable regulations, organizational policies, and other significant factors. Therefore, the CSA cannot provide detailed, prescriptive guidance pertinent to every organization and cloud service implementation.

The CCM Implementation Guidelines are a collaborative product of the volunteer CCM Working Group based on shared CSP and CSC experiences in implementing and securing cloud services and using CCM controls. Workgroup insight covers myriad topics and queries, including how can organizations:

> - implement controls for the first time?
> - improve an existing implementation?
> - answer a CAIQ question?
> - better understand what a customer's security responsibilities are?
> - leverage CCM controls within a specific platform or architecture?

[1] https://cloudsecurityalliance.org/research/guidance/, accessed on 8/12/2021.

[2] currently in peer review and to be released in November 2021.

1. Introduction

1.1 What is the Cloud Control Matrix

The CCM is a security control framework that is dedicated to managing risk in the cloud. It was developed to address the lack of a cloud-relevant security and compliance framework, because, at the time of its creation, risk management was solely focused on addressing traditional computing infrastructure. The CCM is meant to fill this gap by helping CSPs and CSCs assess overall cloud service security risks.

For CSPs, the CCM means to establish best practices to support the secure implementation of cloud infrastructure and services. For cloud customers, the CCM enables them to better evaluate and assess CSPs.

The CCM includes detailed security concepts and principles aligned with *CSA Security Guidance v4,* which guides "how" security principles should be implemented in a cloud architecture. Conversely, the CCM recommends "what" should be done. The CSA encourages organizations to use the CCM as a companion to the *CSA Security Guidance* because it allows users to identify security controls and understand how they should be applied.

1.1.1 CCM Purpose and Scope

Regardless of organizational types (CSPs vs. CSCs), the nature of an enterprise, organizational sizes (i.e., large corporation vs. small company), or cloud delivery models, IaaS vs. PaaS vs. SaaS, the CCM can be used to define, implement and enforce security requirements and monitor their implementation. The CCM assists companies in translating their internal organizational, operational, and legal stipulations into a standardized set of cloud-relevant policies, procedures, and technical control objectives.

The CCM is also a tool for internal and external assessments or audits. It is designed to be used in alignment with the CAIQ, which provides a set of "yes" or "no" questions that can be answered to determine if the CCM controls are being met. Both documents help auditors understand if an organization follows its internal governance policies and fulfills its legal and regulatory obligations.

For example, based on an internal risk assessment, an organization might identify the need to protect the confidentiality, integrity, and availability of information related to a manufacturing process. The datasets have varying levels of sensitivity and criticality, as they are stored in a cloud database and processed by several cloud-based applications. The organization can use the CCM to identify specific policy, procedural and technical requirements and define control objectives that will be included in the organizational security program. It uses those control objectives to enforce mandates related to internal users, business partners, and CSPs and monitor adherence to internal policies and external compliance requirements.

1.1.2 CCM Structure

The *CCM v4.0* is structured into 17 security domains and 197 controls. The 17 domains were based on CSA's security guidance document and inspired by major frameworks, such as *ISO/IEC 27001* and *ISO/IEC 27002*. Each CCM domain defines what category a control falls under. CCM was deliberately designed like existing non-cloud leading information security frameworks to leverage familiarity with those existing frameworks.

A&A	Audit & Assurance
AIS	Application & Interface Security
BCR	Business Continuity Mgmt & Op Resilience
CCC	Change Control & Configuration Management
CEK	Cryptography, Encryption & Key Management
DCS	Datacenter Security
DSP	Data Security & Privacy
GRC	Governance, Risk Management & Compliance
HRS	Human Resources Security
IAM	Identity & Access Management
IPY	Interoperability & Portability
IVS	Infrastructure & Virtualization Security
LOG	Logging & Monitoring
SEF	Sec. Incident Mgmt, E-Disc & Cloud Forensics
STA	Supply Chain Mgmt, Transparency & Accountability
TVM	Threat & Vulnerability Management
UEM	Universal EndPoint Management

Figure 1: List of CCM v4 cloud security domains and their acronyms

1.1.3 CCM Domains Description

The *CCM v4.0* includes 17 cloud security domains. These domains are listed below, along with a description of each one's unique purpose and use.

Audit and Assurance

The Audit and Assurance (A&A) domain consists of six (6) control specifications. This domain is designed to support the CSP and CSC in defining and implementing an audit management process to support audit planning, risk analysis, security control assessment, conclusion, remediation, report generation, and reviews of past reports and supporting evidence.

Having a clear understanding of the level of assurance expected by customers along with industry compliance standards and self-imposed business requirements is of paramount importance for CSPs. Failing to execute an auditing plan can have substantial negative impacts regarding loss of control and governance, compliance shortcomings, and ultimately financial, operational, and reputational damages.

The Audit and Assurance domain utilizes six controls that support CSPs. The domain:

- Defines and maintains an audit and assurance policy and procedures.
- Performs independent assessments.
- Performs independent audit and assurance assessments according to risk-based plans and policies.
- Verifies compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.
- Manages the audit process and prepares and executes a risk-based corrective action plan to remediate audit findings.
- Reviews and reports the remediation status to relevant stakeholders.

Application and Interface Security

The Application and Interface Security (AIS) domain involves seven (7) control specifications to help cloud organizations migrate towards secure design, development, deployment, and operations of applications and their interfaces in the cloud. The AIS controls assist organizations in identifying risks to cloud landscapes and mitigates these risks in the application's design and development phase. It is also vital that organizations test cyber resilience to threats with remediation of vulnerabilities by complementary automation and manual code review in the deployment and operations phase. The controls also help organizations align their AIS security goals with business objectives and regulatory compliance.

Business Continuity Management and Operational Resilience

The Business Continuity and Operational Resilience (BCR) domain helps CSPs and CSCs ensure that cloud services they provide or use are dependable. The domain guides resiliency strategies—including the development of mitigation planning and implementation efforts—to enable organizations to continue business when faced with foreseen and unforeseen disruptions. The domain consists of eleven (11) control specifications. The first three specifications aid businesses in defining business continuity and operational resilience policies, assess the impact of unavailability and associated risks and determine strategies to reduce disruption impacts. The next four specifications support actions to create business continuity plans and related documentation, exercise the documented continuity plans, and establish a formal communications capability. The final four specifications help establish backup capabilities, an official disaster response plan, exercise the disaster recovery (DR), and install relevant equipment redundancy. The BCR domain should help establish assurances about the ability to respond to, withstand, and recover from disruptions.

Change Control and Configuration Management

The Change Control and Configuration Management domain incorporates nine (9) controls. These controls are designed to mitigate risks associated with configuration changes to information technology (IT) assets by adherence to a robust change management process—regardless of whether IT assets are managed internally or externally.

This domain ensures IT asset configurations are only modified to an approved baseline after the change management authority authorizes planned changes.

Cryptography, Encryption and Key Management

The Cryptography, Encryption and Key Management (CEK) domain consists of twenty-one (21) control specifications designed to ensure that data and keys are employed to protect and properly secure data. The CEK controls span the Governance, Risk management, and Compliance (GRC) spectrum. They are applicable for governing policies and procedures, risk management, the processing of key lifecycle activities, and cryptographic key management systems (CKMS). Additionally, CEK controls' implementation is a shared responsibility. Generally, the provider is responsible for the security "of" the cloud, while the customer is responsible for the security "in" the cloud. The detailed implementation and allocation of these responsibilities are dependent on the model (i.e., on-premises, in the cloud, hybrid, etc.), services used (IaaS, PaaS, SaaS), and the applicability of any laws and regulations.

Datacenter Security

This domain consists of fifteen (15) control specifications that aid organizations providing data center hosting services, referred to as "Cloud Service Providers". These CSPs are expected to implement these specifications to protect cloud service customers› data hosted in the data center. The controls cover a wide range of topics on data center security, with one control per control title. All controls in this domain are expected to be implemented, and each control is of equal importance. This is true in the rest of the domains as well.

Data Security and Privacy Lifecycle Management

The Data Security and Privacy Lifecycle Management domain is a new domain introduced in *CCM v4.0*. It features nineteen (19) controls on privacy and data security. These controls are not industry or sector-specific and not focused on a particular country or regulation. However, these controls have been developed by considering the common elements and requirements of major privacy regulations. They are generally applicable to organizations worldwide and are expected to serve as a valuable baseline—with the caveat that some organizations operating in some locations or sectors may have to implement supplemental data protection controls. Lastly, as with other domains, these controls have been developed after several rounds of analysis by an international team of subject matter experts (SMEs).

Governance, Risk Management and Compliance

The Governance, Risk Management, and Compliance (GRC) domain uses eight (8) control specifications to support, define, and direct organizational security and compliance efforts (specifically corporate and IT governance). Governance controls help manage confidentiality, integrity, and availability (CIA) by providing guidance, tools, and solutions for ensuring a secure environment.

The GRC domain's objective is to provide direction for all levels of security commonly managed by a governance committee or board of directors. This domain is structured to develop, implement, and document security policies (regulatory, advisory, and informative), governance and enterprise risk programs, standards, baselines, guidelines, and procedures to meet compliance while reducing risks and vulnerabilities with the implementation of security controls.

Human Resources

The Human Resources (HRS) domain is pivotal to the success of an organization's compliance structure. Human Resources is the conduit between IT security and personnel and encompasses personnel interaction with systems, technology, assets, and data. The domain utilizes thirteen (13) controls to support the organization in ensuring personnel comply with security policies designed to protect the organization, clients, and workforce. Key elements of the Human Resources domain include, but are not limited to, personnel background screening, employment agreement content, employee onboarding, communicating roles and responsibilities, security awareness training, code of conduct and the acceptable use of technology, remote work procedures, compliance responsibilities, role-change procedures, employee offboarding, and the return of organizational assets.

The Human Resources domain also includes controls necessary for ensuring that information security policies are correctly presented, documented, communicated, and enforced.

Identity and Access Management

The Identity and Access Management (IAM) domain features sixteen (16) control specifications and addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology cloud environments. The principles of least privileges and role-based access control are enabled by fulfilling IAM requirements. In addition, the IAM domain covers technical and organizational requirements to ensure that appropriate individual network entities—such as users and devices—have access to the relevant resources at the right times for the right reasons.

In the cloud context, users are employees and business partners of CSPs and CSCs. Domain requirements cover processes and technical best practices to securely manage and implement privileged and non-privileged access rights to cloud assets.

Interoperability and Portability

The CCM's Interoperability and Portability (IPY) domain has four (4) control specifications to address interoperability and portability in the cloud environment. Interoperability is the requirement that a processing system's components work together to achieve their intended result. Furthermore, it should be possible for the system to continue to work if elements are replaced with new or different parts from other providers. Portability allows application and data components to continue to work the same way when moved from one cloud environment to another without being changed. Portability is achieved by removing dependencies on the underlying environment. A portable feature can be moved easily and reused regardless of the provider, platform, operating system, location, storage, or other elements of the surrounding environment.

Lack of interoperability and portability can expose both cloud customers and CSPs to various risks, such as:

- Application, vendor or provider lock-in
- Processing incompatibility and conflicts causing service disruption
- Application reengineering or business process changes
- Costly data migration or data conversion
- Retraining or retooling management software may be required
- Loss of data or application security
- Lack of compliance

Organizations should have measures to mitigate risks related to the lack of interoperability and portability, which justifies control specifications. Examples of such actions include:

- Make published APIs securely available.
- Establish policies and procedures and define the terms of information processing interoperability and portability for application development.
- Implement standardized network protocols for the import and export of data.
- Implement standardized network protocols for the management of all interoperability and portability systems.
- Document relevant interoperability and portability standards in use.
- Use an industry-recognized virtualization platform and standard virtualization formats.

Infrastructure and Virtualization Security

The Infrastructure and Virtualization Security (IVS) domain guides CSPs and CSCs in implementing controls to secure infrastructure and virtualization technologies.

Infrastructure encompasses all hardware, software, networks, facilities, etc., required to deliver IT services. Virtualization technologies use software to create an abstraction layer over computer hardware that allows the hardware elements (such as processors, memory, storage, etc.) to be divided into virtual computers.

In on-premises operations, virtualization technologies are used for virtual desktops. Virtualization is also one of the vital elements of IaaS cloud offerings and private clouds.

The nine (9) controls in the IVS domain promote the implementation and maintenance of policies and procedures to effectively plan, secure, and improve infrastructure resilience and utilize virtualization technologies. These include:

- **Planning:** Accurate resource planning ensures availability, quality, and adequate resource capacity to deliver the required system performance (as determined by the business).
- **Security:** Network security measures, such as host operating systems hardening, monitoring, segmenting environments, and encrypting and restricting communications between environments to only authenticated and authorized connections.
- **Resilience:** Implementing best practices for migration to cloud environments, identifying high-risk environments and maintaining network architecture documentation, and defining and implementing defense-in-depth techniques for protection, detection, and timely responses to network-based attacks.

The planning, security, and resilience controls encompassed by the CCM IVS domain will improve the overall security posture of any utilized infrastructure and virtualization technologies.

Logging and Monitoring

Logging and Monitoring is a critical process of security operations. The thirteen (13) controls in this domain emphasize governance and process to empower organizations with cloud-based business with the means to realize efficient logging and monitoring.

Logs from operating systems, services, and applications play a crucial part in incident management and response, digital forensics, and the formation of a holistic view of business processes and assets. Organizations with standardized processes can leverage information being collected and correlated by logging and monitoring tools. These controls can help organizations govern the technical implementation of logging and monitoring tools.

Logging is necessary for non-repudiation, and monitoring and alerting help form timely responses to security incidents.

Security Incident Management, E-Discovery, and Cloud Forensics

The Security Incident Management, E-Discovery, and Cloud Forensics (SEF) domain has eight (8) control specifications designed to ensure that established policies and tested procedures are enacted to appropriately respond to security incidents to mitigate business risks (including any requirements for security breach notifications).

Supply Chain Management Transparency and Accountability

The Supply Chain Management Transparency and Accountability (STA) domain delineates a broad set of supply chain risk management controls, including requirements for:

> - Defining and managing the SSRM between the CSP and the CSC.
> - Third-party providers employ appropriate security measures to protect the confidentiality, integrity, and availability of information, applications, and services across the full technology stack.
> - Policies and procedures for monitoring and managing security and compliance across the supply chain.

The STA domain features fourteen (14) control specifications.

Threat and Vulnerability Management

The Threat and Vulnerability Management (TVM) domain consists of ten (10) control specifications that address a wide range of concerns that could develop into ongoing issues to the security architecture and engineering of an organization’s infrastructure. The domain focuses on assessing and mitigating vulnerabilities that may evolve and impact assets, security architectures, designs, and solution components. A management and risk mitigation strategy includes parameters to:

> - Control security issues.
> - Understand how security policies drive threat management.
> - Drive the ability to identify flaws to countermeasure attacks.

A vulnerability management plan should address internal and external event data clearly defined and documented, even with accepted risks. An organization's risk posture should include the following guidance measures in its threat and vulnerability risk management strategy:

> - Establish, implement, enforce and maintain policies, procedures, and technical measures to prevent the execution of malware on enterprise-owned or managed assets.
> - Implement technical measures and supporting processes for vulnerability detection and use a risk-based model to prioritize the remediation of identified vulnerabilities.
> - Implement a strategy for tracking and reporting vulnerability identification and remediation activities.
> - Provide stakeholders with a summary of identified weaknesses if the system owner shares responsibility for the remediation and inform stakeholders of the policies and procedures for threat and vulnerability management.
> - Update detection tools, threat signatures, and indicators of compromise.
> - Perform periodic penetration testing.
> - Establish metrics for vulnerability identification and remediation at defined intervals.

Additional domain elements may include vulnerability responses dependent upon other domains—including BCR, CEK, SEF, IVS, and SEF. This holistic vulnerability management appraisal assures that organizations identify and understand weaknesses and can plan accordingly.

Universal Endpoint Management

The Universal Endpoint Management (UEM) domain focuses on implementing controls to mitigate the risks associated with using a computer while outside the corporate office, including mobile devices and endpoint devices in general.

The risk with mobile computing and endpoint security mainly relates to user behavior and the awareness (or lack of awareness) of a company's approach to acceptable use of devices and technologies (e.g., managed vs. unmanaged, enterprise-owned vs. personal).

The UEM domain supports organizations in effectively implementing fourteen (14) control specifications such as maintaining an inventory of all endpoints, approving services and applications acceptable for use by endpoints, implementing security measures like automatic lock screens, firewalls, and anti-malware detection, and utilizing prevention technologies, storage encryption, and data loss prevention technologies.

The domain also supports aligning endpoint-specific policies and procedures with overall organizational security standards. These include:

> - Managing changes to endpoint operating systems, patch levels, and/or applications through the company's change management processes.
> - Implementing procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices.
> - Incorporating strategies and technical and/or contractual measures to maintain proper security of third-party endpoints with access to organizational assets.

Internet of Things (IoT) technologies are not included in the scope of this domain.

1.1.4 Components

Along with the core 197 security and privacy controls, the *CCM v4.0* includes additional tools, such as:

> - Controls Applicability Matrices.
> - Mappings.
> - Consensus Assessment Initiative Questionnaire (CAIQ).
> - Implementation Guidelines (included in this document).
> - Auditing Guidelines.
> - Metrics.

CCM Control Specifications and Applicability Matrices

The CCM control specifications are mapped to the controls applicability matrix, which is comprised of three main groups:

> - Typical Control Applicability and Ownership
> - The architectural relevance - cloud stack components
> - The organizational relevance

The typical control applicability and ownership matrix describes standard SSRM control ownership and applicability for all controls for the three main cloud service models: IaaS, PaaS, and SaaS. Common SSRM ownership designations allocate responsibilities typical for implementing a given CCM control between a CSP and a CSC, as required by control STA-04. Some controls are clearly the province of IaaS providers (e.g., data center security controls), whereas other controls are applicable across all service models (e.g., identity and access management). This CCM matrix describes the applicability of each control to the three cloud service models, helping users understand what is relevant in specific cases.

The architectural relevance group indicates the architectural relevance of each CCM control per cloud stack component from the perspective of the *CSA Cloud Reference Model*. The section focuses on numerous elements, including physical, network, compute, storage, application, and data. In addition, because the CCM is mapped to existing security controls specifications from various legal and regulatory frameworks—and that same matrix is mapped to the security capabilities of the architecture—enterprises can easily assess which capabilities comply with applicable regulations and best-practice frameworks.

The organizational relevance group indicates the connection between each CCM control and its implementation by the respective cloud relevant functions within an organization. The functions included are: "Cybersecurity", "Internal Audit", "Architecture Team", "Software Development Team", "Operations", "Legal/Privacy", "Governance/Risk/Control", "Supply Chain Management", and "Human Resources".

Scope Applicability (Mappings)

An important CCM aspect is that it maps to other security standards, regulations, and frameworks. When the CCM was created, there were already many different information security standards, best practices, and regulations in existence (e.g., ISO/IEC 27001 and 27002, PCI DSS, NERC CIP, BITS , BSI). Many companies already had their internal structures and frameworks set up and aligned with those standards.

The CSA wanted to provide cloud sector-specific controls while ensuring that organizations had clear paths to connect their existing control frameworks and programs with the cloud-relevant controls included in the CCM. Therefore, the CSA built all the controls created in the CCM as an extension of existing framework controls. The CSA constructed a mapping, or a linkage, between a framework control (e.g., ISO 27001) and the CCM to realize this ambition. The CCM then builds on the framework to provide a control specific to the cloud sector—and then takes it one step further by ensuring controls link to a particular area within a cloud architecture. Then, the CCM helps identify if a specific control is relevant for IaaS, PaaS, or SaaS. Because the CCM makes links through mapping, it provides an initial internal controls system that identifies which controls organizations should enact to further a cloud journey and implementation processes.

The Consensus Assessment Initiative Questionnaire (CAIQ)

The CAIQ provides cloud customers and auditors with questions for CSPs about security posture, adherence to CSA best practices (CCM and the CSA Security Guidance) and customer SSRM responsibilities. The CAIQ is a companion document designed to support better adoption of the CCM. While the CCM defines the control specification and implementation guidelines, the CAIQ defines questions to evaluate and inform implementation. In addition, the CAIQ (and the *CSA STAR Registry*) should be used by CSPs to provide SSRM ownership and customer security responsibility guidance to current and prospective CSCs per CCM controls STA-01 through STA-06.

The relationship between a CCM control and CAIQ questions is often one to many. This is by design because the CCM is based on 197 controls, whereas the latest version of the CAIQ (version 4) has 261 questions. Depending on the nature and the complexity of the CCM control, there may be one or several questions posed to verify the implementation of a certain control.

The CAIQ, similar to the CCM, comes in a spreadsheet format with a structure similar to the CCM. The CAIQ includes columns for CSPs to respond to CAIQ questions ("Yes," "No," or "NA") while specifying SSRM ownership of CCM controls the CAIQ question pertains to. The CAIQ also includes columns for CSPs to describe how they meet their portions of the controls and any associated customer security responsibilities. Cloud service providers should delineate SSRM ownership, explain how they meet control requirements, and clarify customer security responsibilities at the question level.

The CAIQ and the *CSA STAR Registry* provide a framework and forum for CSPs to provide useful information that current and prospective customers can use to evaluate how controls have been implemented. Furthermore, these tools enable providers to delineate their implementation of the SSRM for customer benefit.

Implementation Guidelines

The *CCM Implementation Guidelines* constitute a new addition to *CCM v4.0*. The guidelines' main goal is to support the implementation of CCM controls and provide further guidance and recommendations on CCM control specifications. The guidelines included in this document provide structured guidance on interpreting and implementing the CCM control specifications.

Sections 1.2 and 2 in this document introduce the *CCM Implementation Guidelines* and their contents. The *CCM Implementation Guidelines* are a collaborative product based on CSP and CSC experiences implementing and securing cloud services while using CCM controls under the SSRM. However, the guidelines are not meant to be a "how-to" manual for CCM control implementation. Given the comprehensive nature of the CCM controls, their operationalization largely depends on the nature of the cloud service and its architecture, the types of technology used, applicable risks and regulations, organizational policies, the threat environment, and other significant factors. Therefore, CSA cannot provide detailed, prescriptive guidance applicable to every organization and cloud service controls' implementation.

Auditing Guidelines

The *CCM v4.0 Auditing Guidelines (AGs)* are tailored to the control specifications of each of the 17 cloud security domains of the *Cloud Control Matrix version 4 (CCM v4.0)*. The guidelines represent a new component of CCM v4.0 that did not exist previously in CCM v3.0.1.

The AGs aim to facilitate and guide a CCM audit. Auditors are provided with a set of assessment guidelines per *CCM v4.0* control specifications. These guidelines seek to improve the controls' auditability and help organizations more efficiently achieve compliance (with either internal or external third-party cloud security audits).

The auditing guidelines are not exhaustive or prescriptive by nature. Rather, they represent a generic guide through recommendations for assessment. Auditors must customize the descriptions, procedures, risks, controls, and documentation. These elements must conform to organizational-specific audit work programs and service(s) in the scope of the assessment to address the specific audit objectives.

The CSA auditing guidelines are slated for official release in December 2021.

Metrics

A metric is a standard for measurement that defines the rules for performing the measurement and understanding the results of a measurement (ISO/IEC 19086-1). In the context of cloud computing, there is a growing interest in defining metrics that can be used to evaluate the security of an information system, potentially in real-time.

Security metrics can be used for several purposes:

- *Measuring the effectiveness of an information system*. Using metrics allows organisations to assign qualitative or quantitative values to various attributes of an information system. By carefully selecting attributes that reflect the implementation of security control, metrics can be used to measure the effectiveness of these controls.
- *Increasing the maturity of an organization governance and risk management approach*. Organizations that select and implement security metrics are required to adopt the necessary tools to notably categorize their assets and measure associated security attributes. This work is not trivial, so the ability to conduct it illustrates that the organisation has reached a certain level of maturity in information security management.
- *Increasing transparency and accountability, enabling continuous compliance*. Organizations that adopt metrics can provide visibility to the relevant stakeholders into their security and privacy practices and better explain and justify their Service Level Agreement. Metrics could even be used as a foundation for a continuous certification scheme that goes beyond what traditional point-in-time certifications offer today.

The CCM metrics catalog is the product of the work conducted by industry experts in the CSA Continuous Audit Metrics Working Group. The catalog does not aim to be exhaustive or complete; and the initial release aims to offer support for those organizations seeking for a more systematic evaluation of the efficiency and effectiveness of the CCM controls implementation.

The proposed metrics aim to support internal CSP governance, risk, and compliance (GRC) activities and provide a helpful baseline for service-level agreement transparency. Additionally, these metrics might be integrated within the STAR Program in the future, providing a foundation for continuous certification.

The *CCM Implementation Guidelines* presented in this document suggest the use of metrics to ascertain the correct implementation of several controls. Moreover, CSA is leading an effort to define a catalog of cloud security metrics[3] that are mapped to the *Cloud Control Matrix version 4 (CCM v4.0)*.

[3] https://docs.google.com/document/d/14J0qV3N5LY2IeuZ2aZLdSst-mMbegdb-fUMLmC4Kclk/edit, accessed on 24/8/21.

1.1.5 CCM Columns

The CCM V4 spreadsheet, as of the date of publication of this document, includes six tabs:

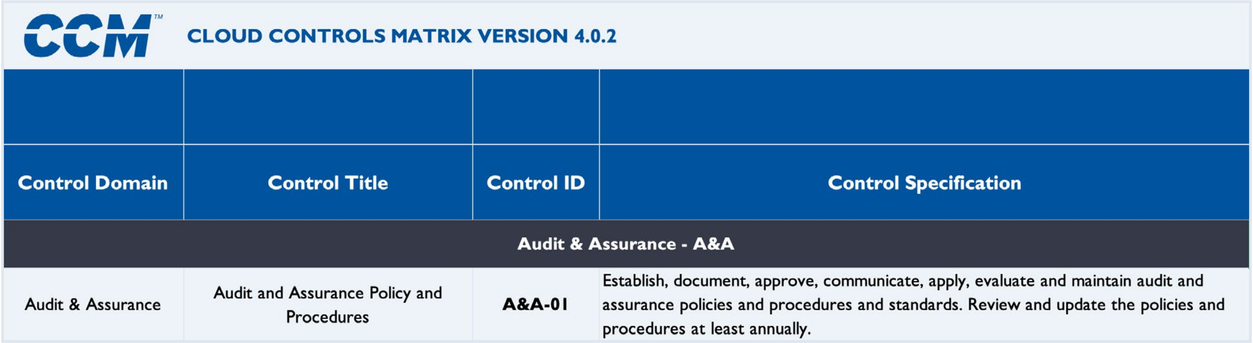
> - Introduction.
> - CCM Controls.
> - Implementation Guidelines.
> - CCM Scope Applicability (Mappings).
> - Consensus Assessments Initiative Questionnaire (CAIQ).
> - Acknowledgments.

a. CCM Controls

This is the core of the CCM V4. It includes 197 controls structured in 17 domains.

Each control is described by a:

> - Control Domain: the name of the domain each control pertains to.
> - Control Title: The control's title.
> - Control ID: The control's identifier.
> - Control Specification: The control's requirement(s) description.



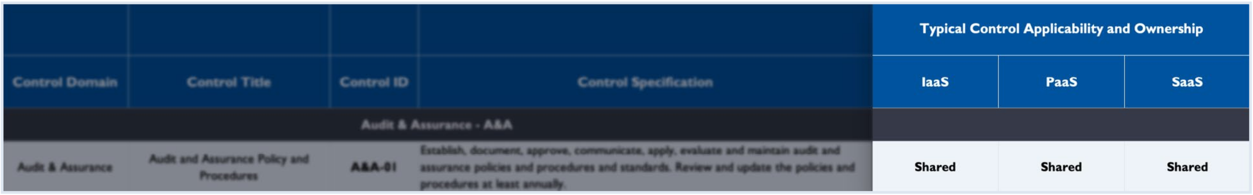
CLOUD CONTROLS MATRIX VERSION 4.0.2

Control Domain	Control Title	Control ID	Control Specification
Audit & Assurance - A&A			
Audit & Assurance	Audit and Assurance Policy and Procedures	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.

Figure 2: Snapshot of CCMv4 'Audit & Assurance' domain's control specification.

In addition, this tab includes the following sections (groups of columns):

> - **The Typical Control Applicability and Ownership matrix.** These columns describe the standard SSRM control ownership and applicability for all controls for the three main cloud delivery models: IaaS, PaaS, and SaaS. Common SSRM ownership designations allocate responsibilities typical for implementing a given CCM control between a CSP and a CSC. The matrix indicates whether a control's responsibility is usually "CSP-Owned", "CSC-Owned", or "Shared" between the CSP and CSC (as required by control STA-04). The SSRM control ownership varies from service to service, depending on the cloud service model and the implementation of each specific cloud service. Accordingly, CSPs should provide detailed, service-specific SSRM guidance to facilitate secure customer service implementations. Version No. 4 of the CAIQ has been enhanced to provide a framework and forum for CSPs to document and share this crucial information with current and prospective customers (per CCM controls STA-01 - STA-06).



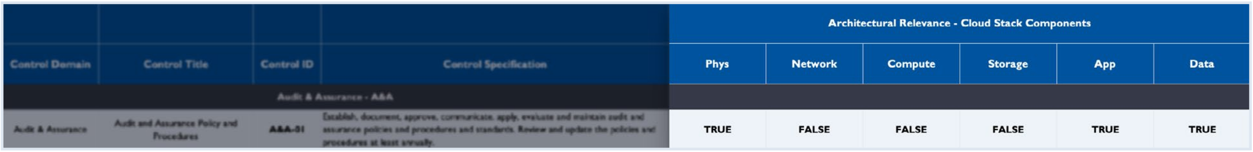
				Typical Control Applicability and Ownership		
Control Domain	Control Title	Control ID	Control Specification	IaaS	PaaS	SaaS
Audit & Assurance - A&A						
Audit & Assurance	Audit and Assurance Policy and Procedures	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	Shared	Shared	Shared

Figure 3: Snapshot of CCMv4 'Audit & Assurance' domain and control applicability per IaaS-PaaS-SaaS.

- **The Architectural Relevance and Cloud Stack Components matrix.** These columns indicate the architectural relevance of each CCM control—per cloud stack component—from the perspective of the *CSA Cloud Reference Model*. The section focuses on the following components: "Physical", "Network", "Compute", "Storage", "App (Application)", and "Data."

  The relevance box associated with each component is marked as "TRUE" if the control is relevant to a component and "FALSE" if not.

  The architectural relevance represents a high-level simplification, and CCM users should revise those attributions depending on their specific cloud environments and technologies used.

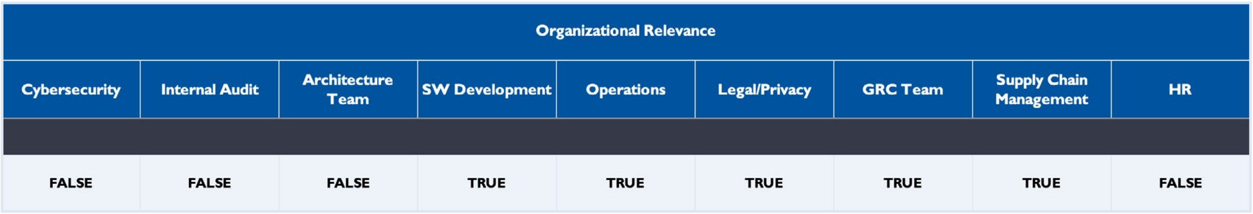


				Architectural Relevance - Cloud Stack Components					
Control Domain	Control Title	Control ID	Control Specification	Phys	Network	Compute	Storage	App	Data
Audit & Assurance - A&A									
Audit & Assurance	Audit and Assurance Policy and Procedures	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	TRUE	FALSE	FALSE	FALSE	TRUE	TRUE

Figure 4: Snapshot of CCMv4 'Audit & Assurance' domain and control architectural relevance

- **The Organizational Relevance matrix.** This group of columns indicates the relevance between each CCM control and its implementation by the respective cloud relevant functions within an organization. The functions included are: "Cybersecurity", "Internal Audit", "Architecture Team", "SW (Software) Development Team", "Operations", "Legal/ Privacy", "GRC (Governance/Risk/Control) Team", "Supply Chain Management", and "HR (Human Resources)."

  The "relevance box" associated with each component is marked as "TRUE" if the control is relevant to a component and "FALSE" if not.



Organizational Relevance								
Cybersecurity	Internal Audit	Architecture Team	SW Development	Operations	Legal/Privacy	GRC Team	Supply Chain Management	HR
FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE

Figure 5: Snapshot of CCMv4 controls organizational relevance columns.

b. Implementation Guidelines

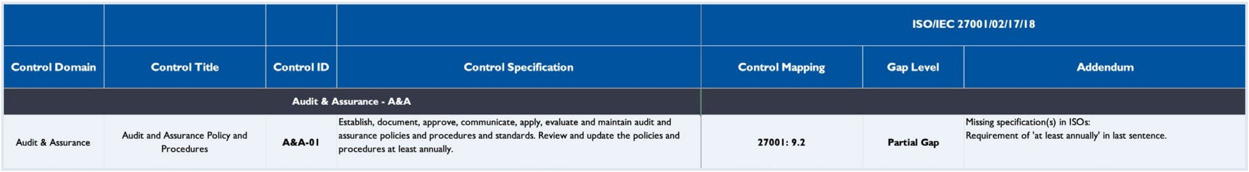
This tab includes the implementation guidelines which provide suggestions, recommendations and examples of how to implement the CCM controls.

c. CCM Scope Applicability (Mappings)

This tab includes the mappings between CCM V4 and numerous standards (ISO 27001/2/17/18) and best practices (CIS v8.0) control sets relevant to cloud computing.

For each standard, CCM V4 is mapped to include the following three columns:

> - Control Mapping. The indication of which control(s) in the target standard (e.g., ISO27001) corresponds to the CCM control.
> - Gap Level. The gap level a control (or controls) in the target standard has when compared with the CCM control. The gap levels used are:
>   - No Gap: In case of full correspondence.
>   - Partial Gap: If the control(s) in the target standard does not fully satisfy the corresponding CCM control's requirements.
>   - Full Gap: If there is no control in the target standard to fulfill the corresponding CCM control's requirements.
> - Addendum. The suggested compensating control organizations could implement to cover the gap between the control in the target standard and the corresponding CCM control.



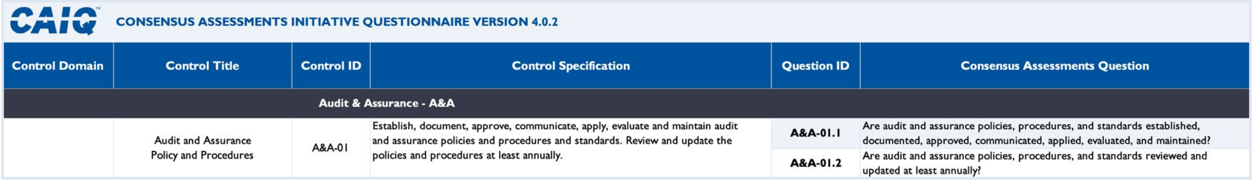
				ISO/IEC 27001/02/17/18		
Control Domain	Control Title	Control ID	Control Specification	Control Mapping	Gap Level	Addendum
Audit & Assurance - A&A						
Audit & Assurance	Audit and Assurance Policy and Procedures	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	27001: 9.2	Partial Gap	Missing specification(s) in ISOs: Requirement of 'at least annually' in last sentence.

Figure 6: Snapshot of a CCMv4 control mapping to ISO standards illustrating the relevant columns.

d. Consensus Assessments Initiative Questionnaire (CAIQ)

This tab includes the questionnaire associated with CCM controls, commonly known as CAIQ. The CAIQ consists of 261 questions structured in the 17 domains of the CCM. Each question is described in the following manner:

> - Question ID: the question's identifier.
> - Question: the description of the question.



CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.2

Control Domain	Control Title	Control ID	Control Specification	Question ID	Consensus Assessments Question
Audit & Assurance - A&A					
	Audit and Assurance Policy and Procedures	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?
				A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?

Figure 7: Snapshot of a CCMv4 control and corresponding CAIQv4 assessment questions.

e. Acknowledgments

This tab acknowledges the volunteers who contributed to *CCM v4.0*'s development.

1.1.6 CCM Target audience

The CCM was created to help cloud customers, cloud service providers, and auditors and consultants.

Cloud customers: The CCM allows cloud customers to build a detailed list of requirements and controls they want their CSP to implement as part of their overall third-party risk management and procurement program. It also helps normalize security expectations, provides a cloud taxonomy, and improves understanding of the security measures implemented in the cloud supply chain. Because the actors within a cloud supply chain are independent organizations, each has its own way of expressing and representing its security requirements. Each actor might use a different vocabulary or apply policies that differ from others. It is vital to define a taxonomy—or a set of agreed-upon terms—to standardize the various languages in such a context. That is why CCM plays a critical role and why more overarching frameworks are necessary to simplify interoperability.

Cloud customers can use the CCM controls to do the following:

> - Map organizational, operational and legal requirements to control objectives.
> - Build an operational cloud risk management program.
> - Build a third-party risk management program.
> - Build an internal and external cloud audit plan.

When organizations build cloud risk management programs, the CCM can help measure, assess, and monitor risks associated with CSPs or particular services. The CCM allows customers to understand the gaps between their own security needs and CSP security capabilities. Customers can then use the CCM to identify compensating controls to close gaps between organizational needs and provider offerings.

When building a third-party risk management program, the CCM allows customers to assess a cloud service during the overall service lifecycle. For example, it can be used to evaluate the service before its acquisition, compare offerings from different CSPs, and monitor alignment with internal requirements during the service execution.

When organizations build cloud risk management programs, the CCM can help measure, assess, and monitor risks associated with CSPs or particular services. The CCM allows customers to understand the gaps between their own security needs and CSP security capabilities. Customers can then use the CCM to identify compensating controls to close gaps between organizational needs and provider offerings.

When building a third-party risk management program, the CCM allows customers to assess a cloud service during the overall service lifecycle. For example, it can be used to evaluate the service before its acquisition, compare offerings from different CSPs, and monitor alignment with internal requirements during the service execution.

Cloud service providers (CSPs): The CCM serves multiple purposes for CSPs. First and foremost, it offers cloud-specific, industry-validated best practices CSPs can follow to guide internal security programs. In addition, it provides standardized language CSPs can use to communicate with customers and business partners.

The CCM mapping feature allows CSPs to demonstrate alignment with other recognized international, national, and industry frameworks and compliance with the *CSA STAR* program—which relies on the CCM as one of its foundational frameworks (see Chapter 9 for more details). In addition, the *CSA STAR* program enables organizational transparency and reduces the number of security questionnaires they must provide for customers. These benefits can be realized when organizations complete the CCM extended question self-assessment (the CAIQ) and submit it to the *CSA STAR Registry*—a free, publicly accessible registry documenting CSP-provided security controls.

CSPs can use CCM controls to:

- Build an internal security program based on mature and industry-recognized best practices.
- Facilitate communication and interoperability with business partners and customers.
- Demonstrate commitment to security and transparency about security postures.
- Streamline compliance by leveraging mapping between CCM controls and the controls in other international, national, and industry frameworks.
- Reduce time and effort spent addressing customer questionnaires.
- Demonstrate commitment to security to regulators by adhering to the CSA STAR program (see Chapter 9).
- Build a cloud internal and external audit plan.

Auditors and Consultants: Auditors and consultants can use the CCM to guide clients in designing, planning, and executing activities dedicated to cloud customers and CSPs.

Consultants and auditors can leverage CSA resources to:

- Help organizations assess their cloud maturity.
- Establish controls aligned with the CCM.
- Compare organizations with market peers through benchmarking.

1.1.7 CCM Compliance Documentation

To provide an organizational record and prepare for compliance audits, CCM users should focus on documenting compliance with the CCM V4 controls that they are responsible for in whole or in part under the Shared Security Responsibility Model (SSRM) that always exists between the Cloud Service Provider (CSP) and their Cloud Service Customers (CSC).

CCM users should start by developing or assembling high level CCM compliance and SSRM control applicability and implementation summary documentation as appropriate for their cloud role, e.g. as a Cloud Service Provider (CSP) or Cloud Service Customer (CSC).

- For CSPs a fully completed Consensus Assessment Initiative Questionnaire v4 (CAIQv4)[4] will generally be a good starting point. Completed CAIQ questionnaires can be published in the CSA's Security, Trust, Assurance, and Risk (STAR) Registry[5] and/or maintained internally by the CSP using the Excel questionnaire template. Fully completed questionnaires will include the optional CSP Implementation Description and CSC Responsibilities (Optional/Recommended) columns.
- For CSCs, the CSA does not have a specific questionnaire or compliance documentation template. However, organizations should have (or develop) some form of CCM compliance documentation to incorporate SSRM customer security responsibilities (as delineated by the CSP per CCM STA control requirements). For example, some CSCs will tailor a version of the CCM controls spreadsheet and/or a copy of their CSP's CAIQ questionnaire to incorporate customer security control response information (e.g., adding additional columns to standard artifacts). Alternatively, CSCs may utilize an internal GRC application to assemble similar details. This compiled data can generate appropriate reports for compliance review and audit purposes.

In addition to high-level SSRM control implementation summary information, more detailed supporting documentation (e.g., technical designs, process and procedure documentation, and evidence of compliance) should be developed for specific control domains and individual controls (as appropriate). This documentation should be based on the detailed guidelines underscored in this document and an organization's security auditor or assessor requirements.

[4] https://e.cloudsecurityalliance.org/e/908632/security-questionnaire-caiq-v4/5k7gm/16076104?h=MnauEgRXjmy71XyORAtJaJr5idpEVy7uzLeD2hYNSrs, accessed on 25/8/21.
[5] https://e.cloudsecurityalliance.org/e/908632/star-registry-/5k7gp/16076104?h=MnauEgRXjmy71XyORAtJaJr5idpEVy7uzLeD2hYNSrs, accessed on 25/8/21.

1.2 CCM Implementation Guidelines

This section introduces the purpose and scope of the implementation guidelines.

1.2.1 Purpose and Scope

The document contains implementation guidelines tailored to the control specifications for each of *CCM v4.0.*'s 17 cloud security domains. The guidelines represent a new element for *CCM v4.0* that did not exist in *CCM v3.0.1*.

The implementation guidelines aim to support organizations and provide guidance for implementing every *CCM v4.0* security and privacy control specification. Currently, the guidelines are technology/ vendor agnostic, meaning they are not tailored to a specific technology but defined at the same high level as each CCM control specification. However, they include more details regarding best practices for implementing such controls, as recommended by cloud organizations.

The implementation guidelines are not exhaustive nor prescriptive. Instead, they represent a generic guide highlighting recommendations. Therefore, security practitioners must customize the descriptions, procedures, risks, controls, and documentation and tailor these to their risk management programs and cloud service(s) (in the scope of the risk assessment) to address specific security objectives and implementations.

1.2.2 Target Audience

The intended audiences of this document include cloud consumers, cloud providers, cloud auditors, expert users willing to assist new CCM adopters, and neophytes willing to learn the best approaches to CCM control implementation.

The document assumes that readers have familiarity and knowledge of *CCM 4.0*, CAIQ, and *CSA Security Guidance for Critical Areas of Focus in Cloud Computing*.

Audience members are encouraged to follow industry-standard practices and innovate on their implementation journeys using this guidance.

1.3 Versioning

The final version of this is v1.0.

2. Implementation Guidelines

2.1 Audit and Assurance (A&A)

Control Title:	**Control ID:**	**Control Specification:**
Audit and Assurance Policy and Procedures	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.

Implementation Guidelines:
Both the cloud service provider (CSP) and customer (CSC), should develop a "customized integrated framework", of audit and assurance policies and procedures to incorporate/ demonstrate compliance to leading industry standards and own business requirements, and finally to provide appropriate coverage of controls to assess the respective cloud environment and corresponding services.

Audit and assurance policies and procedures should include, but not limited to:

a. Audit and assurance functions, indicating purposes, responsibility, authority, and accountability, ensuring organizational independence, due professional care, audit objectivity, and proficiency.
b. Audit and assurance plans
c. Audit development policies and procedures, to determine criteria and assertions against which the subject matter will be assessed, quality assurance and supervision, sufficient and appropriate evidence, in accordance with commonly accepted frameworks and audit best practices
d. Audit reporting to communicate the results and findings in the audit.
e. Follow-up Activities to monitor the progress of the implementation of audit findings.

Control Title:	**Control ID:**	**Control Specification:**
Independent Assessments	A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.

Implementation Guidelines:
Independent audit and assurance should be free from conflict of interest and undue influence in all matters related to audit and assurance engagements.

The frequency of audit and assurance evaluations should comply with applicable standards, regulations, legal/contractual obligations, and statutory requirements.

The audit and assurance process should assess all applicable CCM domains.

<table>
<tr><td><b>Control Title:</b>
Risk Based Planning Assessment</td><td><b>Control ID:</b>
A&A-03</td><td><b>Control Specification:</b>
Perform independent audit and assurance assessments according to risk-based plans and policies.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Independent audit and assurance assessments should be based on risk-based plans that define audit objectives, scope, resources, timeline and deliverables, documentation and reporting requirements, use of relevant technology and data analysis techniques, costs, communication, and escalation protocols.
Both CSPs and CSCs may take guidance from industry standards like the Committee of Sponsoring Organizations (COSO) or the International Organization for Standardization (ISO) 31000 for risk management and risk-based planning.</td></tr>
<tr><td><b>Control Title:</b>
Requirements Compliance</td><td><b>Control ID:</b>
A&A-04</td><td><b>Control Specification:</b>
Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Verify compliance with all relevant standards applicable to the audit, such as:
a. Country regulations
b. Standards and certifications
c. Industry sector regulations
d. International applicable regulations such as those regarding privacy and cybersecurity</td></tr>
<tr><td><b>Control Title:</b>
Audit Management Process</td><td><b>Control ID:</b>
A&A-05</td><td><b>Control Specification:</b>
Define and implement an Audit Management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Audit management process security should include:
a. Secure role-based access and authorization and secure communication and storage.
b. Controls to protect audit data confidentiality, integrity, and availability.
c. Periodic reporting, including issues and remediation plans per organizational requirements.</td></tr>
</table>

Control Title:	Control ID:	Control Specification:
Remediation	A&A-06	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and report remediation status to relevant stakeholders.

Implementation Guidelines:
The organization should document a well-defined remediation plan that includes:

a. Remediation tasks and their risk levels.
b. Proactive, continuous monitoring (where applicable) to identify anomalies using a risk-based approach.
c. Specific task owners.
d. Milestones with due dates.
e. Deliverables and current status.

The organization should document, communicate, and enforce change management best practices to address audit findings based on a risk-based approach.

2.2 Application and Interface Security (AIS)

<table>
<tr><td><b>Control Title:</b>
Application and Interface Security Policy and Procedures</td><td><b>Control ID:</b>
AIS-01</td><td><b>Control Specification:</b>
Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for application security to provide guidance to the appropriate planning, delivery and support of the organization’s application security capabilities. Review and update the policies and procedures at least annually.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
The policy should:
a. Include defined roles and responsibilities supported by regular workforce training.
b. Align with organizational purpose and strategy.
c. Provide a framework for setting application security baselines (e.g., NIST, ISO, OWASP, and CIS benchmarks).
d. Guide the development of application security controls.
e. Include a commitment to satisfy applicable requirements and continual improvement.
f. Cover all relevant applications regardless of whether they are developed in-house or via one’s supply chain.
g. Promote the use of an established software development lifecycle (SDLC) in software development, including code review, secure coding training, testing (functional, regression, security, etc.), vulnerability testing, and change management.
h. Ensure vulnerability processes are followed with regular patching, scanning, and remediation before production deployment.
i. Be reviewed by management periodically or after significant changes.</td></tr>
<tr><td><b>Control Title:</b>
Application Security Baseline Requirements</td><td><b>Control ID:</b>
AIS-02</td><td><b>Control Specification:</b>
Establish, document and maintain baseline requirements for securing different applications.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
The baseline requirements should include, but are not limited to:
a. alignment with established application security policies and industry standards,
b. risk assessment (business, technical risks) to evaluate applications security alignment with the baseline and perform regular auditing (scanning/monitoring) to ensure such alignment is achieved,
c. a consideration for unique requirements and characteristics of each application,
d. a consideration for lessons learned from the issues/incidents to feedback into the security policy,
e. incorporation of guidelines on how to meet and/or stay aligned with the established baseline,
f. review by management on a periodic basis.</td></tr>
</table>

Control Title: Application Security Metrics	**Control ID:** AIS-03	**Control Specification:** Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations.

Implementation Guidelines:
Actionable metrics should be defined with consideration to business goals, the criticality of service, security requirements, and compliance obligations.

Example technical metrics include:

- Count or percentage of vulnerabilities by weakness.
- Count or percentage of vulnerabilities by severity.
- Count or percentage of vulnerabilities by detection source (design review, code review, SAST, DAST, penetration test, VDP, or bug bounty).
- Count or percentage of vulnerabilities by environment detected (pre-production vs. production).
- Average time to resolution.
- Count exceeding remediation service level objectives (SLOs).

Example operational metrics include:

- Count or percentage of applications using automated security testing by test type (SAST, DAST, SCA).
- Count or percentage of applications have completed penetration testing in the last “n” months.
- Count or percentage of development teams or individuals who have completed application security training in the last “n” months.
- Count of proactive engagements by development and business teams.
- Results from surveys delivered to application security customers, such as business and development teams.

Reporting:
Reporting should be designed with various users in mind. For example, security professionals, engineering teams, business stakeholders, and executives will often have different interests requiring specialized views, filtering, and delivery mechanisms.

a. The collection, visualization, and distribution of reporting data should be automated.
b. Data may be further analyzed using application criticality, business units, platforms, languages, and other factors relevant to the viewer.
c. Compare actual metrics to standards to evaluate performance.
d. Enable comparisons over time to identify trends.
e. Enable correlations, such as relating a reduction in vulnerabilities of a specific type after new tools or training.

Control Title: Secure Application Design and Development	**Control ID:** AIS-04	**Control Specification:** Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization.

Implementation Guidelines:
Defining security requirements should be the first step in the secure software development lifecycle (SSDLC) process to ensure that security is integrated into the product from its creation. All security requirement aspects should be considered from functional, physical, and business requirements perspectives. In addition, security requirements should derive from security objectives and/or organizational goals and regulatory requirements. Industry standards should be applied at project inception and every stage of the SSDLC process—including requirements analysis, design, coding, testing, deployment, and end-of-life (EoL) processes.

To successfully enable SSDLC security, roles and expectations should be clearly defined and published, and an inventory of applications and their metadata should exist in an easily accessible format.

Appropriate security practice examples for the common stages of an SSDLC are provided below to include the following categories: training, requirements, design, development, testing, and release and response.

A. Training:

  a. Role-based secure development training should be required at multiple stages of employment (or other contractual relationships), including on-boarding and role changes.
  b. Refresher training should be delivered throughout one's career, regardless of position or movement in their organization.
  c. Targeted, specialty training should be created and made available as the organization adopts new technologies.
  d. Progressively advanced training should be made available to relevant employees (and contractors whenever applicable) as they transition through technical roles and/or champion program participants.

B. Requirements:

  a. Generic and specialized security requirements should be defined, published, organized, and easily accessible to all organizational roles.
  b. Every application, during each iteration, should review existing requirements and research if additional requirements are necessary. It is beneficial for the engineering teams to consult with a security professional at this time.

C. Design:

  a. Security-focused design reviews are conducted.
  b. Threat models are developed or modified.
  c. The design of new or enhanced security controls, required by the application design, is developed.

D. Development:

a. Develop, as per design specifications.
b. Abuse cases are used to develop a security-focused unit and integration tests during development.
c. Secure coding practices are implemented and enforced through automation and manual peer code reviews.

E. Security Testing:

a. Manual and automated test plans are developed and executed with abuse cases in mind
b. Automation may include one or more of SCA, SAST, DAST, IAST, fuzzing, credential scans, etc.
c. Penetration testing may be executed during this stage, based on need.
d. Crowdsourced testing or private bug bounty programs may be implemented.

F. Release:

a. Change control is instituted, including gating and documenting releases to ensure requirements and compliance objectives are met.

G. Response:

a. Monitoring and alerting are in place to identify security issues and enable response activities.
b. A response plan exists and can be easily executed when a security issue is discovered.
c. A process is established for monitoring external sources for vulnerability disclosures and responding when applicable.

Control Title:	**Control ID:**	**Control Specification:**
Automated Application Security Testing	AIS-05	Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while enabling organizational speed of delivery goals. Automate when applicable and possible.

Implementation Guidelines:

Note: The implementation guidelines of AIS-05 should be interpreted as further guidance in addition to what is specified in AIS-03 and AIS-04.

Automation of security testing should be implemented to reduce risks and errors and enable the scaling of security practices to meet organizational demands. Multiple test types and integration points will likely be needed to provide the appropriate level of assurance throughout the SDLC. Criteria should be developed for use when assessing the automation required by an application, as not all systems will benefit equally.

Strategy:

a. Identify the goals and requirements of the automation implementation.

Example Goals:

- Security requirements are not relaxed to improve speed.
- All developers can leverage tools to detect security weaknesses while developing software.
- All third-party libraries are scanned for known vulnerabilities.
- All authentication and authorization functions "pass" abuse case unit tests before deployment.
- All website security headers are verified to meet security requirements when deployed.

Example Requirements:

- Applicable programming languages should be supported by static analysis tools.
- Python and C# should be supported by select static analysis tools.
- Automation should not require infrastructure support.
- All automation tools should offer an application programming interface (API).
- All website security headers are verified to meet security requirements when deployed.

Strategy can also include, but is not limited to:

a. Security testing for unintentional side effects and behaviors that are not specified in the test plan or design.
b. Security testing for incident response procedures, such as simulating breaches.
c. Determining which portfolio applications warrant investment in automation. Prioritize the adoption order based on criticality.

Considerations:

a. Security requirements
b. Risk, business, and compliance requirements
c. Development methodology
d. Lifecycle
e. Metrics establishment

Example:

- Count or percentage of (test type) adoption among applications requiring (test type) SAST, DAST, SCA, etc.
- Count or percentage of false positives produced by test automation.
- Count or percentage of execution-time SLA breaches by test automation.
- Soft measures, including satisfaction levels with usability.
- Change in the number of security weaknesses discovered after release.
- Percentage coverage of automated test cases for exposed APIs and SDK functions by service (i.e., the total number of automated test cases for APIs/SDK functions; the total number of APIs/SDK by service).
- Evaluate test types to determine which is best suited for different categories of applications based on the attributes of those in the prioritized inventory.

Considerations:

- Development and security team sizes
- Platform and operating systems
- Maturity of build automation
- Language support

Execution:

a. Avoid approaches that cause unreasonable delays to builds and deployments or require significant process modification or resource commitment from development teams.
b. Seek to adopt automation at multiple SDLC integration points
   Example integration points:
   1. A plugin in the developer's integrated development environment (IDE).
   2. Abuse case unit and integration tests—created and maintained by developers—and executed during development and build cycles.
   3. Static application security testing or SCA scans executed during automated builds.
   4. Dynamic application security testing scans executed during automated deployment.
c. Automate patching when possible.
d. Use metrics to drive feedback loops and continuous improvement.
   1. Maintain an accurate count of license utilization.
   2. Tune automation to reduce false positives and false negatives.
   3. Analyze gaps in support and trends for response and planning.
e. Continue to leverage manual testing for scenarios not easily tested with automation.

Control Title:	**Control ID:**	**Control Specification:**
Automated Secure Application Deployment	AIS-06	Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.

Implementation Guidelines:

The strategies should include:

a. Defined security and automation requirements based on an organization's application deployment needs and standards.
b. Defined roles and responsibilities between security, application teams, and other stakeholder groups.
c. Identification and integration with existing application deployment processes.
d. Customization of secure application deployment for deployment types such as operating systems, network connections, configuration, etc.
e. Logging and monitoring of secure application deployment so that data issues can be promptly addressed by the appropriate people (incident or forensics).
f. Metrics to effectively measure deployment success.

The capabilities should be based on the organization's SSDLC and should include, for instance:

g. Defined and approved list of deployment and automation technologies.
h. Enablement for team members (e.g., developers, administrators, etc.) to dynamically address security issues when needed.

The strategies and capabilities should be reviewed periodically by senior management.

Control Title:	**Control ID:**	**Control Specification:**
Application Vulnerability Remediation	AIS-07	Define and implement a process to remediate application security vulnerabilities, automating remediation when possible.

Implementation Guidelines:

Application security remediation should adhere to the following guidelines:

a. Follow defined remediation processes, designed, tested, and implemented by security and application teams.
b. Remediate risks as early in the SDLC as possible, such as during the design or development stages.
c. Have defined roles and responsibilities, including escalation paths for application security incident response and remediation.
d. Follow a risk-based approach to address high-risk incidents that significantly impact application availability, integrity, or confidentiality.
e. Leverage automation when possible to increase remediation efficiency and accuracy.

Processes, roles, responsibilities, and documentation established for application security remediation should be reviewed periodically by management.

Example:

- GitOps-based remediation of application vulnerabilities.
- Automated remediation efficacy metric: total number of remediations of active critical/ high vulnerabilities performed through Git for the given period.
- Total number of active critical/ high vulnerabilities identified for the given period.

2.3 Business Continuity Management and Operational Resilience (BCR)

<table>
<tr><td><b>Control Title:</b>
Business Continuity Management Policy and Procedures</td><td><b>Control ID:</b>
BCR-01</td><td><b>Control Specification:</b>
Establish, document, approve, communicate, apply, evaluate and maintain business continuity management and operational resilience policies and procedures. Review and update the policies and procedures at least annually.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
The policies should include defined roles and responsibilities supported by regular workforce training.

The policies should:
a. Be appropriate to the organization’s purpose.
b. Provide a framework for setting business continuity objectives.
c. Include a commitment to satisfy applicable requirements and continual improvement.
d. Include organizational risk appetite and tolerance to facilitate appropriate planning, delivery, and support of capabilities in the event of a business disruption.
e. Take guidance from industry standards, such as ISO 22300.</td></tr>
<tr><td><b>Control Title:</b>
Risk Assessment and Impact Analysis</td><td><b>Control ID:</b>
BCR-02</td><td><b>Control Specification:</b>
Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
The business impact analysis (BIA) should incorporate the following components:
a. Identification of critical products and services with their inherent risks.
b. The likelihood and impact of each risk.
c. The organization’s risk appetite and tolerance.
d. The identification of risk dependencies.
e. The identification of appropriate and relevant countermeasures to prevent, detect, and react to the identified risks.

The impact analysis should incorporate the following elements:
f. The immediate and ongoing impacts resulting from disruptions.
g. A recovery time objective (RTO) and recovery point objective (RPO).
h. The estimated internal and external resources required for recovery and resumption.</td></tr>
</table>

Control Title:	**Control ID:**	**Control Specification:**
Business Continuity Strategy	BCR-03	Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite.

Implementation Guidelines:
Business continuity and operational resilience strategies should:

a. Be developed by both cloud service providers and cloud service consumers with consideration of acceptable limits regarding risk appetite and tolerance.
b. Cover all aspects of business continuity and resilience planning—taking inputs from assessed impact and risks—to consider activities for before, during, and after a disruption.
c. Account for the unavailability of all relevant components required to operate the business "as usual" or in a disrupted mode (in parts or total) during a disruption.
d. Cover all actions required to continue and recover prioritized activities within identified timeframes and aligned with organizational risk appetite and tolerance (including the invocation of continuity plans and crisis management capabilities).
e. Cover all activities within the defined scope to protect prioritized activities, reduce disruption likelihood, and limit cloud capability disruption through adequate resourcing.
f. Include detailed solutions and measures for each strategy.

Control Title:	**Control ID:**	**Control Specification:**
Business Continuity Planning	BCR-04	Establish, document, approve, communicate, apply, evaluate and maintain a business continuity plan based on the results of the operational resilience strategies and capabilities.

Implementation Guidelines:
All relevant business continuity plans should be developed consistently to address priorities for operational resilience, testing, maintenance, and information security requirements.

Business continuity plans should be accessible and available to those with the need-to-know and include the following elements:

a. Defined purpose and scope, aligned with relevant dependencies.
b. Assigned roles and responsibilities (i.e., review, update, and approval).
c. Defined lines of communication, roles, and responsibilities.
d. Detailed recovery procedures, manual workaround, and reference information.
e. Method for plan invocation.

The plans should be tested and reviewed at planned intervals (e.g., annually or upon significant organizational or environmental changes).

Control Title:	**Control ID:**	**Control Specification:**
Documentation	BCR-05	Develop, identify, and acquire documentation that is relevant to support the business continuity and operational resilience programs. Make the documentation available to authorized stakeholders and review periodically.

Implementation Guidelines:
The documentation should include but is not limited to:

a. Administrator and user guides
b. Database backup and replication guidelines
c. Architecture diagrams
d. Incident playbooks

Documentation availability is intended to support successful continuity of the following activities:

e. Configuring, installing, deploying changes, and operating the system and/or infrastructure.
f. Effectively using the system's security and business continuity features.
g. Using system automation and structured playbooks where available for fast incident recovery.

The documentation should be interconnected and comparable.

Control Title:	**Control ID:**	**Control Specification:**
Business Continuity Exercises	BCR-06	Exercise and test business continuity and operational resilience plans at least annually or upon significant changes.

Implementation Guidelines:
Exercise and test business continuity and operational resilience plans at least annually or upon significant changes.

Exercises and tests should include but are not limited to:

a. Processes established in the business continuity plan.
b. Alignment with business continuity policies.
c. Critical systems and equipment relevant to the business continuity plan.
d. Roles and responsibilities of the various parties involved in the exercises.
e. The use of CSP support mechanisms in CSC exercises.
f. A review and update of communication templates.
g. Lessons learned from previous events and exercises.
h. Tabletop exercises.

Depending on the level of CSP maturity, the CSP's practices may include automated chaos testing.

Control Title:	**Control ID:**	**Control Specification:**
Communication	BCR-07	Establish communication with stakeholders and participants in the course of business continuity and resilience procedures.

Implementation Guidelines:
A business continuity and resilience program should:

a. Communicate the importance of effective business continuity and the consequences of disruptions to all relevant stakeholders.
b. Communicate the business continuity and resilience policy, objectives, and plans to all relevant stakeholders.
c. Communicate the roles, responsibilities, authorities, and expected competencies to all relevant stakeholders.
d. Establish the criteria, thresholds, and indicators to demonstrate when and how business continuity-related communications should be sent, who should send them, and to whom they should be sent.
e. Establish templates for common communications during a disruption regarding the activation, operation, coordination, and communication of a business continuity response.
f. Establish the people, technology, and processes required for business continuity communications.
g. Establish a response structure that will enable timely warnings and communication to relevant stakeholders.

Clear and effective communication channels should remain available to disseminate information to participants and stakeholders, assess and relay damage, and coordinate a recovery strategy. Failed communication often results in failed business continuity efforts. Thorough planning, testing, and exercising communication procedures within the following four phases are essential to support effective business continuity and the viability of critical business operations.

Control Title:	**Control ID:**	**Control Specification:**
Backup	BCR-08	Periodically backup data stored in the cloud. Ensure the confidentiality, integrity and availability of the backup, and verify data restoration from backup for resiliency.

Implementation Guidelines:
Implementation of backups and/or other means of data preservation (e.g., replication) should follow the following guidelines.

a. The scope, frequency, and duration of cloud retention should comply with:
    1. Applicable laws
    2. Contractual agreements with the cloud customers
    3. The cloud provider’s business requirements

b. The backup approach, including the physical location of backup files, should comply with the privacy and data protection laws and regulations applicable to the data collected.
c. The data backup process should be monitored by employing technical and organizational safeguards. At a minimum, malfunctions should be examined and eliminated promptly by qualified employees to support compliance with the retention's scope, frequency, and duration.
d. Backup and restoration procedures should be periodically tested and the results documented to ensure data can be successfully restored. Tests should be designed so that the reliability of the backup media and the restoration time (RPO, RTO) can be established with sufficient certainty. Any errors and identified improvements (corrective and preventive actions) should be addressed promptly.
e. Restorations should be carried out only after they have been approved by authorized persons (according to contractual agreements with cloud customers or the internal policies of the cloud provider).
f. The cloud service provider, when appropriate, should be able to disclose the exercise results to the cloud services customer as part of the assurance of business continuity and resilience.

Additional guidance is also available in the *NIST Special Publication 800-53 (Rev. 4) CP-9 INFORMATION SYSTEM BACKUP* (latest revision).

Control Title:	**Control ID:**	**Control Specification:**
Disaster Response Plan	BCR-09	Establish, document, approve, communicate, apply, evaluate and maintain a disaster response plan to recover from natural and man-made disasters. Update the plan at least annually or upon significant changes.

Implementation Guidelines:
The response plan should include the ability to protect systems—including the physical environment when possible—from inadvertent unauthorized access during an emergency.

The response plan should include the following when describing environmental threats/natural disasters: fires, medical emergencies, tornadoes, hurricanes, flooding, earthquakes, and other natural disasters.

Civil disturbances can include disgruntled employees/contractors/customers, terrorist attacks, biological attacks, and airborne agents.

Emergency authorities can include first responders and other law enforcement entities.

Control Title:	**Control ID:**	**Control Specification:**
Response Plan Exercise	BCR-10	Exercise the disaster response plan annually or upon significant changes, including if possible local emergency authorities.

Implementation Guidelines:
The plan should be executed at regular intervals based on the organization's BIA. It should be performed as a tabletop exercise and incorporate an annual live event with local authorities (e.g., fire departments, health officials, police departments, anti-terrorist organizations, and anti-cybercrime groups).

Depending on regulatory requirements, the business, and the industry, a disaster recovery (DR) exercise might be required. For example, financial institutions may consider running live on DR for extended periods or simulate component or partial failures to test overall organizational resiliency and recovery abilities.

Control Title:	Control ID:	Control Specification:
Equipment Redundancy	BCR-11	Supplement business-critical equipment with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards.

Implementation Guidelines:
The minimum distance between mirrored or redundant physical systems should support compliance with the organization's defined continuity and availability within contractual agreements or service-level agreements (SLAs).

2.4 Change Control and Configuration Management (CCC)

<table>
<tr><td><b>Control Title:</b>
Change Management Policy and Procedures</td><td><b>Control ID:</b>
CCC-01</td><td><b>Control Specification:</b>
Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). Review and update the policies and procedures at least annually.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
A documented and approved change management policy (and associated process documentation) should:
a. Ensure that changes are tested, documented, risk assessed, and authorized in a consistent and timely manner. All changes (e.g., major, minor, and emergency and the qualifying criteria) in organization assets, applications, system software, and informational technology (IT) infrastructure (e.g., hardware, operating systems, communications equipment, and software) and associated configurations should be under the scope of the change management policy.
b. Be communicated and made accessible to all employees and interested parties involved within the change management process (e.g., service/application owners, project leaders, IT, operating systems staff, contractors, etc.).
c. Include the management of emergency changes.</td></tr>
<tr><td><b>Control Title:</b>
Quality Testing</td><td><b>Control ID:</b>
CCC-02</td><td><b>Control Specification:</b>
Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
A plan to test and review during the development process should be prepared. This plan should include (but is not limited to) relevant activities and test inputs, and expected outputs regarding various conditions that may impact the outcome. For internal organizational developments, the team that oversees development efforts initially can perform such tests. Independent acceptance testing can then be performed (both for internal and external development sources) to determine whether the system functions as intended. Testing should be proportionate to the system's relevance based on its nature.

Testing record(s) should be documented before implementing all planned changes to organization assets (including applications, systems, infrastructure, configuration, etc.), regardless of whether the assets are managed internally or externally (i.e., outsourced).</td></tr>
</table>

The record(s) should comprise a test plan, configuration baseline before the change, the test result, and the new configuration baseline.

The quality testing plan might align with relevant standards or guidelines (i.e., ITIL or ISO 20000, etc.)

Control Title:	**Control ID:**	**Control Specification:**
Change Management Technology	CCC-03	Manage the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced).

Implementation Guidelines:
The organization should:

- Collaborate with relevant internal and external parties involved in the change management process.
- Assess the impact and type of change to determine the risk of the change before it is applied.
- Adopt Change Management Technologies to manage the change management workflow.

These tools should help adequately manage the authorization process, including activity logging. In addition, real-time reporting/monitoring capabilities should be implemented to monitor change progress so that quick decisions can be made to manage the risks of unforeseen issues due to the change implementation.

Understanding how those relevant components impact the security and usability of the supply chain that supports organizational environments should be one aspect of such collaboration.

Control Title:	**Control ID:**	**Control Specification:**
Unauthorized Change Protection	CCC-04	The organization should establish procedures and implement technical measures to prevent and/or detect any unwanted/unauthorized changes (e.g., additions, removals, and updates) to organizational assets production, including applications, systems, infrastructure, configuration, etc.

Implementation Guidelines:
The organization should establish procedures and implement technical measures to prevent and/or detect any unwanted/unauthorized changes (e.g., additions, removals, and updates) to organizational assets production, including applications, systems, infrastructure, configuration, etc.

<table>
<tr><td>**Control Title:**
Change Agreements</td><td>**Control ID:**
CCC-05</td><td>**Control ID:**
Conclude provisions limiting changes directly impacting CSCs owned environments/tenants to explicitly authorized requests within service level agreements between CSPs and CSCs.</td></tr>
<tr><td colspan="3">**Implementation Guidelines:**
Processes and procedures established by both the CSP and CSC should reflect respective change management responsibilities with respect to the scope of services being provided and/or consumed. There should be acknowledgement of each party's responsibility, where applicable and it should be part of a written change management agreement between CSC and CSP. The acknowledgment should include a reference to limitations related to changes impacting CSC-owned environments/tenants.

NOTE: The CSP may need to apply changes that impact CSC-owned environments/tenants without the explicit authorization of the CSC (in case those changes would be required for the overall security of the CSP system). If those types of changes are applied, the CSC should be consulted promptly.</td></tr>
<tr><td>**Control Title:**
Change Management Baseline</td><td>**Control ID:**
CCC-06</td><td>**Control ID:**
Establish change management baselines for all relevant authorized changes on organization assets.</td></tr>
<tr><td colspan="3">**Implementation Guidelines:**
A change management baseline reflects the minimum policies, procedures and technical measures established to achieve organizational objectives, and requirements (i.e., CCC-02 implementation guidelines).</td></tr>
<tr><td>**Control Title:**
Detection of Baseline Deviation</td><td>**Control ID:**
CCC-07</td><td>**Control ID:**
Implement detection measures with proactive notification in case of changes deviating from the established baseline.</td></tr>
<tr><td colspan="3">**Implementation Guidelines:**
The organization should establish a policy and procedures to detect deviations from the established control baseline. When a deviation is detected, the organization should follow the incidence management policies and procedures defined in SEF-01.</td></tr>
<tr><td>**Control Title:**
Exception Management</td><td>**Control ID:**
CCC-08</td><td>**Control ID:**
Implement a procedure for the management of exceptions, including emergencies, in the change and configuration process. Align the procedure with the requirements of GRC-04: Policy Exception Process.</td></tr>
</table>

Implementation Guidelines:
The procedure for exceptions' management should include, but is not limited to:

a. Change management baselines
b. Unauthorized assets
c. Evidence collection and management

Control Title: Change Restoration	**Control ID:** CCC-09	**Control ID:** Define and implement a process to proactively roll back changes to a previously known good state in case of errors or security concerns.

Implementation Guidelines:
Rollback procedures should be created and tested with each change request.

2.5 Cryptography, Encryption and Key Management (CEK)

Control Title: Encryption and Key Management Policy and Procedures	**Control ID:** CEK-01	**Control Specification:** Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Cryptography, Encryption and Key Management. Review and update the policies and procedures at least annually.

Implementation Guidelines:
Policies and procedures on the use, protection, and lifetime of cryptographic keys should be developed and implemented through their full lifecycle.

Policies and procedures include but are not limited to the following considerations:
A. Policies and procedures relating to organization/management.

a. Roles and responsibilities (See GRM for general considerations)
b. Data protection (DSP domain for general considerations)
    1. Data encryption
    2. Algorithm
c. Change management (See CCC domain for general considerations)
    1. Cost-Benefit analysis
d. Risk management (See BCR/GRC domains for general considerations)
e. Monitoring and reporting (see LOG and monitoring domain for general considerations)
f. Transaction/activity logging (see LOG and monitoring domain for general considerations)
g. Incident handling (see SEF domain for general considerations)
h. Audit (See A&A domain for general considerations)

B. Policies and procedures relating to key management.

a. Key generation
b. Key distribution
c. Key rotation
d. Key revocation
e. Key destruction
f. Key activation
g. Key suspension
h. Key deactivation
i. Key archival
j. Key compromise
k. Key recovery
l. Key inventory management
m. Key purposes
n. Key access

Control Title:	**Control ID:**	**Control Specification:**
CEK Roles and Responsibilities	CEK-02	Define and implement cryptographic, encryption and key management roles and responsibilities.

Implementation Guidelines:

Below are some examples of possible roles and responsibilities:

a. Keys managers should not be able to access protected data or the cryptographic engine.
b. Separation of duties should include two or more individuals control a single process.
c. Split Knowledge requires no one person knows the complete value of an encryption key.
d. No one person should know the entire passphrase used to create encryption keys.
e. Restrict access rights to the least resources required (least privilege).
f. A policy authority is responsible for all operational cryptographic key management system (CKMS) roles and reports to the executive IT.

Roles and responsibilities should be defined and followed:

a. Generation or acquisition of key information .
b. Secure distribution of private and secret keys,and the metadata.
c. Establishment of cryptoperiods.
d. Key and certificate inventory management.
e. Revocation of compromised keys and the establishment of replacement keys and/or certificates.
f. Management of the storage and recovery of operational and backed-up key information.
g. Storage and recovery of archived key information.
h. Checking the integrity of stored key information before using it.
i. Destruction of private or secret keys that are no longer required.

Control Title:	**Control ID:**	**Control Specification:**
Data Encryption	CEK-03	Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards.

Implementation Guidelines:

Data protection/data encryption is the process of changing plaintext into ciphertext using a cryptographic algorithm and key.

a. Organizations should be able to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields).
b. Data at rest involves databases, end-user workstations, and file servers.
c. Data in transit involves system interfaces, public networks, and electronic messaging.
d. Cryptography provides data protection: confidentiality, integrity, availability, and source authentication.
e. Cryptographic key management system security policies rules need to protect the confidentiality, integrity, availability, and source authentication of all keys, algorithms, and metadata.
f. Key management technology and processes should be NIST FIPS validated and/or National Security Agency (NSA)-approved by other relevant international standardization bodies.
g. Approved algorithms and key sizes should reside in the CKMS.
h. Quantum-resistant encryption is developing quickly, and it is recommended that this technology is closely monitored so the organization is not exposed.

Control Title:	**Control ID:**	**Control Specification:**
Encryption Algorithm	CEK-04	Use encryption algorithms that are appropriate for data protection, considering the classification of data, associated risks, and usability of the encryption technology.

Implementation Guidelines:

A risk-based approach to encryption algorithms adoption should consider, but not be limited to:

a. Cryptographic key management system algorithms should not exceed the anticipated lifetime of the CKMS and the information it protects.
b. Cryptographic key management system security policies should protect the confidentiality, integrity, availability, and source authentication of all keys, algorithms, and metadata.
c. The (CKMS) should include, but is not limited to:
    1. Approved algorithms
    2. Hardware security modules (HSMs)
    3. Key sizes
d. The adoption of the appropriate key size and algorithm types should be done based on cost-benefit analysis and the level of risk to data (please see the reference to quantum-resistant encryption in CEK-03).

<table>
<tr><td><b>Control Title:</b>
Encryption Change Management</td><td><b>Control ID:</b>
CEK-05</td><td><b>Control Specification:</b>
Establish a standard change management procedure, to accommodate changes from internal and external sources, for review, approval, implementation and communication of cryptographic, encryption and key management technology changes.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Key change management is the process of managing all changes to key management governance, organization, infrastructure, and activities.
a. Changes to the key management system and its policies and procedures should be analyzed and approved before implementation.
b. Changes should be documented to show the reasoning behind the changes and include a path to rollback to the previous status.
c. If unauthorized changes are made to the software, the software should be recovered.
d. There should be security audits after every significant change to the key management system.
e. All audit results should be reported to the system authority.</td></tr>
<tr><td><b>Control Title:</b>
Encryption Change Cost Benefit Analysis</td><td><b>Control ID:</b>
CEK-06</td><td><b>Control Specification:</b>
Manage and adopt changes to cryptography-, encryption-, and key management-related systems (including policies and procedures) that fully account for downstream effects of proposed changes, including residual risk, cost, and benefits analysis.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Encryption change cost-benefit analysis is the process of comparing the benefit of encryption changes to its cost.
a. Key change management cost-benefit analysis/return on investment (ROI) should be calculated for all key management-related changes.
b. Every analysis should fully account for downstream effects of proposed changes, including residual risks.
c. Every analysis should be reviewed and approved.
d. Six months after a change, compare the anticipated ROI to the actual ROI.
e. Significant deviation from the planned ROI should be audited.
f. Report all audit results to the system authority.</td></tr>
<tr><td><b>Control Title:</b>
Encryption Risk Management</td><td><b>Control ID:</b>
CEK-07</td><td><b>Control Specification:</b>
Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.</td></tr>
</table>

Implementation Guidelines:
Key risk management is the process of managing the risks to key management governance, organization, infrastructure, and activities.

a. Assess the risks of unauthorized disclosure, modification, destruction, or information loss.
b. Cryptoperiod selections should consider the risk and consequences of information exposure.
c. Evaluate the tradeoffs of manual versus automated key distribution.
d. Reduce compromised key risks by (1) not using such keys for new encryption activities and (2) only using keys to decrypt material previously decrypted under this key.
e. Adjust the audit scope and frequency to align with the risk assessment.
f. Apply algorithm strength in proportion to the risk of information exposure.
g. Assess risks to operational continuity versus the risks of key material data exposure when considering key recovery.

Control Title:	**Control ID:**	**Control Specification:**
CSC Key Management Capability	CEK-08	CSPs must provide the capability for CSCs to manage their own data encryption keys.

Implementation Guidelines:
Key management capability is the process of CSPs providing CSCs the capability to manage CSC-owned or generated encryption keys.

a. The CSC and CSP should agree on the definition and scope of CSC-managed keys and document this (shared responsibility) in the SLA, applicable contracts, policies, and procedures.
b. The CSP should allow the CSC to manage policies, procedures, and processes.
c. The CSP should empower the CSC to manage keys and data encryption keys.
d. The CSP should enable the CSC to manage key encryption keys or master keys used to encrypt data keys.
e. The CSP should allow the CSC to use the key management system (e.g., transactions, reporting, etc.).
f. Optionally, the CSC should supply CSC-generated master encryption keys using bring-your-own-key (BYOK) mechanisms per the SLA.

Control Title:	**Control ID:**	**Control Specification:**
Encryption and Key Management Audit	CEK-09	Audit encryption and key management systems, policies, and processes with a frequency that is proportional to the risk exposure of the system with audit occurring preferably continuously but at least annually and after any security event(s).

Key audit is the process of assessing the organization, governance, infrastructure, policies, procedures, and activities.

a. Audits assess compliance with “key management” policies and procedures.
b. Audits assess the design and effectiveness of “key management” controls and the control environment.
c. Audits assess compliance with industry and regulatory standards (e.g., Health Insurance Portability and Accountability Act (HIPAA), payment card industry (PCI)).
d. Audits results are reported to the key management system authority.
e. Audits are performed according to key- and risk-management policies.
f. Request third-party certification reports and review issues with the CSP and auditor.
g. At a minimum, sensitive audit information and sensitive audit tools should be cryptographically protected.

Control Title:	**Control ID:**	**Control Specification:**
Key Generation	CEK-10	Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used.

Implementation Guidelines:

The key generation process should be cryptographically secure.

a. Keys should be generated:
    1. using random bit generators (RBGs) and possibly other parameters, or
    2. generated based on keys that are created in this fashion.
b. Key management technology and processes should be NIST FIPS validated or NSA-approved or comparable.
c. All relevant transitions/activity should be recorded (logged) in the inventory management system (CKMS).

Control Title:	**Control ID:**	**Control Specification:**
Key Purpose	CEK-11	Manage cryptographic secret and private keys that are provisioned for a unique purpose.

Implementation Guidelines:

Key distribution is the process of logically or physically transferring keys.

a. Distribution of asymmetric key pairs (public, ephemeral, centrally) requires protection mechanisms.
b. Distribution of symmetric keys requires their own protection mechanisms.
c. Distribution of other key materials requires their own protection mechanisms.
d. Distributed keys should be protected at rest, in storage, in transit, and to the appropriate extent (even when in use).
e. Distribution controls must address confidentiality, integrity, and availability.
f. Manual or automated (preferable) distribution may be used.
g. All relevant transitions/activity should be recorded (logged) in the inventory management system (CKMS).

Control Title:	Control ID:	Control Specification:
Key Rotation	CEK-12	Rotate cryptographic keys in accordance with the calculated cryptoperiod, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements.

Implementation Guidelines:

Key rotation generates (based on policy) a new key version of a key used to encrypt data.

a. Non-primary (old) keys should be used to decrypt data previously encrypted before re-encrypting the data with new keys.
b. Old data may be re-encrypted using new keys based on organizational policy and technology capacity.
c. When rotating keys, consider the following principles:
    - Cryptographic mechanism strength: algorithm, key length, and mode of operation.
    - The volume of information flow or the number of transactions.
    - The security life of the data.
    - The security functions, such as data encryption, digital signature, and key protection.
    - The number of key copies and the distribution of those copies.

d. All relevant transitions/activity should be recorded (logged) in the inventory management system (CKMS).

Control Title:	Control ID:	Control Specification:
Key Revocation	CEK-13	Define, implement and evaluate processes, procedures and technical measures to revoke and remove cryptographic keys prior to the end of its established cryptoperiod, when a key is compromised, or an entity is no longer part of the organization, which include provisions for legal and regulatory requirements.

Implementation Guidelines:

Key revocation removes keys from operational use before their expiration dates.

a. Key revocation of a “symmetric key” restricts the use of the key material.
b. Key revocation of an asymmetric key specifically refers to the private key.
c. Perform emergency revocation when keys are lost or compromised.
d. Revocation statuses should be available to all who have relied on the key.
e. Use certificate revocation lists (CRLs) or other relevant mechanisms to inform stakeholders.
f. ROI: Cost to decrypt then re-encrypt large distributed databases with a significant number of key holders.
g. ROI: Risk of long-term cryptoperiods versus short and the amount of data encrypted with one key.
h. All relevant transitions/activity should be recorded (logged) in the inventory management system (CKMS).

Control Title:
Key Destruction

Control ID:
CEK-14

Control Specification:
Define, implement and evaluate processes, procedures and technical measures to destroy keys stored outside a secure environment and revoke keys stored in Hardware Security Modules (HSMs) when they are no longer needed, which include provisions for legal and regulatory requirements.

Implementation Guidelines:
Key destruction removes all traces to prevent recovery by physical or electronic means.

a. When a key is to be destroyed, all key copies should be destroyed.
b. Keys should be destroyed when they are not needed to minimize compromise risks.
c. Secret and private keys should be destroyed so they cannot be recovered by any means.
d. Public keys may be kept or destroyed.
e. Notify stakeholders in advance of key destruction.
f. Consider laws, regulations, and their retention requirements for keys and/or metadata.
g. Key recovery information (KRI) should be protected against unauthorized disclosure or destruction.
h. All relevant transitions/activity should be recorded (logged) in the inventory management system (CKMS).

Control Title:
Key Activation

Control ID:
CEK-15

Control Specification:
Define, implement and evaluate processes, procedures and technical measures to create keys in a pre-activated state when they have been generated but not authorized for use, which include provisions for legal and regulatory requirements.

Implementation Guidelines:
Activated keys are used to protect information cryptographically.

a. Pre-activated keys are activated by entering the start date of the validity/cryptoperiod.
b. Keys which are not activated for use are not ready to encrypt data.
c. Non-activated keys should only be used to perform proof-of-possession or key confirmation.
d. If pre-activated keys are no longer needed, they should be destroyed.
e. If there are suspicions about the integrity of a given key, it should be moved to the compromised state.
f. All relevant transitions/activity should be recorded (logged) in the inventory management system (CKMS).

Control Title:
Key Suspension

Control ID:
CEK-16

Control Specification:
Define, implement and evaluate processes, procedures and technical measures to monitor, review and approve key transitions from any state to/from suspension, which include provisions for legal and regulatory requirements.

Implementation Guidelines:
Suspended keys are not used for a period.

a. Keys may be suspended for leaves of absence or suspicion of compromise.
b. Suspensions should be investigated before transitioning to activation, revocation, or replacement.
c. Suspended keys should not be used to encrypt data, but they can decrypt data.
d. Do not process encryption applied after the beginning of a suspension period.
e. All relevant transitions/activity should be recorded (logged) in the inventory management system (CKMS).

Control Title:	**Control ID:**	**Control Specification:**
Key Deactivation	CEK-17	Define, implement and evaluate processes, procedures and technical measures to deactivate keys at the time of their expiration date, which include provisions for legal and regulatory requirements.

Implementation Guidelines:
Deactivated keys should not be used to encrypt but can be used to decrypt.

a. Upon the expiration date, keys should not be able to encrypt data.
b. The deactivated state should transition to the destroyed state when keys are no longer needed.
c. Metadata should be retained for audit purposes.
d. All relevant transitions/activity should be recorded (logged) in the inventory management system (CKMS).

Control Title:	**Control ID:**	**Control Specification:**
Key Archival	CEK-18	Define, implement and evaluate processes, procedures and technical measures to manage archived keys in a secure repository requiring least privilege access, which include provisions for legal and regulatory requirements.

Implementation Guidelines:
Key archiving places keys in long-term storage.

a. Archived key material can support the later recovery of information.
b. While archived key material may be needed in the future, the key material should be destroyed when no longer required.
c. The key recovery process should include the generation, storage, and access of the long-term storage keys used to protect backed-up and archived key information.
d. Archives should be used for long-term key access.
e. The inventory system should record the storage and recovery of archived key information.
f. All relevant transitions/activity should be recorded (logged) in the inventory management system (CKMS).

Control Title:	Control ID:	Control Specification:
Key Compromise	CEK-19	Define, implement and evaluate processes, procedures and technical measures to use compromised keys to encrypt information only in controlled circumstances, and thereafter exclusively for decrypting data and never for encrypting data, which include provisions for legal and regulatory requirements.

Implementation Guidelines:

Compromised keys/states are keys that may be waiting for the performance of an investigation to determine the appropriate disposition. Compromised keys should be revoked using the organization's emergency revocation policy.

When appropriate, relevant stakeholders should be notified that keys previously used to encrypt their data have been compromised and that those keys are no longer used for encryption.

These compromised keys should be notated in the organization's "Compromised Key Lists (CKLs)" along with a summary of users notified, notification timeframes, or reasons that notifications were not made to compromised key users.

Compromised keys await an investigation to determine disposition.

a. Perform emergency revocation when keys are lost or compromised.
b. A compromised status should be available to all who have relied on the key.
c. Use CKLs to inform stakeholders.
d. Compromised status is also reflected in the inventory management system.
e. Use audits to uncover undetected compromised keys.
f. Analyze events to support recovery from compromises.
g. Detail the method for revoking and re-keying compromised keys.
h. Use cryptoperiods to limit compromised key damage.
i. A compromised key should only be used to process data it has protected for the sole purpose of de-encrypting the data.
j. All transitions/activity shall be recorded (logged) and the key state updated in the inventory management system (CKMS).

Control Title:	Control ID:	Control Specification:
Key Recovery	CEK-20	Define, implement and evaluate processes, procedures and technical measures to assess the risk to operational continuity versus the risk of the keying material and the information it protects being exposed if control of the keying material is lost, which include provisions for legal and regulatory requirements.

Implementation Guidelines:
Key recovery retrieves or reconstructs keys from backups or archives. When recovering keys, consider:

a. The type of key (e.g., private signature keys or symmetric data encryption keys).
b. The application in which the key will be used (e.g., interactive communication or file storage).
c. Whether the key is "owned" by the local entity, another entity, or is shared.
d. The role of the entity in communication (e.g., sender or receiver).
e. The algorithm or computation in which the key will be used.
f. All relevant transitions/activity should be recorded (logged) in the inventory management system (CKMS).

Control Title:	**Control ID:**	**Control Specification:**
Key Inventory Management	CEK-21	Define, implement and evaluate processes, procedures and technical measures in order for the key management system to track and report all cryptographic materials and changes in status, which include provisions for legal and regulatory requirements.

Implementation Guidelines:
Cryptographic Key Management Systems (CKMS), whether manual or automated, exist to process, control, store and report key management activity.

The CKMS should:

a. Capture, track and label all changes in status.
b. Continuously monitor for unknown cryptographic assets.
c. Generate and distribute key information.
d. Acquire or generate public-key certificates.
e. Backup archive and inventory key information.
f. Maintain a database that maps entities to an organization's certificate or key structure.
g. Provide maintenance and distribution of revoked key or certificate reports.
h. Generate audit requests and process audit responses.
i. Crypto materials include keys, certificates, and HSMs.
j. Key management technology and processes should be NIST FIPS validated and NSA-approved.
k. Cryptographic key management system security policies should protect the confidentiality, integrity, availability, and source authentication of all keys, certificates, algorithms, and metadata.
l. All relevant transitions/activity should be recorded (logged) in the inventory management system (CKMS).

2.6 Datacenter Security (DCS)

<table>
<tr><td><b>Control Title:</b>
Off-Site Equipment Disposal Policy and Procedures</td><td><b>Control ID:</b>
DCS-01</td><td><b>Control Specification:</b>
Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure disposal of equipment used outside the organization's premises. If the equipment is not physically destroyed a data destruction procedure that renders recovery of information impossible must be applied. Review and update the policies and procedures at least annually.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
When clients delete, leave, or egress a cloud platform, the provider should follow a sequence of structured steps to ensure that client data has been expunged from the provider environment according to the terms in the contract and best practice (per vetted guidance sources such as NIST 800-88). In addition, the client may request verification that data has been effectively removed.

These steps should include, but are not limited to:
a. Removal of sensitive data or systems not regularly accessed by the organization, service provider, partner, etc. (stand-alone systems).
b. Completion of a confidentiality assessment—including a verified process for select information sanitization and disposal processes.
c. A record of the process should be documented and communicated to support decisions.
d. All sanitized or destroyed assets should be logged into a tracking system with a certificate of media disposition (clear, purge, or destroy).</td></tr>
<tr><td><b>Control Title:</b>
Off-Site Transfer Authorization Policy and Procedures</td><td><b>Control ID:</b>
DCS-02</td><td><b>Control Specification:</b>
Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location. The relocation or transfer request requires the written or cryptographically verifiable authorization. Review and update the policies and procedures at least annually.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
The communications between services that facilitate movements of workloads, application data, etc., should be encrypted based on globally recognized crypto algorithms such as AES-256. Additionally, communication may include measures such as obfuscation or de-identification to render the information in transit illegible. NIST 800-122 (Guide to Protecting the Confidentiality of Personally Identifiable Information - PII) provides relevant and effective techniques for obscuring sensitive data, such as personally identifiable information (PII), etc.</td></tr>
</table>

<table>
<tr><td><b>Control Title:</b>
Secure Area Policy and Procedures</td><td><b>Control ID:</b>
DCS-03</td><td><b>Control Specification:</b>
Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for maintaining a safe and secure working environment in offices, rooms, and facilities. Review and update the policies and procedures at least annually.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
The CSP should identify the manageable parts of the data center and consider operational criteria, such as effectiveness, efficiency, compliance, reliability, risk management, functionality, availability, integrity, and confidentiality. Then, the CSP should prepare and maintain policies and procedures for each part.

Policies and procedures should include provisions to restrict physical access to the facilities to prevent unauthorized entry.

Facility areas that house, store, and transact customer data should be configured to prevent confidential information or activities from being visible and audible from the outside. Electromagnetic shielding should also be considered as appropriate (ISO standard; ISO_IEC_27002_2013 - 11.1.3 (c)).

In addition, the facility itself should be designed and positioned to reduce the risk of natural disasters. Systems and infrastructure should be deployed to enhance fire prevention—typically utilizing zoned dry-pipe sprinkler systems. These systems are intended to be deployed throughout the facility and not just within the computer room.</td></tr>
<tr><td><b>Control Title:</b>
Secure Media Transportation Policy and Procedures</td><td><b>Control ID:</b>
DCS-04</td><td><b>Control Specification:</b>
Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media. Review and update the policies and procedures at least annually.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Secure transportation of physical media should include secure information-handling policies and procedures for storage, packaging by internal or external personnel (third-parties, such as couriers), internal delivery, packaging for external mail or courier services, and shipping tracking.</td></tr>
<tr><td><b>Control Title:</b>
Assets Classification</td><td><b>Control ID:</b>
DCS-05</td><td><b>Control Specification:</b>
Classify and document the physical, and logical assets (e.g., applications) based on the organizational business risk.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
The facility management should develop a naming convention for asset classification that meets legal, value, and business requirements to protect restricted information sharing.</td></tr>
</table>

<table>
<tr><td><b>Control Title:</b>
Assets Cataloguing and Tracking</td><td><b>Control ID:</b>
DCS-06</td><td><b>Control Specification:</b>
Catalogue and track all relevant physical and logical assets located at all of the CSP’s sites within a secured system.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Datacenter personnel should utilize a solution that enables inventory tracking and managing physical locations of servers and other data center assets while eliminating paper and manual processes. A hosted asset tracking solution for servers, switches, data center asset tracking and racks typically uses passive radio frequency identification (RFID), global positioning system (GPS), and/or Bluetooth Low Energy (BLE) technologies.</td></tr>
<tr><td><b>Control Title:</b>
Controlled Access Points</td><td><b>Control ID:</b>
DCS-07</td><td><b>Control Specification:</b>
Implement physical security perimeters to safeguard personnel, data, and information systems. Establish physical security perimeters between the administrative and business areas and the data storage and processing facilities areas.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Physical security perimeters should be restricted to authorized personnel only. They may include (but are not limited to): fences, walls, barriers, guards, gates, external boundary protection, bollards, fencing, guard dogs, armed guards, physical authentication mechanisms, reception desks, and security patrols.</td></tr>
<tr><td><b>Control Title:</b>
Equipment Identification</td><td><b>Control ID:</b>
DCS-08</td><td><b>Control Specification:</b>
Use equipment identification as a method for connection authentification.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Where applicable, use location-aware technologies to validate connection authentication integrity based on known equipment locations.</td></tr>
<tr><td><b>Control Title:</b>
Secure Area Authorization</td><td><b>Control ID:</b>
DCS-09</td><td><b>Control Specification:</b>
Allow only authorized personnel access to secure areas, with all ingress and egress points restricted, documented, and monitored by physical access control mechanisms. Retain access control records on a periodic basis as deemed appropriate by the organization.</td></tr>
</table>

<table>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Monitor, control, and isolate data storage and processing facilities, including ingress and egress points to service and delivery areas and other points where unauthorized personnel may enter the premises. Organizations should retain access logs for authorized personnel for no less than six (6) months. Facilities owners should adopt the ISO/IEC 27001:2013 (A.11.1.2) standard. Record the dates and times of visitor entries and departures, and supervise all visitors unless their access has been previously approved. Visitors should only be granted access for specific, authorized purposes and issued with instructions on area security requirements and emergency procedures. Authenticate visitor identities by any appropriate means (i.e., validation with government-issued identification (ID), such as an official identity document, driver's license, passport, etc.).</td></tr>
<tr><td><b>Control Title:</b>
Surveillance System</td><td><b>Control ID:</b>
DCS-10</td><td><b>Control Specification:</b>
Implement, maintain, and operate datacenter surveillance systems at the external perimeter and at all the ingress and egress points to detect unauthorized ingress and egress attempts.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
The external and internal perimeter should be equipped with security alarm systems and surveillance devices such as: movement sensors, cameras, etc., and monitored by security personnel. The recordings should be retrained for a defined period.</td></tr>
<tr><td><b>Control Title:</b>
Unauthorized Access Response Training</td><td><b>Control ID:</b>
DCS-11</td><td><b>Control Specification:</b>
Train datacenter personnel to respond to unauthorized ingress or egress attempts.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Comprehensive training on detecting and responding to various kinds of unauthorized access attempts should be provided to relevant data center personnel and issued periodically.</td></tr>
<tr><td><b>Control Title:</b>
Cabling Security</td><td><b>Control ID:</b>
DCS-12</td><td><b>Control Specification:</b>
Define, implement and evaluate processes, procedures and technical measures that ensure a risk-based protection of power and telecommunication cables from a threat of interception, interference or damage at all facilities, offices and rooms.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
All cabling should be shielded (when possible) to protect against electromagnetic interference (EMI). Additionally, hide cabling (i.e., under the floor, above cabinets in caged, cable-management systems, etc.) or—at a minimum—protect with (PVC) tubing (or something similar) when possible to protect against unauthorized physical access.</td></tr>
</table>

<table>
<tr><td><b>Control Title:</b>
Environmental Systems</td><td><b>Control ID:</b>
DCS-13</td><td><b>Control Specification:</b>
Implement and maintain data center environmental control systems that monitor, maintain and test for continual effectiveness the temperature and humidity conditions within accepted industry standards.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Examples of environmental systems include but are not limited to temperature and humidity systems, fire prevention, and detection systems.
Environmental system reviews should include activities to ensure continual effectiveness, and environmental control systems should be maintained at normal operational levels during a power outage.</td></tr>
<tr><td><b>Control Title:</b>
Secure Utilities</td><td><b>Control ID:</b>
DCS-14</td><td><b>Control Specification:</b>
Secure, monitor, maintain, and test utilities services for continual effectiveness at planned intervals.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Examples of utility services include but are not limited to water, power, telecommunications, and internet connectivity.
Service reviews should include activities to protect from unauthorized interception or damage and ensure the services are designed with automated failover or other redundancies if planned or unplanned disruptions occur.</td></tr>
<tr><td><b>Control Title:</b>
Equipment Location</td><td><b>Control ID:</b>
DCS-15</td><td><b>Control Specification:</b>
Keep business-critical equipment away from locations subject to high probability for environmental risk events.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Keep business-critical equipment away from locations subject to a high probability of environmental risks, such as switchyards and chemical facilities. Hazards include fires, flooding (e.g., waterlogging, water pipe exposure), dust, wind (i.e., exposure to open doors/windows), and natural disasters (earthquakes and hurricanes).</td></tr>
</table>

2.7 Data Security and Privacy Lifecycle Management (DSP)

Control Title:	**Control ID:**	**Control Specification:**
Security and Privacy Policy and Procedures	DSP-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the classification, protection and handling of data throughout its lifecycle, and according to all applicable laws and regulations, standards, and risk level. Review and update the policies and procedures at least annually.

Implementation Guidelines:
Policies and procedures should include provisions for the following:

a. Data classifications with clear definitions and examples.
b. Acceptable use, handling, and storage of data by classifications.
c. How long the classified data should be retained.
d. How/when the classified data should be destroyed.
e. Responsibilities of data stewards.

Maintain a data inventory and document data flow diagrams and associated technical measures.

Document data protection controls and third-party data sharing practices. This documentation and associated risks should be shared with customers and data owners as needed.

Examples include but are not limited to:

- Access controls and data loss prevention (DLP) solutions with data tagging capabilities.
- Define testing intervals based on data classification types or levels.
- Executive leadership should approve policies (cf. GRC-01).
- Note: Data life cycles include all stages (processing, storage, and transmission).

Control Title:	**Control ID:**	**Control Specification:**
Secure Disposal	DSP-02	Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means.

Implementation Guidelines:
Data deletion should be conducted securely and effectively to ensure that it is not recoverable by any means, including forensic techniques. Examples include but are not limited to cross-cut shredding or incinerating hard copy materials, and writing zeros.

Control Title:	**Control ID:**	**Control Specification:**
Data Inventory	DSP-03	Create and maintain a data inventory, at least for any sensitive data and personal data.

Implementation Guidelines:
The data inventory should provide visibility into the location, volume, and context of all sensitive data and PII through data discovery activities that result in a data inventory. Continuously support the classification process using discovery.

Control Title:
Data Classification

Control ID:
DSP-04

Control Specification:
Classify data according to its type and sensitivity level.

Implementation Guidelines:
Implement data classification by defining organizational data categories, such as public data, confidential data, etc. Automated tools to label files, per their sensitivity levels, may be used. Appropriate security measures/protection should be implemented, per its categorization.

Use data classification, tagging, or metadata fields based on industry-standard frameworks such as (but not limited to):

a. Carnegie Mellon University: Guidelines for Data Classification
b. SANS Institute: Tagging Data to Prevent Data Leakage (Forming Content Repositories)

Control Title:
Data Flow Documentation

Control ID:
DSP-05

Control Specification:
Create data flow documentation to identify what data is processed, stored or transmitted where. Review data flow documentation at defined intervals, at least annually, and after any change.

Implementation Guidelines:
Review and update the data flow documentation periodically.

Control Title:
Data Ownership and Stewardship

Control ID:
DSP-06

Control Specification:
Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually.

Implementation Guidelines:
A data responsibility matrix can be defined, documented, and communicated. The matrix should include, but is not limited to:

a. Data type.
b. The associated obligations (regulatory, contractual, or otherwise).
c. The persons or roles responsible for the data.
d. The frequency at which the documented personal and sensitive data should be reviewed.

Control Title:
Data Protection by Design and Default

Control ID:
DSP-07

Control Specification:
Develop systems, products, and business practices based upon a principle of security by design and industry best practices.

<table>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Data protection and privacy consideration should be included by default at the design stage and throughout the product development lifecycle. In addition, design documentation should clearly describe how data is protected.</td></tr>
<tr><td><b>Control Title:</b>
Data Privacy by Design and Default</td><td><b>Control ID:</b>
DSP-08</td><td><b>Control Specification:</b>
Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. Ensure that systems’ privacy settings are configured by default, according to all applicable laws and regulations.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
In line with privacy considerations by design and default principles, the default/out-of-the-box settings should align with the applicable regional privacy regulations.</td></tr>
<tr><td><b>Control Title:</b>
Data Protection Impact Assessment</td><td><b>Control ID:</b>
DSP-09</td><td><b>Control Specification:</b>
Conduct a Data Protection Impact Assessment (DPIA) to evaluate the origin, nature, particularity and severity of the risks upon the processing of personal data, according to any applicable laws, regulations and industry best practices.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Data protection impact assessment, which is essentially risk assessment from a privacy perspective, should be performed by the data controller before processing if such personal data processing is likely to result in a high risk to the rights and freedoms of natural persons.</td></tr>
<tr><td><b>Control Title:</b>
Sensitive Data Transfer</td><td><b>Control ID:</b>
DSP-10</td><td><b>Control Specification:</b>
Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
When defining processes, procedures, and technical measures for data transfer, consider data transfer within the organization and externally.
Personal data transfer in transit should be protected by strong encryption or similar techniques to prevent unauthorized access by eavesdropping or data transfer interception.</td></tr>
</table>

Control Title:
Personal Data Access, Reversal, Rectification and Deletion

Control ID:
DSP-11

Control Specification:
Define and implement processes, procedures and technical measures to enable data subjects to request access to, modification, or deletion of their personal data, according to any applicable laws and regulations.

Implementation Guidelines:
The data subject should be able to access, view, rectify, or delete personal data in the system or by logging a request with the service provider. The service provider should respond to such requests in alignment with the relevant data protection laws.

Control Title:
Limitation of Purpose in Personal Data Processing

Control ID:
DSP-12

Control Specification:
Define, implement and evaluate processes, procedures and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject.

Implementation Guidelines:
Implement and maintain processes, procedures, and technical measures to ensure the following:

a. The data subject is made aware of the nature and purpose of information collection.
b. The information is relevant and limited to processing requirements.
c. Processing is performed in a reasonable manner that does not infringe upon the data subject's privacy.
d. Processing is for a specific, explicitly defined, and lawful purpose related to a function or activity of the responsible party.
e. Where the controller intends to further process the personal data for an alternative purpose to which the personal data were collected, the data subject should be informed of the purpose and provide consent before additional processing.
f. Information is stored only as long as required.

Control Title:
Personal Data Sub-processing

Control ID:
DSP-13

Control Specification:
Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.

Implementation Guidelines:
The CSP should identify subcontractors and sub-processors that participate in the data processing, along with the chain of accountabilities and responsibilities used to ensure that data protection requirements are fulfilled.

The CSP should inform the cloud customer of any intended changes concerning the addition or replacement of subcontractors or sub-processors and allow the cloud customer to object to such changes or terminate the contract.

The data protection obligations agreed upon between the CSP and the cloud customer should be supported by any subcontractors or sub-processors used by the CSP.

The CSP remains liable to the cloud customer for data protection, regardless of whether the CSP uses subcontractors or not.

Control Title:	**Control ID:**	**Control Specification:**
Disclosure of Data Sub-processors	DSP-14	Define, implement and evaluate processes, procedures and technical measures to disclose the details of any personal or sensitive data access by sub-processors to the data owner prior to initiation of that processing.

Implementation Guidelines:
The CSP should document and notify the data owner of the data that will be accessed by sub-processors. Information may include, but are not limited to, categories of data, special categories of data, and processing operations.

Control Title:	**Control ID:**	**Control Specification:**
Limitation of Production Data Use	DSP-15	Obtain authorization from data owners, and manage associated risk before replicating or using production data in non-production environments.

Implementation Guidelines:
Before replicating data or using data in non-production systems copied from the production system, perform a risk analysis and obtain data owner approval. Then, implement privacy risk mitigating techniques such as anonymization, pseudonymization, etc. (if required).

Control Title:	**Control ID:**	**Control Specification:**
Data Retention and Deletion	DSP-16	Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations.

Implementation Guidelines:
Organizational data retention and deletion practices encompassing both physical and electronic data should be established and implemented.

<table>
<tr><td><b>Control Title:</b>
Sensitive Data Protection</td><td><b>Control ID:</b>
DSP-17</td><td><b>Control Specification:</b>
Define and implement processes, procedures and technical measures to protect sensitive data throughout its lifecycle.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Information rights management technology should be used and applied (when applicable) to all sensitive data. This technology can add a security layer that will help protect files from unauthorized copying, viewing, printing, forwarding, deleting, and editing.</td></tr>
<tr><td><b>Control Title:</b>
Disclosure Notifications</td><td><b>Control ID:</b>
DSP-18</td><td><b>Control Specification:</b>
The CSP must have in place, and describe to CSCs the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations. The CSP must give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
The CSP should have a process that describes how to respond to requests by law enforcement authorities, such as a subpoena, official investigations, or legal proceedings initiated by governmental and/or law enforcement officials. This process should be transparent to the interested CSCs unless otherwise prohibited.</td></tr>
<tr><td><b>Control Title:</b>
Data Location</td><td><b>Control ID:</b>
DSP-19</td><td><b>Control Specification:</b>
Define and implement processes, procedures and technical measures to specify and document the physical locations of data, including any locations in which data is processed or backed up.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
The CSP should track where data is stored, processed, and backed up to ensure it is in line with the laws and regulations applicable to the CSP and ensure those locations are not prohibited.
In addition, the physical locations' registry should be kept up to date and shareable with CSC (if requested).</td></tr>
</table>

2.8 Governance, Risk Management and Compliance (GRC)

<table>
<tr><td>**Control Title:**
Governance Program Policy and Procedures</td><td>**Control ID:**
GRC-01</td><td>**Control Specification:**
Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Review and update the policies and procedures at least annually.</td></tr>
<tr><td colspan="3">**Implementation Guidelines:**
Organizational leadership should govern the program. The program should include—but is not limited to—policies and procedures regarding legal matters, industry-specific regulations, regional requirements, compliance mandates, security and privacy requirements, and information governance. Management of each business area should include the implementation of all applicable governance policies and procedures. Policies and procedures should be reviewed and updated at least annually.</td></tr>
<tr><td>**Control Title:**
Risk Management Program</td><td>**Control ID:**
GRC-02</td><td>**Control Specification:**
Establish a formal, documented, and leadership-sponsored Enterprise Risk Management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks.</td></tr>
<tr><td colspan="3">**Implementation Guidelines:**
The enterprise risk management (ERM) program should consider—and not be limited to—cloud-related information security and data privacy risks. The program should include risk management elements such as risk identification, risk assessment, risk treatment, and risk reporting. Management of each business area should consist of the implementation of the applicable ERM program policies and procedures.
The ERM program should also feature a formal statement of risk appetite and may include creating and maintaining a risk register that reflects the likelihood of occurrence, potential business impacts, risk levels, and proposed mitigation actions for each risk.</td></tr>
<tr><td>**Control Title:**
Organizational Policy Reviews</td><td>**Control ID:**
GRC-03</td><td>**Control Specification:**
Review all relevant organizational policies and associated procedures at least annually or when a substantial change occurs within the organization.</td></tr>
<tr><td colspan="3">**Implementation Guidelines:**
Management-approved defined policies and procedures should be communicated to all employees for adherence. Evaluate policies, procedures, and assigned responsibilities for accuracy and efficacy at least annually and when there are significant internal changes or alterations in the external operating environment.</td></tr>
</table>

Control Title:	**Control ID:**	**Control Specification:**
Policy Exception Process	GRC-04	Establish and follow an approved exception process as mandated by the governance program whenever a deviation from an established policy occurs.

Implementation Guidelines:
The exception process should be defined and approved by the management team and communicated across the organization to promote adherence. Integrate exemptions with the information security risk management process, and review organizational risks whenever a deviation from an established policy occurs.

Control Title:	**Control ID:**	**Control Specification:**
Information Security Program	GRC-05	Develop and implement an Information Security Program, which includes programs for all the relevant domains of the CCM.

Implementation Guidelines:
The program should identify and assign roles, responsibilities, and management commitment.

The CCM domains to address within the information security governance program include, but are not limited to:

a. Audit and assurance
b. Application and interface security
c. Business continuity management and operational resilience
d. Change control and configuration management
e. Cryptography, encryption, and key management
f. Datacenter security
g. Data security and privacy lifecycle management
h. Governance, risk management, and compliance
i. Human resources
j. Identity and access management
k. Interoperability and portability
l. Infrastructure and virtualization security
m. Logging and monitoring
n. Security incident management, e-discovery, and cloud forensics
o. Supply chain management, transparency, and accountability
p. Threat and vulnerability management
q. Universal endpoint management

Management should promote coordination among organizational entities responsible for the different aspects of cloud security and privacy risks. Review the program as required to address threat landscape changes and substantial organization changes.

<table>
<tr><td>**Control Title:**
Governance Responsibility Model</td><td>**Control ID:**
GRC-06</td><td>**Control Specification:**
Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs.</td></tr>
<tr><td colspan="3">**Implementation Guidelines:**
RACI charts (responsible, accountable, consulted, and informed) charts may be used to document roles and responsibilities. Specific people or teams should be assigned for each documented role in the governance program, policies, and procedures. Roles and responsibilities should be reviewed and updated periodically.</td></tr>
<tr><td>**Control Title:**
Information System Regulatory Mapping</td><td>**Control ID:**
GRC-07</td><td>**Control Specification:**
Identify and document all relevant standards, regulations, legal/contractual, and statutory requirements, which are applicable to your organization.</td></tr>
<tr><td colspan="3">**Implementation Guidelines:**
Documentation should reflect the requirements relevant to the organization and be updated regularly to reflect changes in the internal and external operational environments. Communicate requirement changes to management and other personnel, and implement them promptly.</td></tr>
<tr><td>**Control Title:**
Special Interest Groups</td><td>**Control ID:**
GRC-08</td><td>**Control Specification:**
Establish and maintain contact with cloud-related special interest groups and other relevant entities in line with business context.</td></tr>
<tr><td colspan="3">**Implementation Guidelines:**
Management should establish and maintain contact with special interest groups or professional associations to receive early warnings and advice regarding new threats, vulnerabilities, and regulatory updates.</td></tr>
</table>

2.9 Human Resources (HRS)

Control Title:	**Control ID:**	**Control Specification:**
Background Screening Policy and Procedures	HRS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for background verification of all new employees (including but not limited to remote employees, contractors, and third parties) according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, the business requirements, and acceptable risk. Review and update the policies and procedures at least annually.

Implementation Guidelines:

Personnel working under organizational control—including full-time employees, part-time employees, consultants, and temporary staff—should undergo a screening process appropriate for their role and responsibilities before granting access to the corporate network or systems.

Depending on the applicable legislation, inform candidates beforehand about screening activities. Personnel screening should consider all relevant privacy, PII protection, and employment-based legislation and should (when permitted) include the following:

a. Availability of satisfactory references.
b. Verification of the applicant's curriculum vitae, including claimed academic and professional qualifications.
c. Independent identity verification (passports or similar documents).
d. Additional role-specific verifications, such as a credit review if the person will have fiscal responsibilities.

The organization should consider rescreening individuals at regular intervals. Rescreening may also occur if the employee's responsibilities or access to confidential data have increased since their last screening.

The organization should have policies to determine who can screen personnel, how, when, and why the screening is required, where data is stored, and what the retention period constitutes.

All relevant data about personnel should be considered PII and managed accordingly. If the screening is done by an external entity or another organizational department, sensitive information like historic remuneration details should be redacted if irrelevant to the screening process.

Control Title:
Acceptable Use of Technology Policy and Procedures

Control ID:
HRS-02

Control Specification:
Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets. Review and update the policies and procedures at least annually.

Implementation Guidelines:
The organization should establish a policy on acceptable use requirements and standards for protecting and handling the organizational assets and communicate them as sufficient to personnel. In addition, the policy should provide clear direction on how individuals should utilize these assets.

Personnel should acknowledge their understanding and accept responsibility to use information processing resources.

The policy should include, but is not limited to:

a. Expected security behaviors of individuals.
b. Unacceptable behavior of individuals.
c. Permitted use of the organization's assets.
d. Prohibited use of the organization's assets.
e. Organizational monitoring activities.

Policies and procedures should be reviewed and updated at least annually or whenever there are significant changes in the environment, and personnel should be retrained when these changes occur.

Control Title:
Clean Desk Policy and Procedures

Control ID:
HRS-03

Control Specification:
Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures that require unattended workspaces to not have openly visible confidential data. Review and update the policies and procedures at least annually.

Implementation Guidelines:
The organization should establish and communicate a "clean desk" policy to guide personnel on reducing the risk of unauthorized access to information.

The following guidelines should be considered:

a. Sensitive or critical business information (e.g., on paper or electronic storage media) should be locked away—ideally in a safe, cabinet, or other security furniture—when not required.
b. User endpoint devices should be protected by key locks or other physical security means when not in use.

c. Documents containing sensitive information from multi-function devices (such as printers and other reproduction technologies) should be stored securely. When these documents are no longer required, they should be discarded using secure disposal methods.
d. Whiteboard and other types of displays should be cleared when not required.
e. Computers should be configured to automatically lock the computer screen after an idle period (screen lock timeout).
f. Users should be trained to log out of systems or lock computer screens when not at workstations.

The organization should have procedures to vacate facilities, including conducting a final sweep before leaving to validate the organization's assets are not left behind (e.g., documents fallen behind drawers or furniture).

Control Title:	**Control ID:**	**Control Specification:**
Remote and Home Working Policy and Procedures	HRS-04	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect information accessed, processed or stored at remote sites and locations. Review and update the policies and procedures at least annually.

Implementation Guidelines:
Organizations allowing remote working activities should issue a policy that defines the conditions and restrictions of working away from a regular office.

The following matters should be considered:
a. The use of lockable filing cabinets
b. Secure transportation between locations
c. Remote access
d. Clean desk
e. Remote printing
f. Information disposal

Secure communications should take the following into account:
g. The need for remote access to the organization's internal systems.
h. The sensitivity of the information that will be accessed and passed over the communication link.
i. The need to connect to internal systems.
j. The use of remote access (such as virtual desktop access) that prevents processing and information storage on privately-owned equipment.
k. The threat of unauthorized access to information or resources from others at the remote working site (i.e., family, friends, and others in a public environment).
l. The use of home and public networks.
m. The requirements or restrictions on the configuration of wireless network services.
n. Protection against malware and firewall requirements.
o. The use of multi-factor authentication mechanisms when remote access to the organization's network is allowed.

The guidelines should also include:

p. Where the use of privately owned equipment not under the organizational control is not allowed.
q. Revocation of authority and access rights and the return of the equipment when the remote-working activities are terminated.

Control Title:	**Control ID:**	**Control Specification:**
Asset Returns	HRS-05	Establish and document procedures for the return of organization-owned assets by terminated employees.

Implementation Guidelines:
The organization should establish and communicate a policy and procedure for the return of assets owned or controlled by the organization upon the termination of a personnel contract.

The organization should identify and document all information and other associated assets to be returned or disabled.

Information and assets can include:

a. User endpoint devices
b. Portable storage devices
c. Specialist equipment
d. Authentication hardware (e.g., mechanical keys, physical tokens, and smartcards) for information systems, sites, and physical archives
e. Physical copies of information

The organization should prevent the unauthorized copying of information (e.g., intellectual property) by personnel under a notice of termination.

Control Title:	**Control ID:**	**Control Specification:**
Employment Termination	HRS-06	Establish, document, and communicate to all personnel the procedures outlining the roles and responsibilities concerning changes in employment.

Implementation Guidelines:
The organization should establish and communicate a 'termination of employment' policy that defines the responsibilities and duties that should remain valid after termination of employment or a change in employment status. This may include guidelines on information confidentiality, intellectual property, and other knowledge obtained while personnel was employed under the organization's control, and responsibilities contained within any additional confidentiality agreements. These responsibilities should be included in employment terms and conditions.

The process for termination or change of employment should also be applied to external personnel (i.e., suppliers) when contract or job termination occurs or there is a role change within the organization.

Control Title:	**Control ID:**	**Control Specification:**
Employment Agreement Process	HRS-07	Employees sign the employee agreement prior to being granted access to organizational information systems, resources and assets.

Implementation Guidelines:
Employees should not be granted access to systems or information unless they have signed the employment agreement featuring terms and conditions concerning information security. The terms and conditions of employment should be appropriate to the employee based on their role. Additionally, roles and responsibilities should be communicated during the hiring process.

The terms and conditions concerning information security should be reviewed and updated if relevant laws, regulations, or information security policies change. Furthermore, personnel may be asked to acknowledge and agree to such changes.

Control Title:	**Control ID:**	**Control Specification:**
Employment Agreement Content	HRS-08	The organization includes within the employment agreements provisions and/or terms for adherence to established information governance and security policies.

Implementation Guidelines:
The agreement between the employee and organization should include—but is not limited to—a confidentiality or non-disclosure agreement if the employee will have access to confidential data.

Policy statements relevant to the employee/contractor should be communicated through training.

Employee legal responsibilities regarding their rights as an employee of the organization (i.e., whistleblower, data protection regulations, etc.) should include guidance on how to handle both physical and digital assets.

The organization should take appropriate and proportionate action if an employee is in breach of an agreement.

Control Title:	**Control ID:**	**Control Specification:**
Personnel Roles and Responsibilities	HRS-09	Document and communicate roles and responsibilities of employees, as they relate to information assets and security.

Implementation Guidelines:
The organization should identify and document information asset protection responsibilities and carry out specific information security processes. Responsibilities for information security risk management activities— and especially accepting residual risks—should be defined.

These responsibilities should be supplemented, where necessary, with more detailed guidance for specific sites and information processing facilities.

Individual responsibilities should be defined, documented, and communicated. Furthermore, this delegation should not absolve the primary responsibility holder from removing an individual's authority.

Control Title:	**Control ID:**	**Control Specification:**
Non-Disclosure Agreements	HRS-10	Identify, document, and review, at planned intervals, requirements for non-disclosure/ confidentiality agreements reflecting the organization's needs for the protection of data and operational details.

Implementation Guidelines:
The non-disclosure agreement should address requirements to protect confidential information using legally binding terms. Agreement terms should be based on the organization's information security requirements. The type of information covered should define permissible access and information handling protocols. The agreement should include, but is not limited to:

a. What information is protected.
b. The length of the agreement.
c. Interested parties to the agreement.
d. The responsibilities of each party in the agreement.
e. Terms for the destruction of data once the agreement has ended.
f. Expected actions if a breach of agreement terms occurs.

Control Title:	**Control ID:**	**Control Specification:**
Security Awareness Training	HRS-11	Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organization and provide regular training updates.

Implementation Guidelines:
Security awareness training should educate personnel about their responsibilities and the necessary means for securing corporate assets.

Security awareness training should consider the roles and responsibilities of organizational members.

Training may include a test to measure personnel's understanding of the responsibilities and protections required to secure corporate assets. This evaluation may be used to improve training and verify that relevant knowledge transfer occurs. Additionally, a training attendance registry should be maintained.

<table>
<tr><td><b>Control Title:</b>
Personal and Sensitive Data Awareness and Training</td><td><b>Control ID:</b>
HRS-12</td><td><b>Control Specification:</b>
Provide all employees with access to sensitive organizational and personal data with appropriate security awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Security awareness training should educate personnel on their responsibilities and the necessary means for securing personal and sensitive data.

Training should include the various regulatory and legal requirements that impact personal and sensitive data handling.

Furthermore, training should occur regularly to incorporate changes in organizational procedures, processes, and policies.</td></tr>
<tr><td><b>Control Title:</b>
Compliance User Responsibility</td><td><b>Control ID:</b>
HRS-13</td><td><b>Control Specification:</b>
Make employees aware of their roles and responsibilities for maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
The organization should maintain a training and awareness program that regularly reminds personnel of their responsibilities. These responsibilities include maintaining awareness and compliance with policies, procedures, and applicable legal, statutory, and/or regulatory obligations.

The training and awareness program may include several awareness-raising activities via appropriate physical or virtual channels, such as campaigns, booklets, posters, newsletters, websites, information sessions, briefings, e-learning modules, and emails.</td></tr>
</table>

2.10 Identity and Access Management (IAM)

<table>
<tr><td><b>Control Title:</b>
Identity and Access Management Policy and Procedures</td><td><b>Control ID:</b>
IAM-01</td><td><b>Control Specification:</b>
Establish, document, approve, communicate, implement, apply, evaluate and maintain policies and procedures for identity and access management. Review and update the policies and procedures at least annually.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Organizations should document access control policies for the registration, management, and removal of digital identities. Additionally, the guidelines should be communicated within the organization.

The policy should:
a. Include, but not be limited to, roles and responsibilities concerning creation, changes, and deletion of access controls (including a regular review of access).
b. Conduct reviews regularly (at least annually).

The organization should leverage the identity and access management policy to establish a security baseline.</td></tr>
<tr><td><b>Control Title:</b>
Strong Password Policy and Procedures</td><td><b>Control ID:</b>
IAM-02</td><td><b>Control Specification:</b>
Establish, document, approve, communicate, implement, apply, evaluate and maintain strong password policies and procedures. Review and update the policies and procedures at least annually.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Organizations should establish a clear policy on strong password usage for different technical areas. Organizations should also have a monitoring mechanism to evaluate the effectiveness of policy implementation.

The policy should be reviewed periodically (at least annually) based on business requirements. In addition, the policy should clearly describe its applicability and scope, and management should promote effective communication to ensure effective implementation within the organization.

Organizations should also have policies and procedures for all personnel (employees, vendors, or other third parties) who have access to organizational data. Additionally, control-testing strategies should be employed to test these policies and be maintained regularly.</td></tr>
<tr><td><b>Control Title:</b>
Identity Inventory</td><td><b>Control ID:</b>
IAM-03</td><td><b>Control Specification:</b>
Manage, store, and review the information of system identities, and level of access.</td></tr>
</table>

Implementation Guidelines:
Organizations should maintain a database of all system identities having access to different cloud environments and assets. The database should illustrate a correlation between digital identities, assets where the access is provisioned, and the type of access being provisioned (i.e., business users, system users, privilege users, etc.). In addition, the database should be regularly reviewed to ensure access is revoked or changed based on job role changes.

The identity and access management database should incorporate single sign-on and multi-factor authentication for user access.

Database access should be based on need-to-know and least-privilege principles and should follow best practices (such as role-based access control and segregation of duties). Finally, all access (especially privileged access) should be logged and monitored for anomalies and unauthorized use and linked to alerting systems as appropriate.

Control Title:	Control ID:	Control Specification:
Separation of Duties	IAM-04	Employ the separation of duties principle when implementing information system access.

Implementation Guidelines:
Access control policy should provide instruction on separation of environment and separation of duties, and cover the following:

a. Maintain separation of duties between the production, testing, and development environments while limiting read/write access to all environments (such as production, development, and testing).
b. Maintain separation of duties should and require multiple layers of approval (e.g., business approval, system owner approval) to ensure the integrity of access to different systems.

Control Title:	Control ID:	Control Specification:
Least Privilege	IAM-05	Employ the least privilege principle when implementing information system access.

Implementation Guidelines:
User and service account access should leverage access control methods, such as role-based access control (RBAC) and attribute-based access control (ABAC). In addition, conduct regular reviews of access processes (including auditing, when appropriate) to identify non-adherence to the principle of least privilege.

Restrict privileged access and access to administrative accounts should be via the principle of least privilege and a need-to-know basis. Furthermore, access should be set to ”deny all“ unless specifically allowed.

<table>
<tr><td><b>Control Title:</b>
User Access Provisioning</td><td><b>Control ID:</b>
IAM-06</td><td><b>Control Specification:</b>
Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
The organizations should address any changes to the identity and access controls using the pre-established baseline. These changes could be from the proactive management of exploits via vulnerability scanning or reactive management of issues via incident management.</td></tr>
<tr><td><b>Control Title:</b>
User Access Changes and Revocation</td><td><b>Control ID:</b>
IAM-07</td><td><b>Control Specification:</b>
De-provision or respectively modify access of movers / leavers or system identity changes in a timely manner in order to effectively adopt and communicate identity and access management policies.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Deprovisioning should automatically remove associated authorizations. For systems not integrated into automated processes, deprovisioning processes should be manually carried out by system owners. De-provisions to customer data should be made known to cloud customers where applicable.</td></tr>
<tr><td><b>Control Title:</b>
User Access Review</td><td><b>Control ID:</b>
IAM-08</td><td><b>Control Specification:</b>
Review and validate user access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
The principle of separation of duties should also be considered when conducting user access reviews.

Access should be reviewed when users resign, are terminated, change roles, and/or no longer need the authorization to carry out duties for any other reason.</td></tr>
<tr><td><b>Control Title:</b>
Segregation of Privileged Roles</td><td><b>Control ID:</b>
IAM-09</td><td><b>Control Specification:</b>
Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles such that administrative access to data, encryption and key management capabilities and logging capabilities are distinct and separated.</td></tr>
</table>

Implementation Guidelines:
Processes and procedures should be communicated within the organization for adherence and enforcement and regularly reviewed (at least annually).

Separation of duties should be established and implemented between development/test and production environments. With this control, a developer may use an administrator-level account with elevated privileges in the development environment and a separate account with user-level access to the production environment. In addition, appropriate levels of logs should be gathered from the production systems for further monitoring and analysis via security operations.

These operations should be managed using split knowledge and dual control where key management operations are used.

Control Title:	**Control ID:**	**Control Specification:**
Management of Privileged Access Roles	IAM-10	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the culmination of segregated privileged access.

Implementation Guidelines:
Administrators should be allowed to log in as themselves and elevate privilege by systematically requesting a new role assignment to obtain the rights they need to perform tasks. This can be accomplished by establishing temporary, time-bound privileged access for both on-premises and cloud-based infrastructure. The duration of approval validity should be automatically limited. Only authorized users/roles should be pre-approved to request elevation of privileged access.

The privileged access roles and rights should be reviewed periodically. Additionally, all the privilege access rights should be assigned based on multiple approval approaches (i.e., system owner, manager of user, etc.).

All privileged accounts and elevation of privileges should be monitored for suspicious activity, such as login failures or attempts to escalate permissions using a security information and event management (SIEM) solution.

Control Title:	**Control ID:**	**Control Specification:**
CSCs Approval for Agreed Privileged Access Roles	IAM-11	Define, implement and evaluate processes and procedures for customers to participate, where applicable, in the granting of access for agreed, high risk (as defined by the organizational risk assessment) privileged access roles.

Implementation Guidelines:
Processes and procedures should include the following:

- Access to privileged user IDs should be restricted to least privilege and business need to know.
- Require documented approval by authorized parties specifying required privileges.
- All actions taken by any individual with root or administrative privileges should be logged.
- Use of and changes to privileged accounts, including elevation of privileges should be monitored for suspicious activity such as logon failures or attempts to escalate permissions using a SIEM solution.

Control Title:	**Control ID:**	**Control Specification:**
Safeguard Logs Integrity	IAM-12	Define, implement and evaluate processes, procedures and technical measures to ensure the logging infrastructure is read-only for all with write access, including privileged access roles, and that the ability to disable it is controlled through a procedure that ensures the segregation of duties and break glass procedures.

Implementation Guidelines:
The organization should consider the following for the control's implementation:

a. Logs should be stored in a centralized log management solution with separation of duties maintained by an independent team if possible.
b. Logs should be integrated with a SIEM-type solution for real-time monitoring to raise alerts in case of any violation.

Control Title:	**Control ID:**	**Control Specification:**
Uniquely Identifiable Users	IAM-13	Define, implement and evaluate processes, procedures and technical measures that ensure users are identifiable through unique IDs or which can associate individuals to the usage of user IDs.

Implementation Guidelines:
All users should be assigned a unique ID before allowing access to system components or applications. Allocating a unique ID to each person with access ensures each individual is uniquely accountable for their actions. When such accountability occurs, actions taken on critical data and systems can be traced to known, authorized users and processes.

The organization should have a process to detect any creation of non -individual accounts in any infrastructure/application (either in the cloud or on-premises).

<table>
<tr><td><b>Control Title:</b>
Strong Authentication</td><td><b>Control ID:</b>
IAM-14</td><td><b>Control Specification:</b>
Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multi factor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
All individual, non-console administrative access and remote access to the systems and applications should be secured using multi-factor authentication. Multi-factor authentication should contain a minimum of two of the three authentication methods:
a. Something you know, such as a password or passphrase.
b. Something you have, such as a token device or smart card or digital certification*.
c. Something you are, such as a biometric.

* Note: a digital certificate is a valid option for "something you have" as long as it is unique for a particular user)</td></tr>
<tr><td><b>Control Title:</b>
Passwords Management</td><td><b>Control ID:</b>
IAM-15</td><td><b>Control Specification:</b>
Define, implement and evaluate processes, procedures and technical measures for the secure management of passwords.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
The organization should adopt the following guidelines for the secure management of passwords:
• Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a network system.
• All non-console administrative access should be encrypted using strong cryptography.
• Using strong cryptography, all authentication credentials (such as passwords or phrases) should be rendered unreadable during transmission and storage on all system components.
• Verify user identity before modifying any authentication credential (i.e., performing password resets, provisioning new tokens, or generating new keys).
• Passwords/passphrases should meet the criteria of industry best practices.
• Alternatively, the password/passphrases should have complexity and strength at least equivalent to the parameters specified above.
• Change user passwords/passphrases per the organization password standard.
• Limit password reuse per the organization password standard.
• Set passwords/passphrases for first-time use and upon reset to a unique value for each user and change immediately after the first use.</td></tr>
</table>

Document and communicate authentication policies and procedures to all users, including the following concepts:

a. Guidance on selecting strong authentication credentials.
b. Guidance for how users should protect their authentication credentials.
c. Generic user IDs are disabled or removed.
d. Shared user IDs do not exist for system administration and other critical functions.
e. Shared and generic user IDs are not used to administer any system components.

Guidance on selecting strong passwords may include suggestions to help personnel select hard-to-guess passwords that don’t contain:

f. Dictionary words
g. Information about the user (such as the user ID)
h. Names of family members, date of birth, etc.

Guidance for protecting authentication credentials may include not writing down passwords or saving them in insecure files and being alert for malicious individuals who may attempt to exploit their passwords (see NIST 800:53 password controls for details).

Control Title:	**Control ID:**	**Control Specification:**
Authorization Mechanisms	IAM-16	Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.

Implementation Guidelines:
The information system should require approvals for authorizations to access the system resources and follow communicated and approved applicable policies.

The organization should adopt multiple authorization concepts (i.e., user manager, system/information owner).

2.11 Interoperability and Portability (IPY)

<table>
<tr><td><b>Control Title:</b>
Interoperability and Portability Policy and Procedures</td><td><b>Control ID:</b>
IPY-01</td><td><b>Control Specification:</b>
Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for:
a. Communications between application interfaces
b. Information processing interoperability
c. Application development portability
d. Information/Data exchange, usage, portability, integrity, and persistence
Review and update the policies and procedures at least annually.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
The organization should leverage security testing of interoperability and portability policies and procedures.</td></tr>
<tr><td><b>Control Title:</b>
Application Interface Availability</td><td><b>Control ID:</b>
IPY-02</td><td><b>Control Specification:</b>
Provide application interface(s) to CSCs so that they programmatically retrieve their data to enable interoperability and portability.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
These APIs should support interoperability between components and facilitate the secure migration of applications and data between environments. Documentation supports API functionality, being updated regularly and given to customers alongside new API versions. Furthermore, security issues should be considered during development and updates.</td></tr>
<tr><td><b>Control Title:</b>
Secure Interoperability and Portability Management</td><td><b>Control ID:</b>
IPY-03</td><td><b>Control Specification:</b>
Implement cryptographically secure and standardized network protocols for the management, import and export of data.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Evidence of executed and planned security tests upon all interoperability and portability systems should be provided per contractual agreements or upon request.</td></tr>
</table>

Control Title: Data Portability	**Control ID:** IPY-04	**Control Specification:** Agreements must include provisions specifying CSCs access to data upon contract termination and will include: a. Data format b. Length of time the data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy
Implementation Guidelines: N/A (This field is intentionally left blank)		

2.12 Infrastructure and Virtualization Security (IVS)

Control Title: Infrastructure and Virtualization Security Policy and Procedures	**Control ID:** IVS-01	**Control Specification:** Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Review and update the policies and procedures at least annually.
Implementation Guidelines: Infrastructure Virtualization Security Policy and Procedures should include, but are not limited to: a. Governance and control VM lifecycle management. b. Storage restriction of VM images and snapshots. c. Backup and failover systems. d. Tagging for the VM based on sensitivity / risk level. e. A formal change management process for creation, storage, and use of VM images. Approve changes only when necessary. f. Consistent security policy and configuration across the physical/virtual network. g. Implementation of security technologies that span physical and virtual environments with a consistent policy management and enforcement framework. To implement security technologies that span physical and virtual environments with a consistent policy management and enforcement framework. h. Firewalls, whether physical or virtual, to isolate groups of VMs from other hosted groups. i. Design and implementation access from each trust level to physical and virtual management and security systems.		
Control Title: Capacity and Resource Planning	**Control ID:** IVS-02	**Control Specification:** Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business.

Implementation Guidelines:
Projections of future capacity requirements should be made regularly (at least annually—with proactive actions taken—to mitigate risks of system overload or downtime due to overwhelming demand or increased workloads.

Cloud service providers should maximize resource utilization and optimize resource allocation to ensure adequate performance is delivered in line with the promised capacity.

Cloud service consumers should specify performance and resource requirements in line with the business objectives.

Control Title:	**Control ID:**	**Control Specification:**
Network Security	IVS-03	Monitor, encrypt and restrict communications between environments to only authenticated and authorized connections, as justified by the business. Review these configurations at least annually, and support them by a documented justification of all allowed services, protocols, ports, and compensating controls.

Implementation Guidelines:
Network communications justified by the business should be allowed, encrypted, and require authorization. Conversely, unjustified network communications should be disallowed.

Container application-aware network monitoring tools should be leveraged for:

a. Automated determination of proper container networking surfaces, including both inbound ports and process-port bindings.
b. Detection of traffic flows between containers and other network entities over both wire traffic and encapsulated traffic.
c. Detection of network anomalies—such as unexpected traffic flows within the organization's network, port scanning, or outbound access to potentially dangerous destinations.
d. Detection of invalid or unexpected malicious processes—and data they introduce into the environment.

Control Title:	**Control ID:**	**Control Specification:**
OS Hardening and Base Controls	IVS-04	Harden host and guest OS, hypervisor or infrastructure control plane according to their respective best practices, and supported by technical controls, as part of a security baseline.

Implementation Guidelines:
Supporting technical controls should aid situations when only the ports, protocols, and services necessary to meet business needs are provided. Such controls should be based on benchmarks (e.g., CIS).

Implement anti-malware, file integrity monitoring, and logging, and utilize hardware rooted trust in virtual trusted platform modules (vTPMs).

Whenever possible, organizations should use minimalistic, container-specific host operating systems (OSs), with all other services and functionality disabled—and with read-only file systems and other hardening practices employed to reduce attack surfaces.

a. Hosts that run containers should only run containers and not other apps—such as web servers or databases—outside of containers.
b. Hosts that run containers should be continuously scanned for vulnerabilities and updated promptly.
c. The host OS should not run unnecessary system services.
d. Access to the container host should be based on the need-to-know and least privilege principles.
e. File integrity monitoring and host intrusion detection should be leveraged for containers.

Control Title:	**Control ID:**	**Control Specification:**
Production and Non-Production Environments	IVS-05	Separate production and non-production environments.

Implementation Guidelines:
Separation of the environments may include:

- Stateful inspection firewalls
- Domain/realm authentication sources
- Clear segregation of duties for personnel accessing these environments as part of their job duties

Apply sanitization routines on data before loading into non-production, and define environmental boundaries.

Production workloads should be isolated from the lower environments (e.g., development, testing) when possible.

Control Title:	**Control ID:**	**Control Specification:**
Segmentation and Segregation	IVS-06	Design, develop, deploy and configure applications and infrastructures such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented and segregated, monitored and restricted from other tenants.

<table>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
The following should be considered for control implementation:
a. Established policies, procedures, and best-practices
b. Possible definitions of segmentation should range from “total isolation” to “partial logical separation of business-critical assets and/or personal data/sensitive user data, and sessions”.
c. Compliance with legal, statutory, and regulatory compliance obligations in-scope for particular use-cases or scenarios

Workloads between tenants and business lines should be segmented per the least privilege concept to reduce the attack surface. In addition, workload tagging, resource names, and identification should be used for workloads.</td></tr>
<tr><td><b>Control Title:</b>
Migration to Cloud Environments</td><td><b>Control ID:</b>
IVS-07</td><td><b>Control Specification:</b>
Use secure and encrypted communication channels when migrating servers, services, applications, or data to cloud environments. Such channels must include only up-to-date and approved protocols.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Secure communication—when migrating physical servers, services, applications, or data to virtualized environments—could use a combination of confidentiality, integrity, authentication, source authentication, authorization, and non-repudiation.

Building a secure channel of information transmission can be implemented at various network layers. Secure information transmission channels (ports and protocol) should be used such as : SSL, SSH, TLS operates at the application level, IPsec, ICMP at the network level, and PPTP, ARP are at the link layer.

Only up-to-date versions for these protocols should be used (deprecated versions should not be used). Furthermore, only a secure port (e.g., 443) should be used.</td></tr>
<tr><td><b>Control Title:</b>
Network Architecture Documentation</td><td><b>Control ID:</b>
IVS-08</td><td><b>Control Specification:</b>
Identify and document high-risk environments.</td></tr>
</table>

Implementation Guidelines:
The documents or diagrams should include, but are not limited to, the details below:

a. Architecture diagrams, security zone descriptions, and related policies
b. All components (physical, logical)
c. Hypervisors, workloads, hosts, and networks (physical, virtual), etc.
d. Physical site details for each workload
e. Traffic flow between various components
f. All communication channels, including out-of-band communication channels
g. Defined roles and responsibilities
h. Security zones, workloads on each host, security levels for the workloads, etc.,
i. Identify and document dependencies between the different environments and how they impact the risk assessment.

Control Title:	**Control ID:**	**Control Specification:**
Network Defense	IVS-09	Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks.

Implementation Guidelines:
Vulnerabilities in a physical environment also apply in a virtual environment. Configuration flaws/ vulnerabilities in the applications, firewalls, or networks will be vulnerable to exploits. Defense-in-depth techniques should be leveraged for both physical, logical, and administrative, etc., controls.

Defense-in-depth techniques/insights that should be considered include:

a. Deep packet analysis, traffic throttling, and black-holing.
b. Ingress/egress traffic patterns may include media access control (MAC) spoofing and ARP poisoning attacks and/or distributed denial-of-service (DDoS) attacks.
c. Perimeter firewalls implemented and configured to restrict unauthorized traffic.
d. Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings).
e. Develop capabilities to detect unauthorized (rogue) network devices in the network and disconnect quickly.

2.13 Logging and Monitoring (LOG)

<table>
<tr><td><b>Control Title:</b>
Logging and Monitoring Policy and Procedures</td><td><b>Control ID:</b>
LOG-01</td><td><b>Control Specification:</b>
Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies and procedures at least annually.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
The policies and procedures should include considerations regarding:
a. The purpose, scope, roles, responsibilities, and coordination among organizational entities and training.
b. How are incidents handled during a security incident?
c. What information should be logged and monitored, and for how long?
d. Who is notified in the event of an incident?

Logging and monitoring policies and procedures should capture the following events:
e. Individual user accesses to systems.
f. Actions taken by any individual with root or administrative privileges.
g. Access to all audit logs should be restricted based on need-to-know and least privilege principles.
h. Invalid access attempts.
i. Changes, additions, or deletions to accounts with root or administrative privileges.
j. Use of and changes to identification and authentication mechanisms, including elevation of privilege.
k. Initializing, stopping, or pausing of the audit logs.
l. Creation and deletion of system-level objects.</td></tr>
<tr><td><b>Control Title:</b>
Audit Logs Protection</td><td><b>Control ID:</b>
LOG-02</td><td><b>Control Specification:</b>
Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Log protection methodology should be applied in adherence to any applicable legal, statutory or regulatory compliance obligations. In the absence of those requirements, they should adhere to any standards established as appropriate for the business.</td></tr>
<tr><td><b>Control Title:</b>
Security Monitoring and Alerting</td><td><b>Control ID:</b>
LOG-03</td><td><b>Control Specification:</b>
Identify and monitor security-related events within applications and the underlying infrastructure. Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics.</td></tr>
</table>

<table>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Implementation of application security monitoring should include the following components:
a. Generation of alerts from metrics indicating risks beyond established thresholds.
b. Categorization of risks based on business impact analysis and prioritized monitoring of high-impact risks.
c. Consideration of automation capabilities (when applicable) to streamline application security monitoring.
d. Reporting and/or dashboard to provide real-time visibility to security and business stakeholders on application security statuses.
e. Periodic review of monitoring capabilities and processes by a combined group of security, IT and, business stakeholders.</td></tr>
<tr><td><b>Control Title:</b>
Audit Logs Access and Accountability</td><td><b>Control ID:</b>
LOG-04</td><td><b>Control Specification:</b>
Restrict audit logs access to authorized personnel and maintain records that provide unique access accountability.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Audit logs should track access to aid upon detection of suspicious activity and contain sufficient data to support investigative needs for security breaches.

Access to all audit logs should be restricted based on need-to-know and least privilege principles. Additionally, monitor all relevant actions taken. In the case of unintended or unauthorized actions, alerts should occur.</td></tr>
<tr><td><b>Control Title:</b>
Audit Logs Monitoring and Response</td><td><b>Control ID:</b>
LOG-05</td><td><b>Control Specification:</b>
Monitor security audit logs to detect activity outside of typical or expected patterns. Establish and follow a defined process to review and take appropriate and timely actions on detected anomalies.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Failure response capabilities should be in place. Also, consider infrastructure layers (e.g., network, container orchestration, hypervisor, endpoint, control plane, and data plane).

Monitor failures and alerts should they occur.</td></tr>
<tr><td><b>Control Title:</b>
Clock Synchronization</td><td><b>Control ID:</b>
LOG-06</td><td><b>Control Specification:</b>
Use a reliable time source across all relevant information processing systems.</td></tr>
</table>

<table>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Synchronizing system clocks enables proper coordination between systems and facilitates tracing and the reconstitution of activity timelines.

Potential implementation guidance can be derived from the NIST Internet Time Servers overview (see https://tf.nist.gov/tf-cgi/servers.cgi).

Also, the following concepts should be considered:
a. Critical systems have the correct and consistent time.
b. Time is synchronized across all systems.
c. Time data is protected.
d. Time settings are received from industry-accepted time sources.</td></tr>
<tr><td><b>Control Title:</b>
Logging Scope</td><td><b>Control ID:</b>
LOG-07</td><td><b>Control Specification:</b>
Establish, document and implement which information meta/data system events should be logged. Review and update the scope at least annually or whenever there is a change in the threat environment.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Examples of events that should be logged include:
a. Successful and unsuccessful account login events
b. Account management events
c. Object access
d. Policy change
e. Privilege functions
f. Process tracking and system events
g. All administrator activity
h. Authentication checks
i. Authorization checks
j. Data deletions
k. Data access
l. Data changes
m. Permission changes</td></tr>
<tr><td><b>Control Title:</b>
Log Records</td><td><b>Control ID:</b>
LOG-08</td><td><b>Control Specification:</b>
Generate audit records containing relevant security information.</td></tr>
</table>

Implementation Guidelines:
Relevant security log information should include but is not limited to:

- The event type
- The event time
- The event location
- The event source
- The event outcome
- The identities of any individuals or systems associated with the event

Control Title:	**Control ID:**	**Control Specification:**
Log Protection	LOG-09	The information system protects audit records from unauthorized access, modification, and deletion.

Implementation Guidelines:
Access to audit records should be granted based on a least-privilege basis and only to authorized individuals. Changes to logs, including deletions, should be tracked and approved by authorized individuals. Logs should be backed up per organizational policies.

Control Title:	**Control ID:**	**Control Specification:**
Encryption Monitoring and Reporting	LOG-10	Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures, and controls.

Implementation Guidelines:
Compliance breaches and deviations from standard operations should be reported as defined in the organization's incident management process (as outlined in SEF-01). In addition, file-integrity monitoring or change-detection software should be used to prevent changes in existing log data.

Control Title:	**Control ID:**	**Control Specification:**
Transaction/ Activity Logging	LOG-11	Log and monitor key lifecycle management events to enable auditing and reporting on usage of cryptographic keys.

Implementation Guidelines:
Logging of key lifecycle events should include but are not limited to the following events: key generation, key usage, key storage (including backup), and archiving and key deletion. In addition, only authorized personnel should have access to key materials, and all access attempts should be logged and reviewed.

Document and implement all key-management processes and procedures for cryptographic keys, including:

a. Generation of strong cryptographic keys
b. Secure cryptographic key distribution
c. Secure cryptographic key storage
d. Key revocation after expiry
e. Split knowledge and dual control as needed for manual key management operations
f. Prevention of unauthorized substitution of cryptographic keys

Control Title:	**Control ID:**	**Control Specification:**
Access Control Logs	LOG-12	Monitor and log physical access using an auditable access control system.

Implementation Guidelines:

The organization should monitor and log all physical access via the following means:

a. Verifying physical access of individuals when they enter secure areas.
b. Maintaining physical access logs for the facilities
c. Escorting visitors at all times.
d. Reviewing access control logs regularly.

The organization should use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data, correlate with other entries, and store the data for at least three months (unless otherwise restricted by law.)

The organization should implement physical and/or logical controls to restrict access to publicly accessible network jacks. For example, limit physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.

The organization should develop procedures to distinguish between onsite personnel and visitors with an emphasis on the following considerations:

e. Identifying onsite personnel and visitors (for example, assigning badges)
f. Changing access requirements
g. Revoking or terminating onsite personnel and expired visitor identification

The organization should develop procedures to control physical access for onsite personnel to sensitive areas as follows:

h. Access should be authorized and based on individual job functions.
i. Access should be revoked immediately upon termination. Furthermore, all physical access mechanisms, such as keys, access cards, etc., should be returned or disabled.

Control Title:	**Control ID:**	**Control Specification:**
Failures and Anomalies Reporting	LOG-13	Define, implement and evaluate processes, procedures and technical measures for the reporting of anomalies and failures of the monitoring system and provide immediate notification to the accountable party.

Implementation Guidelines: The organization should define which actions are taken depending on the type of logging and monitoring failure. Anomalies can include software errors, failures to capture some or all logs, failure to backup audit logs, or storage exceeded notifications. This guidance should apply to all information system logs. Organizations should implement a process for the timely detection and reporting of failures of critical security control systems, such as (but limited to): a. Firewalls b. Intrusion detection systems (IDS)/intrusion prevention systems (IPS) c. File integrity monitoring (FIM) d. Anti-virus e. Physical access controls f. Logical access controls g. Audit logging mechanisms

2.14 Security Incident Management, E-Discovery, and Cloud Forensics (SEF)

Control Title:	**Control ID:**	**Control Specification:**
Security Incident Management Policy and Procedures	SEF-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Security Incident Management, E-Discovery, and Cloud Forensics. Review and update the policies and procedures at least annually.
Implementation Guidelines: Management-approved policies and procedures for organizations and personnel who manage incidents should incorporate clearly defined roles and responsibilities—including guidelines on managing the "chain of custody" for forensic evidence collected from affected systems, devices, cloud services, applications, and personnel. These policies, procedures, and supporting systems should result in legally admissible evidence. Policies should require establishing a core, qualified, and standing incident response team that holds the capability to assess, respond, learn, and communicate appropriately. Appropriate reporting standards and procedures shall include lessons learned and key performance indicators (KPIs), which should be defined and implemented for incident response processes and training. Appropriate information should be shared with affected third parties (including customers) promptly.		

Control Title: Service Management Policy and Procedures	**Control ID:** SEF-02	**Control Specification:** Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the timely management of security incidents. Review and update the policies and procedures at least annually.
Implementation Guidelines: Policies and procedures should address personnel involved in the entire incident and event management lifecycle— which includes prevention, identification, investigation, and resolution— as well as periodic training for this personnel.		
Control Title: Incident Response Plans	**Control ID:** SEF-03	**Control Specification:** Establish, document, approve, communicate, apply, evaluate and maintain a security incident response plan, which includes but is not limited to: relevant internal departments, impacted CSCs, and other business critical relationships (such as supply-chain) that may be impacted.
Implementation Guidelines: Incident response plans should provide a roadmap for handling incidents involving the organization's cloud services and the products and services upon which those services rely. These plans should apply whether those dependencies are internal (such as IT, operations, support, and legal) or external (suppliers, vendors, partners, customers, and other third parties).		
Control Title: Incident Response Testing	**Control ID:** SEF-04	**Control Specification:** Test and update as necessary incident response plans at planned intervals or upon significant organizational or environmental changes for effectiveness.
Implementation Guidelines: Periodically test, update, and verify the effectiveness of incident response plans using various event scenarios. For critical operations, plans should be tested at least annually. Test results should be documented and communicated—with follow-up action plans developed as appropriate. Incident response plans should be reconciled with the organization's business continuity and disaster recovery plans. Organizations should also test, update, and improve incident response plans after: a. Significant organizational changes. b. External supply chain disruptions and natural disasters. c. Security attacks, particularly those resulting in security breaches.		

<table>
<tr><td><b>Control Title:</b>
Incident Response Metrics</td><td><b>Control ID:</b>
SEF-05</td><td><b>Control Specification:</b>
Establish and monitor information security incident metrics.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Organizations should define, implement and monitor metrics associated with events and incidents to detect any weaknesses in the operational processes or technical controls which support effective incident management. Metrics may quantify:
a. Volume of events and ratio of events to incidents.
b. Incidents by type, product, department, severity, etc.
c. Timeliness of procedural execution for identification, investigation, and resolution.
d. Variances from documented procedures.</td></tr>
<tr><td><b>Control Title:</b>
Event Triage Processes</td><td><b>Control ID:</b>
SEF-06</td><td><b>Control Specification:</b>
Define, implement and evaluate processes, procedures and technical measures supporting business processes to triage security-related events.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Processes, procedures, and technical measures should be defined and implemented to support the investigation and evaluation of security-related events that allow the organization to prioritize events by severity and impact. The objective for these measures is to prioritize the timely analysis of event information and rapid engagement of the incident response process.

Methodologies—including processes, tools, or machine learning algorithms used in incident handling—should periodically be reviewed for efficacy and accuracy in the current operating environment.</td></tr>
<tr><td><b>Control Title:</b>
Security Breach Notifications</td><td><b>Control ID:</b>
SEF-07</td><td><b>Control Specification:</b>
Define and implement processes, procedures and technical measures for security breach notifications. Report security breaches and assumed security breaches including any relevant supply chain breaches, as per applicable SLAs, laws and regulations.</td></tr>
</table>

Implementation Guidelines:
Security breach notification processes and procedures should reflect legal and regulatory requirements, which may be applicable based on data types processed, organizational geography, or customer geography, etc. Organizational procedures should also reflect contractual customer and partner commitments regarding breach notifications. Security breach governance should include document procedures and instructions as well as training to familiarize personnel with their respective roles and responsibilities.

Accurately and promptly report information security breaches to affected, relevant parties through predefined communication channels, per applicable legal, statutory, and regulatory obligations. Clearly describe the event which occurred and its result, and identify any required or recommended actions for the affected parties. Where applicable, notifications should be sent to relevant parties in a timely manner.

Control Title:	**Control ID:**	**Control Specification:**
Points of Contact Maintenance	SEF-08	Maintain points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.

Implementation Guidelines:
Maintain points of contact by establishing liaisons and preparing them for any investigations requiring rapid engagement with law enforcement.

Document and update security incident contact information regularly. Additionally, processes and responsibilities should be documented and maintained for information accuracy that reflects organizational changes to internal operations and external regulatory environments. Personnel sending security notifications should use these identified contacts.

2.15 Supply Chain Management, Transparency, and Accountability (STA)

<table>
<tr><td><b>Control Title:</b>
SSRM Policy and Procedures</td><td><b>Control ID:</b>
STA-01</td><td><b>Control Specification:</b>
Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the application of the Shared Security Responsibility Model (SSRM) within the organization. Review and update the policies and procedures at least annually.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Cloud service implementations involve a shared security responsibility model (SSRM) between the CSP and the CSC. Although specific details vary from service to service (e.g., depending on the cloud service model and the particular implementation), both CSPs and CSCs should have organizational policies and procedures that delineate how the SSRM should be documented, implemented, managed, communicated, enforced, and audited.</td></tr>
<tr><td><b>Control Title:</b>
SSRM Supply Chain</td><td><b>Control ID:</b>
STA-02</td><td><b>Control Specification:</b>
Apply, document, implement and manage the SSRM throughout the supply chain for the cloud service offering.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
The SSRM explicitly details each specific service based on the cloud service model and implementation specifics. Accordingly, each party in the supply chain should document, implement and manage their SSRM responsibilities for their specific service. This includes supporting service providers such as infrastructure as a service (IaaS) providers engaged by primary software as a service (SaaS) CSPs and specialized CSPs (e.g., IDaaS, CASB, DDOS/CDN/DNS services) employed by the CSP and/or the CSC.</td></tr>
<tr><td><b>Control Title:</b>
SSRM Guidance</td><td><b>Control ID:</b>
STA-03</td><td><b>Control Specification:</b>
Provide SSRM Guidance to the CSC detailing information about the SSRM applicability throughout the supply chain.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Shared security responsibility model guidance should include references describing SSRM applicability throughout the supply chain.</td></tr>
<tr><td><b>Control Title:</b>
SSRM Control Ownership</td><td><b>Control ID:</b>
STA-04</td><td><b>Control Specification:</b>
Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM for the cloud service offering.</td></tr>
</table>

Implementation Guidelines:
Cloud service implementations involve an SSRM between the CSP and the CSC, which varies from service to service depending on the cloud service model and the specific implementation. Accordingly, CSPs should provide comprehensive SSRM guidance to facilitate secure CSC service implementations.

Any CSP control responses should identify control applicability and ownership for their specific service.

a. Cloud service provider-owned: CSP is fully responsible.
b. Cloud service customer-owned: CSC is fully responsible.
c. Third-party outsourced: The CSP has fully outsourced this control to a third party (e.g., a supporting CSP), but the CSP is fully accountable to the CSC for the third party's performance from a supply chain perspective.
d. Shared CSP and CSC: Both the CSP and CSC have responsibilities (independent or dependent). If the CSP has partially outsourced control to a third party, that should be noted in the CSP implementation description.
e. Shared CSP and third party: The CSP has partially outsourced control to a third party (e.g., a supporting CSP). Hence, the CSP and the third party have responsibilities—but the CSC has no responsibilities. The CSP is fully accountable to the CSC for the third party's performance from a supply-chain perspective.
f. N/A: Not applicable to this specific cloud service offering (no SSRM responsibilities).

Cloud service providers should also describe the following for each control (as appropriate) for its service and the specific ownership classification:

g. Cloud service provider implementation description: How the CSP meets (or doesn't meet) the controls they are responsible for, wholly or partially. This should explain why N/A controls are not applicable for the specific service and describe the extent to which responsibility for particular controls is outsourced to third parties.
h. Cloud service customer responsibilities: A detailed description of CSC security responsibilities for the controls the customer is responsible for, wholly or partially, with references and external links (as appropriate).

The *CSA's Consensus Assessments Initiative Questionnaire* (CAIQ) should be used by CSPs to provide SSRM ownership and guidance to current and prospective CSCs. In cases where the CAIQ has multiple questions associated with a single control, CSPs should delineate SSRM ownership and describe how they meet their control requirements at the question level, aligned with the scope of the CSP CAIQ answer.

Control Title:	**Control ID:**	**Control Specification:**
SSRM Documentation Review	STA-05	Review and validate SSRM documentation for all cloud services offerings the organization uses.

Implementation Guidelines:
The CSC should engage with the CSP to address any issues identified as a part of this review, and SSRM changes should be incorporated into the CSC's implementation plans. In addition, any CSC changes to the finalized SSRM documentation should be shared with the CSP as enhancement feedback, as appropriate. Following this communication and any preceding adjustments to the SSRM, CSCs should then implement the finalized SSRM controls and test the controls to validate the proper operation of CSC security controls (including CSP integration where there are dependencies). This implementation and testing should occur during production readiness assessments and transitions.

Control Title:	**Control ID:**	**Control Specification:**
SSRM Control Implementation	STA-06	Implement, operate, and audit or assess the portions of the SSRM which the organization is responsible for.

Implementation Guidelines:
Both the CSP and CSC should implement the finalized SSRM and then thoroughly document and test it to validate proper operation of security control implementations—including integration testing where there are interdependencies. Once implemented, both the CSP and CSC should operate, monitor and audit, and/or assess their service performance according to the finalized SSRM and remain engaged with their supply chain and customers to understand, implement and manage SSRM changes over time.

Particular areas that require proactive supply chain SSRM engagement with corresponding levels of (secure) transparency include:

a. Incident and vulnerability management
b. Change and configuration management
c. Periodic SSRM-aligned audit reviews and security assessments with appropriate risk management

Control Title:	**Control ID:**	**Control Specification:**
Supply Chain Inventory	STA-07	Develop and maintain an inventory of all supply chain relationships.

Implementation Guidelines:
Both the CSP and CSC should develop, manage and maintain a comprehensive inventory of all supply chain relationships (i.e., third-party product and service providers) involved in implementing, operating, and securing their respective cloud service implementations. This process should include assembling, tracking, and maintaining key organizational roles, contracts, contacts, and risk-related information about each third party in the supply chain regularly (and when significant changes occur) to facilitate supply chain risk management practices.

Control Title:	**Control ID:**	**Control Specification:**
Supply Chain Risk Management	STA-08	CSPs periodically review risk factors associated with all organizations within their supply chain.

Implementation Guidelines:
Both the CSP and CSC should follow applicable local and international third-party risk management (TPRM) best practices in managing supply chain risks, including periodic reviews of organizational and technical risk factors, contract requirements, environmental changes, and security incident response capabilities for all supply chain organizations. There may also be applicable regulatory requirements and standards to consider.

Control Title:	Control ID:	Control Specification:
Primary Service and Contractual Agreement	STA-09	Service agreements between CSPs and CSCs (tenants) must incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope, characteristics and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third party assessment • Service termination • Interoperability and portability requirements • Data privacy

Implementation Guidelines:
Service agreement content should include, but is not limited to the following:

a. Scope, characteristics and location of business relationship and services offered: (e.g., service level agreements, customer (tenant) data acquisition, exchange and usage -including data processing restrictions, feature sets and functionality-, personnel and infrastructure components and supporting services for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontractor or outsourced business relationships, geographical location of hosted data, backups and services, and any known regulatory compliance considerations). Refer to STA-08 for CSP management of supply chain applicability (Relevant control domains include particularly DSP, BCR, HRS).
b. Information security requirements (including SSRM): provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes, acceptable use policies and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships, including legal obligations of the CSP to allow government access to customer data. Relevant control domains include particularly DSP, GRM.
c. Change management process: Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts.

d. Monitoring capabilities and controls implemented by the cloud service provider and made available to the cloud customer so as to monitor aspects of the cloud service for which the cloud customer is responsible.
e. Incident management and communication procedures: Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain) complying with SEF's domain control requirements.
f. Right to audit and third party assessment: Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed
g. Service termination: Expiration of the business relationship and treatment of customer (tenant) data impacted
h. Interoperability and portability requirements: Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence
i. Data Privacy (refer to DSP domain)

Control Title:	**Control ID:**	**Control Specification:**
Supply Chain Agreement Review	STA-10	Review supply chain agreements between CSPs and CSCs at least annually.

Implementation Guidelines:
Reviews should include activities to identify non-conformance with contractual requirements and SLAs for services a CSP provides. If non-conformance issues are identified, the parties involved should negotiate and remediate the problems.

Control Title:	**Control ID:**	**Control Specification:**
Internal Compliance Testing	STA-11	Define and implement a process for conducting internal assessments to confirm conformance and effectiveness of standards, policies, procedures, and service level agreement activities at least annually.

Implementation Guidelines:
The scope of assessments should include STA-related policies and procedures while validating adherence to STA controls and SLA requirements. Applicability includes assessing conformance and effectiveness across the supply chain, including the total cloud service technology stack (as appropriate). Refer to A&A-02.

Control Title:	**Control ID:**	**Control Specification:**
Supply Chain Service Agreement Compliance	STA-12	Implement policies requiring all CSPs throughout the supply chain to comply with information security, confidentiality, access control, privacy, audit, personnel policy and service level requirements and standards.

<table>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Contracts throughout the supply chain should include requirements for all third- and fourth-party service providers and personnel with access to CSP and/or CSC systems and information.

Personnel policies should include employment agreements inclusive of information security requirements, security awareness training, and insider risk management.</td></tr>
<tr><td><b>Control Title:</b>
Supply Chain Governance Review</td><td><b>Control ID:</b>
STA-13</td><td><b>Control Specification:</b>
Periodically review the organization’s supply chain partners’ IT governance policies and procedures.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Reviews should validate alignment with applicable industry standards as well as service and contract requirements.</td></tr>
<tr><td><b>Control Title:</b>
Supply Chain Data Security Assessment</td><td><b>Control ID:</b>
STA-14</td><td><b>Control Specification:</b>
Define and implement a process for conducting security assessments periodically for all organizations within the supply chain.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Assessments should validate alignment with applicable industry standards as well as service and contract requirements.</td></tr>
</table>

2.16 Threat and Vulnerability Management (TVM)

<table>
<tr><td><b>Control Title:</b>
Threat and Vulnerability Management Policy and Procedures</td><td><b>Control ID:</b>
TVM-01</td><td><b>Control Specification:</b>
Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to identify, report and prioritize the remediation of vulnerabilities, in order to protect systems against vulnerability exploitation. Review and update the policies and procedures at least annually.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
A policy on threat and vulnerability management (TVM) should be established that includes the intent, purpose, and governance of how a CSP or CSC should address threats and vulnerabilities for their respective scope under the SSRM.

At a minimum, the policy should specify:
a. What should be covered under the scope, especially the need to comply with applicable laws, regulations, and contractual requirements.
b. The frequency of assessments.
c. The methods that should be used.
d. How and when assessments and significant vulnerabilities should be reported, including when it’s appropriate to share vulnerability information with customers and business partners.
e. How reports should be reviewed.
f. How actions to address relevant risks and opportunities should be tracked to closure.
g. Approval of CSP native and (where applicable) third-party data/asset protection capabilities and relevant services for use by appropriate CSC authorities.
h. A well-defined incident response process aligned with an organization’s risk tolerance, accompanied by appropriate communication and notifications.
i. Acceptable periods of remediation of threats in order of severity and criticality of computing infrastructure.
j. Log review and correlation procedures with appropriate threat intelligence capabilities for log, events, metrics, and incidents (preferably through a centralized service).</td></tr>
<tr><td><b>Control Title:</b>
Malware Protection Policy and Procedures</td><td><b>Control ID:</b>
TVM-02</td><td><b>Control Specification:</b>
Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect against malware on managed assets. Review and update the policies and procedures at least annually.</td></tr>
</table>

Implementation Guidelines:
Malware protection policies should focus on inspecting both inbound and outbound traffic and implementing controls to detect, prevent, block, and remove malware. Include expectations of time objectives for remediation programs that seek to ensure systems are free of infection when they connect to enterprise computing resources. Malware protection should be integrated across all computing infrastructure, including compute, network, endpoints, and secure access gateways.

Organizations should centrally manage malware protection mechanisms, including planning, implementing, assessing, authorizing, and monitoring organizational-defined malware protection security controls. This process will help to cohesively address malware within predefined timeframes.

Threat and vulnerability management policy should include the ability to address malware as a specific threat element. This should provide the organization with a guideline to handle malware using appropriate tools, relevant automation, and operational frameworks to meet their risk tolerance.

If malware is identified by antivirus or anti-malware applications using a signature- or behavior-based detection process, malware removal should be updated according to applicable contractual agreements and organizational standards. Additionally, prevention software and associated signatures should be deployed centrally by the service provider throughout their environment.

Control Title:	**Control ID:**	**Control Specification:**
Vulnerability Remediation Schedule	TVM-03	Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk.

Implementation Guidelines:
An integrated TVM system should be implemented that can maintain records of threats and vulnerabilities found over time and the result of their mitigation actions. The Integrated TVM system should be used to mitigate all future risks, by leveraging the previous experiences of the mitigation activities.

A full remediation schedule should be considered. The schedule should classify and prioritize vulnerabilities in order of their severity and threat to the environment, aligned to the expectations of TVM Policy.

Vulnerability remediation schedules should be approved and communicated to all relevant stakeholders (and included in SLA’s).

Control Title:	**Control ID:**	**Control Specification:**
Detection Specification	TVM-04	Define, implement and evaluate processes, procedures and technical measures to update detection tools, threat signatures, and indicators of compromise on a weekly, or more frequent basis.

Implementation Guidelines:
A rolling schedule of detection, reporting, and mitigation should be established so that all actions to address threats and non-conformance are performed on time and reported to the integrated TVM system for monitoring and oversight. In addition, where applicable, implement automation so that threats and non-conformance are mitigated on time.

Control Title:	**Control ID:**	**Control Specification:**
External Library Vulnerabilities	TVM-05	Define, implement and evaluate processes, procedures and technical measures to identify updates for applications which use third party or open source libraries according to the organization's vulnerability management policy.

Implementation Guidelines:
Where a CSC or a CSP uses third party or open source libraries, these should be tracked, scanned and reported on in the integrated TVM system. Installed or used packages, libraries and/or runtimes that are part of their solution with their running version should be included. TVM scans can be performed automatically and the findings should be promptly reported to the integrated TVM system. This activity should be monitored to avoid operational gaps.

The organization should leverage global threat intelligence about threat signatures and vulnerability databases that may contain indicators of attack and compromise. It should also consider implementing automated & recurring processes so that human errors can be avoided.

Control Title:	**Control ID:**	**Control Specification:**
Penetration Testing	TVM-06	Define, implement and evaluate processes, procedures and technical measures for the periodic performance of penetration testing by independent third parties.

Implementation Guidelines:
A formal schedule of red team exercises interspersed with risk assessments, remediation, and penetration testing aligned to the applicable service model (I-P-SaaS, and XaaS) should be established. Penetration testing should comply with all applicable laws and regulations.

A written and signed authorization should be obtained and verified before and after services are rendered. Penetration test schedules should be published on the integrated TVM system to ensure tactics, techniques, and test procedures adhere to documented policies.

Control Title:
Vulnerability Identification

Control ID:
TVM-07

Control Specification:
Define, implement and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organizationally managed assets at least monthly.

Implementation Guidelines:
The integrated TVM system should track vulnerabilities to closure and report them to build oversight of residual risks. Furthermore, the system should retain information that can be reused in future remediation activities.

Organizations should consider establishing an external-facing vulnerability disclosure program to allow external parties to communicate detected vulnerabilities.

Control Title:
Vulnerability Prioritization

Control ID:
TVM-08

Control Specification:
Use a risk-based model for effective prioritization of vulnerability remediation using an industry recognized framework.

Implementation Guidelines:
Vulnerabilities should be prioritized in terms of their relative risk, importance, organizational impact, and urgency. When evaluating impact, consider exposure levels to applicable threats from the organization's specific usage and/or implementation. When evaluating importance, consider the criticality and value of the affected assets. Finally, when assessing urgency, consider the Common Vulnerability Scoring System (CVSS) ratings and timeframes, the relevance to current and ongoing threats, and the effort required for remediation.

Control Title:
Vulnerability Management Reporting

Control ID:
TVM-09

Control Specification:
Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification.

Implementation Guidelines:
The integrated TVM system should have comprehensive vulnerability tracking capabilities. Capabilities should include when discoveries were made and remediated, systems impacted, reasons for the delay (where applicable), and any communications that may have been made to stakeholders.

Control Title:
Vulnerability Management Metrics

Control ID:
TVM-10

Control Specification:
Establish, monitor and report metrics for vulnerability identification and remediation at defined intervals.

Implementation Guidelines:
The integrated TVM system should be used to collect and report metrics about the vulnerability management program. Metrics should demonstrate the coverage, efficacy, and efficiency of o perational TVM activities.

2.17 Universal Endpoint Management (UEM)

Control Title:	**Control ID:**	**Control Specification:**
Endpoint Devices Policy and Procedures	UEM-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. Review and update the policies and procedures at least annually.

Implementation Guidelines:
Policies and procedures for both managed and unmanaged endpoints (including BYOD) should include the following components:

a. Definition of endpoints and the acceptable-use policy requirements for all endpoints (mobile devices, virtual, desktop, etc.). Note: Physical and virtual servers, containers, and similar “endpoints” are addressed in the DCS and IVS domains, while application and interface “endpoints” are discussed in the AIS domain.
b. List the approved systems, servers, applications, application stores, application extensions, and plugins that may be allowed for managed endpoint access and usage and/or enforced through enterprise management tools.
c. Policy and procedures related to installing non-approved applications or approved applications not obtained through a pre-identified application store.
d. Prohibit the circumvention of vendor-supported and integrated (built-in) security controls on endpoints (i.e., jailbreaking or rooting). Enforce these restrictions through detective and preventive controls on the endpoint, managed through a centralized system (e.g., an endpoint, system configuration control, or mobile device management system).
e. Policies regarding privacy expectations and requirements for remote location identification, litigation, e-discovery, and legal holds (especially for personally-owned devices).
f. Policies and procedures related to non-company data loss if a full or partial wipe of a device is required.
g. Performing policy reviews at planned intervals or upon significant organizational or environmental changes.

Policies and procedures should also integrate the following concepts (which may have applicable controls in other domains to consider):

h. Passcodes, biometric authentication, idle/no-use screen locks, and logouts.
i. The use of anti-malware software.
j. The use of encryption for the entire device or data identified as non-public on all endpoints (enforced through technology controls).
k. Each endpoint device should be assigned to a named person who is responsible for it. Such devices may be shared (e.g., in shared work areas), but a single individual should still be assigned responsibility for it.
l. Non-device endpoints should also have “owners” responsible for assessing risks and ensuring appropriate controls.
m. Endpoints should be vetted for policy compliance before being provisioned for organizational use.

<table>
<tr><td>**Control Title:**
Application and Service Approval</td><td>**Control ID:**
UEM-02</td><td>**Control Specification:**
Define, document, apply and evaluate a list of approved services, applications and sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data.</td></tr>
<tr><td colspan="3">**Implementation Guidelines:**
For managed endpoints, universally enforce policies through one or more centralized configuration management tools.

Use risk assessment to determine what (if any) information or systems may be accessed or stored using unmanaged endpoints.</td></tr>
<tr><td>**Control Title:**
Compatibility</td><td>**Control ID:**
UEM-03</td><td>**Control Specification:**
Define and implement a process for the validation of the endpoint device compatibility with operating systems and applications.</td></tr>
<tr><td colspan="3">**Implementation Guidelines:**
The company should have a documented application validation process to test for compatibility issues regarding mobile devices, operating systems, and applications.

Misconfigured endpoints will not only impact operations but will also introduce attack vectors. Poor configuration settings could involve open ports, outdated exceptions, insecure protocols allowed, etc. Any configuration changes once in production should follow change management guidelines (why, what, how) and require appropriate approvals.</td></tr>
<tr><td>**Control Title:**
Endpoint Inventory</td><td>**Control ID:**
UEM-04</td><td>**Control Specification:**
Maintain an inventory of all endpoints used to store and access company data.</td></tr>
<tr><td colspan="3">**Implementation Guidelines:**
All organizational endpoint systems should be identified and protected. In addition, a policy against the inventory should be established and documented (including scan type, number of scans, schedule, and exceptions/exclusions).

An inventory of all mobile devices used to store and access company data should be kept and maintained. Include all device status changes (i.e., operating system, patch levels, lost/decommissioned status, and to whom the device is assigned or approved for usage [BYOD]) in the inventory.

A documented list of approved application stores should be defined as acceptable for mobile devices accessing or storing provider-managed data.</td></tr>
</table>

<table>
<tr><td><b>Control Title:</b>
Endpoint Management</td><td><b>Control ID:</b>
UEM-05</td><td><b>Control Specification:</b>
Define, implement and evaluate processes, procedures and technical measures to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
For managed endpoints, universal policy enforcement through one or more centralized configuration management tools is essential. Note: “Universal” enforcement is not necessarily “unified.” Some vendors claim to offer “unified endpoint management” systems, but none are truly capable of managing all security features of all endpoint types.

For unmanaged endpoints, guidance should be provided but will not be enforced (by definition).

Based on risk assessment, different configurations may be acceptable for systems access and/or information storage—resulting in various degrees of end-points management with different access requirements. These may include using container technology for sensitive data isolation. For example, an organization that prohibits using electronic mail for sensitive information may determine that access to company electronic mail using a personally-owned device requires only limited controls (such as an acceptable passcode, a lock screen, reasonably up-to-date software, and no circumvention of vendor security controls [such as jailbreaking or rooting]).</td></tr>
<tr><td><b>Control Title:</b>
Automatic Lock Screen</td><td><b>Control ID:</b>
UEM-06</td><td><b>Control Specification:</b>
Configure all relevant interactive-use endpoints to require an automatic lock screen.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
The organization should implement this requirement through technical controls for all interactive-use endpoints.</td></tr>
<tr><td><b>Control Title:</b>
Operating Systems</td><td><b>Control ID:</b>
UEM-07</td><td><b>Control Specification:</b>
Manage changes to endpoint operating systems, patch levels, and/or applications through the company’s change management processes.</td></tr>
</table>

Implementation Guidelines:
The organization should consider the following points:

a. Changes should be managed strictly and consistently.
b. Formal management responsibilities and procedures should facilitate satisfactory control of all changes to endpoint operating systems, patch levels, and/or applications, including:
    1. The identification and recording of significant changes.
    2. The planning and testing of changes.
    3. The assessment of the potential impacts (including security impacts) of such changes.
    4. The formal approval for proposed changes.
    5. The communication of change details to all respective stakeholders.

Fallback procedures and responsibilities should be defined and implemented, including guidelines for aborting and recovering from unsuccessful changes and unforeseen events.

Control Title:	Control ID:	Control Specification:
Storage Encryption	UEM-08	Protect information from unauthorized disclosure on managed endpoint devices with storage encryption.

Implementation Guidelines:
To minimize data leak risks and protect data stored on the endpoint device, use encryption. Encryption capabilities could be part of common endpoint solutions such as DLP, endpoint firewalls, and PAM. Additionally, they could be standalone (e.g., device container technology, file encryption, and full-disk encryption). The encryption strength should be based on the sensitivity of the data being protected.

Endpoint device policies should use encryption for the entire device or data identified as sensitive on all mobile devices (potentially using container technology). This policy should be enforced through technology controls.

Control Title:	Control ID:	Control Specification:
Anti-Malware Detection and Prevention	UEM-09	Configure managed endpoints with anti-malware detection and prevention technology and services.

Implementation Guidelines:
Organizations should consider the following:

a. Managed endpoints should be protected through anti-malware software, security awareness, appropriate system access, and change management controls.
b. Organizations should have formal policies and technologies implemented to install and upgrade protective measures promptly. These measures include installing and regularly updating anti-malware software and virus definitions (automatically) and whenever updates are available. Additionally, organizations should periodically review and scan installed software and system data content to identify and remove unauthorized software (when possible).

c. Wherever possible, organizations should also:

   1. Disable universal serial bus (USB) ports.
   2. Prohibit writable media use (e.g., DVD-R).
   3. Restrict read-only media (e.g., DVD-ROM) used to legitimate commercial sources for legitimate business reasons (e.g., Linux installation disks) and allow only whitelisted software to run on the endpoint.

d. Employ anti-malware software that offers a centralized infrastructure that compiles information on file reputations or has administrators manually push updates to all machines. After updating, automated systems should verify that each system has received its signature update.

e. Define procedures to respond to malicious code or unauthorized software identification. Checking antivirus or anti-spyware software generates audit logs of checks performed. Malicious code detection and repair software checks to scan computers and media include:

   1. Checking files on electronic or optical media and files received over networks for malicious code before use.
   2. Checking electronic mail attachments and downloads for malicious code or file types that are unnecessary for organizational business before use. This check occurs at different places (e.g., electronic mail servers, desktop computers, and when entering the organization's network).
   3. Checking web traffic—such as hypertext markup language (HTML), JavaScript, and hypertext transfer protocol (HTTP)—for malicious code.
   4. Checking removable media (e.g., USB tokens and hard drives, CDs/DVDs, FireWire devices, and external serial advanced technology attachment devices) when inserted.

f. Have formal policies to prohibit using or installing unauthorized software, including restricting on obtaining data and software from external networks. User awareness and training on these policies and methods should be provided for all users regularly.

g. Bring your own device (BYOD) users should use anti-malware software (where supported).

Control Title:	**Control ID:**	**Control Specification:**
Software Firewall	UEM-10	Configure managed endpoints with properly configured software firewalls.

Implementation Guidelines:
All managed endpoints should properly configure endpoint firewalls to inspect traffic, apply rules, and perform behavioral monitoring. These firewalls will protect the endpoint from malware and attacks originating from inside or outside the corporate network. For example, a web application firewall (WAF) should be used to protect web services from malicious attacks (e.g., structured query language (SQL) injection).

Control Title:	**Control ID:**	**Control Specification:**
Data Loss Prevention	UEM-11	Configure managed endpoints with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment.

<table>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
The organization should have a DLP program to discover, monitor, and protect data with regulatory or compliance implications in transit and at rest across the network, storage, and endpoint systems.

The DLP solution should monitor and control the data flow. Furthermore, any anomalies that exceed normal traffic patterns should be noted, and appropriate action should be taken to address them.

The DLP solution should also be used to monitor for sensitive information (e.g., personally identifiable information), keywords, and metadata in order to discover unauthorized attempts for their disclosure across network boundaries and block such transfers by alerting information security personnel.

The organization should configure the DLP solution to enforce ACLs even when data is copied off a server.</td></tr>
<tr><td><b>Control Title:</b>
Remote Locate</td><td><b>Control ID:</b>
UEM-12</td><td><b>Control Specification:</b>
Enable remote geo-location capabilities for all managed mobile endpoints.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Remote management controls—such as remote data wipe, anti-tampering, and geotracking—should be implemented around endpoint devices to protect if a device is lost or stolen.

All mobile devices (permitted through the company BYOD program or a company-assigned mobile device) should allow for remote wipe by the company's corporate IT—or have all company-provided data wiped by its corporate IT.</td></tr>
<tr><td><b>Control Title:</b>
Remote Wipe</td><td><b>Control ID:</b>
UEM-13</td><td><b>Control Specification:</b>
Define, implement and evaluate processes, procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices.</td></tr>
<tr><td colspan="3"><b>Implementation Guidelines:</b>
Define, implement and evaluate processes, procedures, and technical measures to enable the deletion of company data remotely on managed endpoint devices, such as when a device is lost or stolen. Only rarely should the network administrator or device owner issue the remote wipe command since it is potentially destructive and removes all content until the device returns to its factory state.</td></tr>
<tr><td><b>Control Title:</b>
Third-Party Endpoint Security Posture</td><td><b>Control ID:</b>
UEM-14</td><td><b>Control Specification:</b>
Define, implement and evaluate processes, procedures and technical and/or contractual measures to maintain proper security of third-party endpoints with access to organizational assets.</td></tr>
</table>

Implementation Guidelines:

The organization should perform due diligence before granting third party access to the organization's data or establishing connectivity (and periodically thereafter, commensurate with the risk level of the third-party relationship).

Written agreements (contracts) should be maintained and include an acknowledgment that the third party is responsible for the security of the data the third party possesses or otherwise stores, processes, or transmits on the organization's behalf. In addition, agreements should include requirements to address the information security risks associated with information and communications technology services (e.g., cloud computing services) and the product supply chain. These requirements are subsequently applicable to relevant, third-party (i.e., fourth parties) subcontractors (and so on) throughout the supply chain.

Personnel security requirements should be established and documented—including security roles and responsibilities for third-party providers coordinated and aligned with internal security roles and responsibilities. Monitor providers for compliance.

Additionally, the organization should have a screening process for contractors and third-party users. When organizations provide contractors, the contract should specify the organization's responsibilities for screening and relevant notification procedures if screening has not been completed (or if the results cause doubts or concerns). Similarly, third-party agreements should specify all responsibilities and notification procedures for screening.

Third-party providers should notify a designated individual or role (e.g., a member of the contracting or supply chain function) of any personnel transfers or terminations of third-party personnel who possess organizational credentials, badges, or have information system privileges.

Formal contracts should be employed that, at a minimum, specify:

a. The covered information's confidential nature and value.
b. The security measures to be implemented and/or complied with. These include the organization's information security requirements and appropriate controls required by applicable federal laws, executive orders, directives, policies, regulations, standards and guidance, and third-party access limitations.
c. The service levels to be achieved in the services provided.
d. The format and frequency of reporting to the organization's information security management forum.
e. The arrangement for representation of the third party in appropriate organizational meetings and working groups.
f. The arrangements for third-party compliance auditing.
g. The penalties exacted if any of the preceding specifications fail.

Mutually agreed-upon provisions and/or terms should be established to satisfy customer (tenant) requirements for service-to-service application (API), information processing interoperability, portability for application development and information exchange, usage, and integrity persistence.

Acronyms

ABAC	Attribute Based Access Control
AICPA	Association of International Certified Professional Accountants
API	Application Programming Interface
ARP	Address Resolution Protocol
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BLE	Bluetooth Low Energy
BYOK	Bring Your Own Key
CAIQ	Consensus Assessments Initiative Questionnaire
CASB	Cloud Access Security Broker
CIS	Center for Internet Security
CKL	Compromised Key List
CKMS	Cryptographic Key Management System
CRL	Certificate Revocation List
CSC	Cloud Service Customer
CSP	Cloud Service Provider
COSO	Committee of Sponsoring Organization
DAST	Dynamic Application Security Testing
DDoS	Distributed Denial of Service Attack
DLP	Data Loss Prevention
DPIA	Data Protection Impact Assessment
DR	Disaster Recovery
EMI	Electro-Magnetic Interference
ERM	Enterprise Risk Management
FEDRAMP	Federal Risk and Authorization Management Program
FIM	File Integrity Monitoring
HIPAA	Health Insurance Portability and Accountability Act
HSM	Hardware Security Module
IDaaS	Identity as a Service
IDE	Integrated Development Environment
IDS	Intrusion Detection Systems
IaaS	Infrastructure as a Service
IAST	Interactive Application Security Testing
ICMP	Internet Control Message Protocol
IPS	Intrusion Prevention Systems
ISO/IEC	International Organization for Standardization and the International Electrotechnical Commission
ITIL	Information Technology Infrastructure Library
KPI	Key Performance Indicators
KRI	Key Recovery Information
MFA	Multi Factor Authentication
NIST	National Institute of Standards and Technology
OS	Operating System

OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PAM	Privileged Access Management
PII	Personally Identifiable Information
PPTP	Point-to-Point Tunneling Protocol
RBAC	Role Based Access Controls
RBG	Random Bit Generators
ROI	Return on Investment
RPO	Recovery Point Objective
RTO	Return Time Objective
SaaS	Software as a Service
SAST	Static Application Security Testing
SCA	Software Composition Analysis
SDK	Software Development Kit
SDLC	System Development Life Cycle
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SLO	Service Level Objectives
SME	Subject Matter Expert
SSDLC	Secure Software Development Lifecycle
SSH	Secure Shell
SSL	Secure Sockets Layer
SSRM	Shared Security Responsibility Model
TPRM	Third Party Risk Management
vTPM	Virtual Trusted Platform Module
VDP	Vulnerability Disclosure Program
XaaS	Anything as a Service

Glossary

Acceptable use policy
Set of rules applied by the owner, creator or administrator of a network, website, or service, that restrict the ways in which the network,website or system may be used and sets guidelines as to how it should be used.

Accountability
The ability to map a given activity or event back to the responsible party.

AICPA TSC 2017
Trust Services Criteria for security, availability, processing integrity, confidentiality and privacy.

Algorithm
A mathematical function that is used in the encryption and decryption processes.

Anonymization
Data anonymization is the process of protecting private or sensitive information by erasing or encrypting identifiers that connect an individual to stored data.

Asset
An item that has a value to an organization that is tangible (e.g., a physical item such as hardware, firmware, computing platform, network device, or other technology components) or intangible (e.g., employees, data, information, software, trademarks, copyrights, intellectual property, image), including a virtual computing platform (common in cloud and virtualized environments), and related hardware (e.g., cabinets, computers, keyboards).

Assessments
The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system—Generally, the purpose of an assessment is to get a snapshot of the current reality of your organization.

Auditing
The independent assessment conducted by a qualified assessor of the conformity of the internal and external (cloud) processes within the scope of the applicable regulatory requirements, organizational policies and/or standard requirements.

Availability
Property of being accessible and usable upon demand by an authorized entity.

Breach
The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information.

Bug Bounty
An IT term for a reward or bug bounty program given for finding and reporting bugs in software products.

Capabilities
Reinforcing security and privacy controls implemented by technical, physical, and procedural means.

Certification
The provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements.

CI/CD Pipeline
A series of steps that involves continuous automation and monitoring to deliver new versions of software. The steps that form a CI/CD pipeline are distinct subsets of tasks that typically include build, test, release, deploy, and validate.

Cloud auditor
Cloud service partner with the responsibility to conduct an audit of the provision and use of cloud services.

Cloud Computing
Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

Cloud customer
A person or organization that is a customer of a cloud; note that a cloud customer may itself be a cloud and that clouds may offer services to one another.

Cloud service provider
Party which makes cloud services available.

Compensating control
An internal control that reduces the risk of an existing or potential control weakness resulting in errors and omissions.

Compliance
Adherence to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations, as well as voluntary requirements resulting from contractual obligations and internal policies.

Confidentiality
Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Container
A method for packaging and securely running an application within an application virtualization environment. Also known as an application container or a server application container.

Continuous assurance/compliance
The combination of continuous auditing and continuous monitoring.

Continuous audit
An on-going assessment process that aims to determine the fulfilment of Service Qualitative Objectives (SQOs) and Service Level Objectives (SLOs), conducted at a frequency requested by the purpose of audit.

Control framework
A set of fundamental controls that facilitates the discharge of business process owner responsibilities to prevent financial or information loss in an enterprise.

Controls
Controls are intended to reduce the frequency or impact of realized risk.

Cryptographic algorithm
A cryptographic checksum is created by performing a complicated series of mathematical operations (known as a cryptographic algorithm) that translates the data in the file into a fixed string of digits called a hash value, which is then used as the checksum.

CSA Enterprise Architecture
It is a high-level conceptual model that includes a methodology and a set of tools. It enables security architects, enterprise architects and risk management professionals to assess the status of their internal IT and cloud providers in terms of security capabilities, and it helps them create a road map to meet the security needs of their business. The CSA EA identifies a comprehensive set of functional capabilities and processes grouped in domains. The actions included in each domain are based on best-practice architecture frameworks.

CSA Security Guidance
The fourth version of the Security Guidance for Critical Areas of Focus in Cloud Computing is built on previous iterations of the security guidance, dedicated research, and public participation from the Cloud Security Alliance members, working groups, and the industry experts within our community. This version incorporates advances in cloud, security, and supporting technologies; reflects on real-world cloud security practices; integrates the latest Cloud Security Alliance research projects; and offers guidance for related technologies.

Defense-in-depth
Information security approach in which a series of security mechanisms and controls are defined in a layered approach to protect confidentiality, integrity, and availability.

DevSecOps
An augmentation of DevOps to allow for the integration of security practices in the DevOps approach.

Digital signature
A piece of information, a digitized form of signature, that provides sender authenticity, message integrity and non-repudiation. A digital signature is generated using the sender's private key or applying a one-way hash function.

Disaster Recovery (DR)
Disaster recovery (DR) is the technical component of BCP and focuses on the continuity of information and communication technology systems that support business functions.

Due diligence
The performance of those actions that are generally regarded as prudent, responsible and necessary to conduct a thorough and objective investigation, review and/or analysis.

Dynamic application security testing
A set of tools used to test software during operation and provide feedback on compliance and general security issues. DAST tools are typically used during the testing and QA phase.

Encryption
The process of transforming plaintext into ciphertext using a cryptographic algorithm and key.

Endpoint devices
An endpoint device is the most remote element at the end of the network. These are computers or simple input devices such as laptops, desktops, tablets, mobile phones, Internet-of-things devices, servers, virtual environments, etc., operated by humans, remotely managed or fully automated devices collecting information or responding to commands issues from centralized control points.

Endpoint security
Endpoint security or endpoint protection is an approach to the protection of computer networks that are remotely bridged to client devices.

Enterprise
An organization with a defined mission/goal and a defined boundary, using systems to execute that mission, and with responsibility for managing its own risks and performance.

Enterprise risk management
A process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance.

Fault Tolerance
Refers to the ability of a system (computer, network, cloud cluster, etc.) to continue operating without interruption when one or more of its components fail.

Framework
Provides a common organizing structure for multiple approaches by assembling standards, guidelines, and practices that are working effectively today.

Fuzzing
Fuzz testing or Fuzzing is a Black Box software testing technique, which basically consists in finding implementation bugs using malformed/ semi-malformed data injection in an automated fashion.

General Data Protection Regulation (GDPR)
The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas.

Governance
Ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives.

Governance framework
A framework is a basic conceptual structure used to solve or address complex issues. An enabler of governance. A set of concepts, assumptions and practices that define how something can be approached or understood, the relationships amongst the entities involved, the roles of those involved, and the boundaries (what is and is not included in the governance system).

Hybrid cloud
The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Incident
An occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Incident response
The mitigation of violations of security policies and recommended practices.

Incident response plan
The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's information systems(s)

Identity and access management (IAM)
A framework of policies and technologies for ensuring that the proper people in an enterprise have the appropriate access to technology resources.

Information security
Preservation of confidentiality, integrity, and availability of information.

Infrastructure as a Service (IaaS)
The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

Integrity
Property of accuracy and completeness.

Internet of Things (IoT)
Network of physical objects—"things"—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet.

Interoperability
A characteristic of a product or system, whose interfaces are completely understood, to work with other products or systems, at present or in the future, in either implementation or access, without any restrictions.

Jericho Forum
An international IT security thought-leadership group dedicated to defining ways to deliver effective IT security solutions.

Jurisdictions
Authority granted to a legal body to administer justice, as defined by the kind of case, and the location of the issue.

Key management
Dealing with the generation, exchange, storage, use, crypto-shredding (destruction) and replacement of keys.

Legacy environment
Environments that are on premises of the organization and not in the cloud.

Malware
Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

Maturity
Indicates the degree of reliability or dependency or capability that the business can place on a process achieving the desired goals or objectives.

Metadata
Describes data and gives information about other data.

NIST SP 800-53
Security and Privacy Controls for Federal Information Systems and Organizations.

On premises
On-premises software (commonly misstated as on-premise, and alternatively abbreviated "on-prem") is installed and runs on computers on the premises of the person or organization using the software, rather than at a remote facility such as a server farm or cloud.

Patch management
An area of systems management that involves acquiring, testing and installing multiple patches (code changes) to an administered computer system in order to maintain up-to-date software and often to address security risk.

PCI DSS
The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes.

Penetration testing
A method of testing where testers target individual binary components or the application as a whole to determine whether intra or inter component vulnerabilities can be exploited to compromise the application, its data, or its environment resources.

Phishing
A technique for attempting to acquire sensitive data, such as bank account numbers, or access to a larger computerized system through a fraudulent solicitation in email or on a web site. The perpetrator typically masquerades as a legitimate business or reputable person.

Physical controls
Describe anything tangible that's used to prevent or detect unauthorized access to physical areas, systems, or assets.

Platform as a Service (PaaS)
The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.

Policy
Generally, a document that records a high-level principle or course of action that has been decided on.

Portability
The ability of a computer program to be ported from one system to another.

Private cloud
The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Procedure
A document containing a detailed description of the steps necessary to perform specific operations in conformance with applicable standards. Procedures are defined as part of processes.

Process
Set of interrelated or interacting activities which transform inputs into outputs.

Proof-of-Possession
Provides the means of proving that a party sending a message is in possession of a particular cryptographic key.

Proxy
An application that "breaks" the connection between client and server. Public cloud—1) The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Pseudonymization
It is a data management and de-identification procedure by which personally identifiable information fields within a data record are replaced by one or more artificial identifiers, or pseudonyms.

RACI-style matrix
Illustrates who is Responsible, Accountable, Consulted and Informed within an organizational framework.

Ransomware
A type of malware that attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid.

Regulation
Rules or laws defined and enforced by an authority to regulate conduct.

Remediation
After vulnerabilities are identified and assessed, appropriate remediation can take place to mitigate or eliminate the vulnerability.

Residual risk
The remaining risk after management has implemented a risk response.

Resilience
The ability of an information system to operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities, and to recover to an effective operational posture in a time frame consistent with mission needs.

Risk
Effect of uncertainty on objectives.

Risk appetite
The amount of risk, on a broad level, that an entity is willing to accept in pursuit of its mission.

Risk assessment
A process used to identify and evaluate risk and its potential effects.

Risk management
The coordinated activities to direct and control an enterprise with regard to risk.

Risk profile
The amount of risk that is involved in an investment.

Risk register
A repository of the key attributes of potential and known IT risk issues. Attributes may include name, description, owner, expected/actual frequency, potential/actual magnitude, potential/actual business impact, disposition.

Risk tolerance
The acceptable level of variation that management is willing to allow for any particular risk as the enterprise pursues its objectives.

Sandbox
Is a testing environment that isolates untested code changes and outright experimentation from the production environment or repository, in the context of software development including Web development and revision control.

Serverless computing
A flexible "pay-as-you-go" cloud computing execution model in which the cloud provider runs the server and dynamically manages the allocation of machine resources. Pricing is based on the amount of actual resources consumed by an application, so the developers pay only for the backend services they use.

Service level agreement (SLA)
An agreement, preferably documented, between a service provider and the customer(s)/user(s) that defines minimum performance targets for a service and how they will be measured.

Shadow IT
Refers to IT devices, software and services outside the ownership or control of IT organizations.

Shared responsibility model
The compliance responsibility between the cloud customer and the cloud service provider based on the degree of control each party has over the architecture stack.

Software as a Service (SaaS)
The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.

Software development life cycle (SDLC)
Software development life cycle (SDLC) is composed of the phases deployed in the development or acquisition of a software system.

Stakeholders
Anyone who has a responsibility for, an expectation from or some other interest in the enterprise.

Standards
Metrics, allowable boundaries or the process used to determine whether procedures meet policy requirements.

STAR Program
The Security Trust Assurance and Risk (STAR) Program encompasses key principles of transparency, rigorous auditing, and harmonization of standards.

Static application security testing
A set of technologies designed to analyze application source code, byte code and binaries for coding and design conditions that are indicative of security vulnerabilities. SAST solutions are typically used during the development phase.

Technical controls
(Also known as logical controls) include hardware or software mechanisms used to protect assets.

Third party
1) An outside source from the internal company
2) A third person or organization less directly involved in a matter than the main people or organizations that are involved.

Threat
Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Threat modeling
A process by which potential threats or the absence of appropriate safeguards, can be identified, enumerated, and mitigations can be prioritized.

Virtualization
The simulation of the software and/or hardware upon which other software runs.

Virtual Machine Lifecycle Management (VMLM)
It is a set of processes designed to help administrators oversee the implementation, delivery, operation, and maintenance of virtual machines (VMs) over the course of their existence.

Vulnerability management
An Information Security Continuous Monitoring (ISCM) capability that identifies vulnerabilities [Common Vulnerabilities and Exposures (CVEs)] on devices that are likely to be used by attackers to compromise a device and use it as a platform from which to extend compromise to the network.

Vulnerability
A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events.

Web application
Application software that runs on a web server, unlike computer-based software programs that are stored locally on the Operating System (OS) of the device.