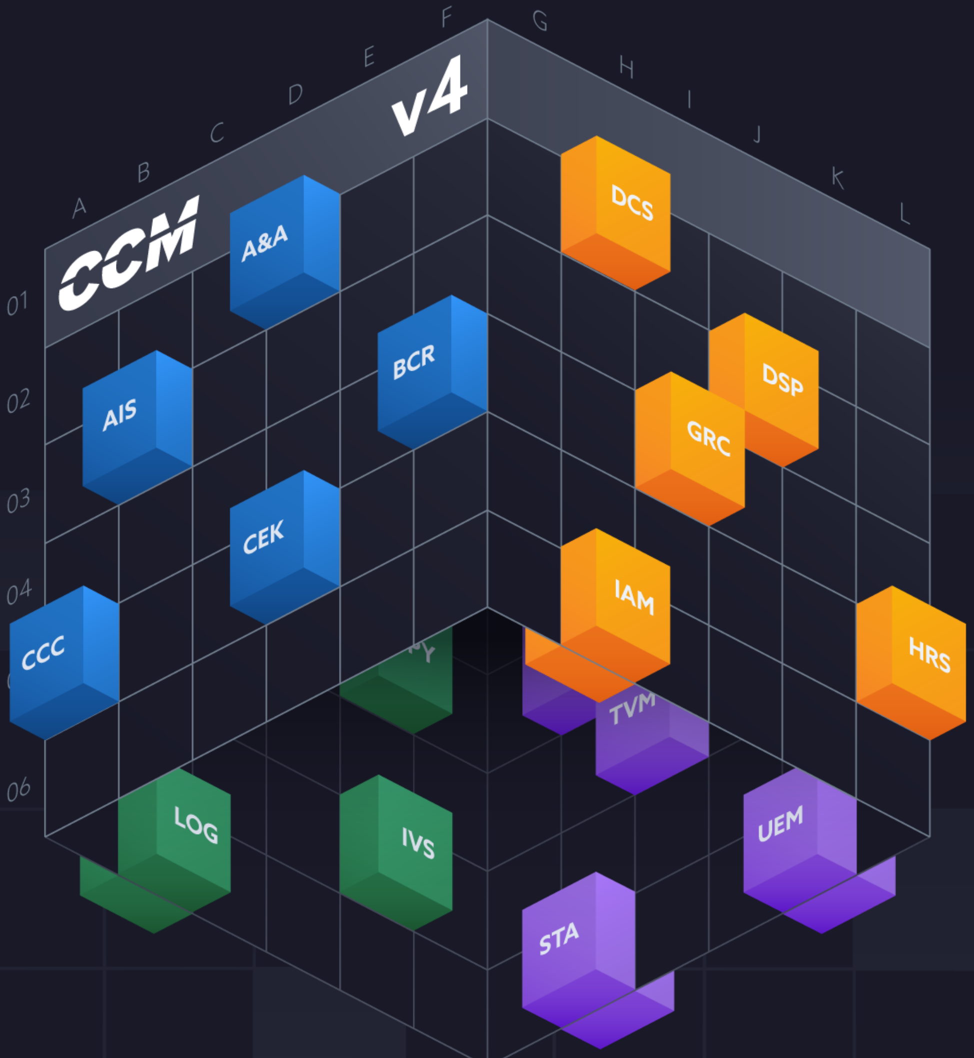
CCM v4.0 Auditing Guidelines



cloud security alliance®

About the CCM Working Group

The CCM WG comprises professionals from the cloud industry, 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 and the Auditing Guidelines is the result of a collective work that is built on the experience and feedback collected from the group and is meant to provide the community with one of the best vendor-neutral cloud security and privacy control frameworks.

The activities of the WG are supervised by co-chairs, who are highly experienced professionals, representing 3 roles in the cloud industry, the Cloud Service Provider (CSP), the Cloud Service Consumer (CSC) and Cloud auditor.

Acknowledgments

Lead Authors:

Sanjeev Gupta (Team Lead)
Parminder Bawa
Renu Bedi
Damian Heal
Jan Jacobsen
Bilal Khattak
David Nickles
Agnidipta Sarkar
Steve Sparkes
Tanya Tipper-Luster
Ashish Vashishtha

Contributors:

Brian Dorsey
Angell Duran
Joel John
Erik Johnson
John D. Maria
Claus Matzke
Vani Murthy
Michael Roza

CCM Leadership:

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

CSA Global Staff:

Claire Lehnert (Design)
Stephen Lumpe (Cover)

Table of Contents

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)[2], with transparency and accountability across the entire supply chain to operationalize this crucial concept.

The Cloud Security Alliance's Cloud Controls Matrix Version 4[3] (CCM v4.0), published in 2021, includes core security and privacy controls and additional components. These include the CCM Controls Implementation Guidelines, the CCM Auditing Guidelines (included in this document), and the Consensus Assessment Initiative Questionnaire[4] (CAIQ). The CCM v4.0 also includes useful supporting information for CCM controls. This information includes typical SSRM control ownership assignments, 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 Auditing Guidelines are a new addition to CCM v4.0 and aim to provide auditors with a baseline understanding of the Cloud Controls Matrix (CCM) audit areas, allowing them to perform a CCM-related audit and assessment. These guidelines are intended to support cloud security audits or assessments (either internal or external) of organizations of any size, business, cloud deployment complexity and maturity.

This document is not meant to be a "how-to" manual for the CCM controls assessment, and therefore, auditors will need to customize the descriptions, procedures, risks, controls and documentation to address the specific objectives of the audit. The CSA cannot provide detailed, prescriptive audit guidance pertinent to every organization and cloud service implementation, but does offer general guidance on these activities.

The CCM Auditing Guidelines are a collaborative product of the volunteers in the CCM Working Group with experience in the auditing of cloud services and CCM controls implementation in many types of organizations.

[1] https://cloudsecurityalliance.org/research/guidance/, accessed on 10/22/21.

[2] https://cloudsecurityalliance.org/artifacts/ccm-v4-0-implementation-guidelines/ (see guidance for CCMv4 controls STA-01 to STA-06), accessed on 10/22/21.

[3] https://cloudsecurityalliance.org/research/cloud-controls-matrix/ , accessed on 10/22/21.

[4] https://cloudsecurityalliance.org/artifacts/star-level-1-security-questionnaire-caiq-v4/ , accessed on 10/22/21.

1. Introduction

This section provides a brief introduction to the purpose and scope of the CCM auditing guidelines, and their use in a CCM-based audit from the SSRM standpoint.

An elaborated introduction to the Cloud Control Matrix v4, its security domains and its underlying components can be found in the CCMv4 implementation guidelines[5] documentation.

1.1. Purpose and Scope

The document contains a set of auditing guidelines that are tailored to the control specifications for each of the 17 cloud security domains of the Cloud Control Matrix version 4 (CCMv4.0). The guidelines represent a new component for CCMv4.0 and did not exist previously in CCMv3.0.1.

The Auditing Guidelines (AGs) are intended to facilitate and guide a CCM audit. To achieve that, auditors are provided with a set of assessment guidelines per CCMv4.0 control specification with an objective to improve the controls' implementation auditability and help organizations to more efficiently achieve compliance (with either internal or external 3rd party cloud security audits).

The auditing guidelines are neither exhaustive nor prescriptive in nature, but rather represent a generic guide in form of recommendations for assessment. Auditors will need to customize the descriptions, procedures, risks, controls and documentation and tailor these to the audit work programs for the organization and service(s) in scope of the assessment, in order to address the specific objectives of an audit.

The CCMv4.0 Auditing Guidelines found in this document constitute an extension to the work that appears in the CCAK guide[6] and its Chapter 7: CCM Auditing Guidelines, and specifically of subsection 7.5: CCM Audit Workbook.

1.2. CCM Compliance Audit Documentation

CCM compliance audits should focus on evaluating the auditee's proper implementation and operation of the CCM V4 controls. The scope of the audit should include the controls that are, in whole or in part, under the responsibility of the auditee (for reference see STA-06).

CCM compliance audits should start by assembling evidence of the process flow; Security, privacy, data integrity, contractual clarity and protections, business continuity, process and system reliability, effectiveness/efficiency of new business processes, configuration management, compliance with cross-jurisdictional for privacy and regulations, etc. as well as the SSRM control applicability and implementation summary documentation as appropriate for the specific audit subject and their role, e.g., as a CSP or CSC.

[5] https://cloudsecurityalliance.org/artifacts/ccm-v4-0-implementation-guidelines/, accessed on 11/15/21.

[6] https://cloudsecurityalliance.org/education/ccak/, accessed on 6/7/21.

- For CSPs, a fully completed Consensus Assessment Initiative Questionnaire v4 (CAIQv4) will generally be a good starting point. Completed CAIQ questionnaires can be published in the CSA's Security, Trust, Assurance, and Risk (STAR) Registry and/or provided directly 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 template, but most organizations will have some form of CCM compliance documentation that should incorporate SSRM customer security responsibilities as delineated by the CSP. CSCs will often 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., by adding additional columns to the standard artifacts. Alternatively, they may have an internal GRC application where they assemble similar information from which appropriate reports can be generated for audit purposes.

In addition to the risk assessment and high level SSRM control implementation summary information, more detailed supporting documentation (e.g., process and procedure documentation, evidence of compliance) should be requested and assembled for specific control domains and individual controls as appropriate based on the detailed guidelines elaborated in this document as well as the auditor's detailed approach and professional methodology. This should include, but not limited to, a risk assessment, risk treatment and a Security Impact Analysis (SIA)[7].

1.3. Key Assumptions

Users of this document should tailor the guidelines with the methodology that suits the needs of the auditee. Auditors should take into consideration the guidance and requirements of ISO19001 and ISO27001, where applicable. In particular, attention is drawn to the need for auditors to verify that a process exists for handling records of non-compliance or exceptions and the associated remediation steps. Additionally, where review of policies are required "at least annually", auditors should consider, and if necessary communicate to auditee, the risks of not reviewing upon significant changes.

1.4. Target Audience

The target audience includes auditors who plan to perform audits against CCM on cloud service providers (CSPs), cloud service customers (CSCs) using the CCM framework to evaluate their cloud service portfolio, and CSPs or CSCs that intend to use the CCM framework to guide the design, development and implementation of their cloud security controls.

1.5. Versioning

This document includes the first draft edition of the CCMv4.0 auditing guidelines and it is marked as version 1.0.

[7] SIA is a process as part of the change control to determine the effect(s) a proposed change can cause to the security posture. By using "process auditing" the auditor should see a direct link between all the connected processes and be able to gauge the effectiveness of the security system

2. Auditing Guidelines

2.1 Audit & Assurance (A&A)

Control Title Audit and Assurance Policy and Procedures	**Control ID** A&A-01	**Control Specification** 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.
Auditing Guidelines 1. Examine policy and procedures to confirm content adequacy in terms of purpose, authority and accountability, responsibilities, planning, communication, reporting, and follow-up. 2. Examine audit charter and determine if independence, impartiality, and objectivity are guaranteed. 3. Examine policy and procedures for evidence of review at least annually.		
Control Title Independent Assessments	**Control ID** A&A-02	**Control Specification** Conduct independent audit and assurance assessments according to relevant standards at least annually.
Auditing Guidelines 1. Examine the process to determine standards and regulations applicable to the organization's systems and environments. 2. Determine if the organization maintains and reviews a list of such standards and regulations. 3. Determine if senior management exercises oversight over the independence of the assessment process. 4. Determine if the audit plan is informed by previous assessments, and is scheduled on an annual basis.		
Control Title Risk Based Planning Assessment	**Control ID** A&A-03	**Control Specification** Perform independent audit and assurance assessments according to risk-based plans and policies.
Auditing Guidelines 1. Examine the process for determining the risks applicable to the organization's systems and environments. 2. Determine if a list of such risks is maintained and reviewed. 3. Determine if senior management exercises oversight over the applicable risks. 4. Determine if the audit plan is risk-based, and is scheduled on an annual basis.		

Control Title	Control ID	Control Specification
Requirements Compliance	A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.

Auditing Guidelines

1. Examine the process for determining the standards and regulations applicable to the organization's systems and environments.
2. Examine the process to determine contractual, legal, and technical requirements applicable to the organization's systems and environments.
3. Determine if the organization maintains and reviews a list of relevant standards, regulations, legal/contractual, and statutory requirements.
4. Determine if senior management exercises oversight over this control specification.
5. Determine if the audit plan is informed by the list of the organisation's requirements.

Control Title	Control ID	Control Specification
Audit Management Process	A&A-05	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.

Auditing Guidelines

1. Examine policy related to the establishment and conduct of audits.
2. Determine if audit programs are established and aligned to the requirements of the organization, including the audit charter.
3. Determine if the organization upholds the independence of the audit program.
4. Determine if the conduct of audits is defined, approved at the appropriate level, and reviewed for effectiveness.

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.

Auditing Guidelines

1. Examine if the outputs of audits are defined by the policy.
2. Determine if the audit findings are reviewed and if appropriate reports are made available to users and senior management.
3. Determine if the identification of risks from audit findings, or changes to them, are made available to users.
4. Determine if corrective actions proposed are planned to align with the organization's risk profile.
5. Determine if a process exists to track changes in risk rating and is used to update risk registers, particularly with regard to residual risk.

6. Examine a sample of proposed corrective actions and determine if they were followed-up in a manner consistent with the organization's policy.
7. Examine audit programs to determine if they are subject to continuous improvement through feedback, review and revisions.
8. Examine if a process exists to review the audit program in light of current and past audits.

2.2 Application & Interface Security (AIS)

Control Title	Control ID	Control Specification
Application and Interface Security Policy and Procedures	AIS-01	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.

Auditing Guidelines

1. Examine policy and procedures for adequacy, approval, communication, and effectiveness as applicable to planning, delivery, and support of the organization's application security capabilities.
2. Examine policy and procedures for evidence of review at least annually.

Control Title	Control ID	Control Specification
Application Security Baseline Requirements	AIS-02	Establish, document and maintain baseline requirements for securing different applications.

Auditing Guidelines

1. Examine policy and procedures for adequacy and effectiveness.
2. Determine if security baseline requirements of respective applications are clearly defined.
3. Examine the process to determine the baseline for an application.

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

Auditing Guidelines

1. Examine policy and procedures for definition of operational metrics, security, and compliance requirements.

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

Auditing Guidelines

1. Examine policy and procedures for definition of SDLC (Software Development Lifecycle), security, and compliance requirements.
2. Examine the state of implementation of the SDLC process.
3. Verify that the SDLC implementation is in accordance with requirements.

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.

Auditing Guidelines

1. Examine policy and procedures for definition of testing strategies, automation of security testing, and change management.
2. Determine security assurance and acceptance criteria for the new information system(s).
3. Determine if the software release process is automated where applicable.

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.

Auditing Guidelines

1. Examine policy and procedures for implementation of application deployment.
2. Determine if segregation of duties (role and responsibilities) is clearly defined among security and application teams.
3. Determine if Identification and integration process is defined and verified for application deployment processes.
4. Evaluate the extent of automation deployed, and criteria used.

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.

Auditing Guidelines

1. Examine the policy and procedures to remediate application security vulnerabilities and automating remediation.
2. Evaluate whether roles and responsibilities, including escalation paths for application security incident response and remediation, are defined and effective.
3. Determine if the organization leverages automation when possible and if this automation increases remediation efficiency.

2.3 Business Continuity Management & 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>Auditing Guidelines</b>
1. Examine policy and procedures for adequacy, approval, communication, and effectiveness as applicable to business continuity and resilience.
2. Examine policy and procedures for evidence of review at least annually.</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>Auditing Guidelines</b>
1. Examine the policy to determine business impact and the criteria for developing business continuity.
2. Evaluate the process to review and approve the policy.</td></tr>
<tr><td><b>Control Title</b>
Business Continuity Strategy</td><td><b>Control ID</b>
BCR-03</td><td><b>Control Specification</b>
Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite.</td></tr>
<tr><td colspan="3"><b>Auditing Guidelines</b>
1. Determine if the organization has established a risk appetite.
2. Determine if the organization has established strategies to reduce impact of business disruptions, within the organization’s risk appetite.</td></tr>
<tr><td><b>Control Title</b>
Business Continuity Planning</td><td><b>Control ID</b>
BCR-04</td><td><b>Control Specification</b>
Establish, document, approve, communicate, apply, evaluate and maintain a business continuity plan based on the results of the operational resilience strategies and capabilities.</td></tr>
</table>

Auditing Guidelines

1. Examine the policy for adequacy, approval, communication, and effectiveness as applicable to planning, delivery, and support of the organization's application security capabilities.
2. Evaluate if the organization's operational resilience strategies and capabilities are used as an input for the policy and implementation.
3. Examine policy and procedures for evidence of review.

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.

Auditing Guidelines

1. Examine the process for determining the documentation required to support business continuity and operational resilience.
2. Examine the process for developing or acquiring such documentation and maintaining its currency.
3. Evaluate the process and implementation of identifying stakeholders and making documentation available.
4. Examine the policy and procedures for evidence of review.

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.

Auditing Guidelines

1. Examine the plans for business continuity and operational resilience tests, with reference to their intended outputs.
2. Examine the schedules of such tests and their periodicity.
3. Evaluate if the plans are tested upon significant changes, or at least annually.

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

Auditing Guidelines

1. Examine the policy for determining stakeholders and participants.
2. Determine if the organization has identified stakeholders and participants.
3. Examine the procedures for communication with identified stakeholders and participants.

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.

Auditing Guidelines

1. Examine the policy for identifying data for which a backup is required.
2. Examine the requirements for the security of such backups.
3. Evaluate the effectiveness of the backup and restore.

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.

Auditing Guidelines

1. Examine the policy and procedures for adequacy, approval, communication, and effectiveness as applicable to a disaster response plan.
2. Examine the policy and procedures for evidence of review, upon significant changes, or at least annually.

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.

Auditing Guidelines

1. Examine the policy for planning and scheduling disaster response exercises, and involving local emergency authorities, if possible.
2. Evaluate if plans are tested upon significant changes, or at least annually.

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.

Auditing Guidelines

1. Examine the process to identify business-critical equipment and any redundant equipment.
2. Examine the process to identify applicable industry standards.
3. Evaluate if the redundant business-critical equipment is independently located at a reasonable distance.

2.4 Change Control & 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>Auditing Guidelines</b>
1. Examine policy and procedures to determine if they cover necessary parts of change management, including scope, documentation, testing, approval, and emergency changes.
2. Examine a sample record of changes to information assets, including systems, networks, and network services to determine if compliance is met with the organization's change management policy and procedures.
3. Examine if the policy and procedures are reviewed and updated at least annually.</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>Auditing Guidelines</b>
1. Examine relevant documentation, observe relevant processes, and/or interview the control owner(s), relevant stakeholders, for change management and determine if the policy control requirements provided in the policy have been implemented.
2. Examine measures that evaluate(s) the organization's compliance with the change and configuration management policy and determine if these measures are implemented according to policy control requirements.</td></tr>
<tr><td><b>Control Title</b>
Change Management Technology</td><td><b>Control ID</b>
CCC-03</td><td><b>Control Specification</b>
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).</td></tr>
<tr><td colspan="3"><b>Auditing Guidelines</b>
1. Examine policy related to the change management of assets.
2. Examine the policy for the identification of risks arising from these changes being applied.
3. Determine if assets are classified based on their management responsibility, and if these have specific risk profiles.</td></tr>
</table>

<table>
<tr><td><b>Control Title</b>
Unauthorized Change Protection</td><td><b>Control ID</b>
CCC-04</td><td><b>Control Specification</b>
Restrict the unauthorized addition, removal, update, and management of organization assets.</td></tr>
<tr><td colspan="3"><b>Auditing Guidelines</b>
1. Examine the policy relating to the authorisation of changes in assets.
2. Examine the implementation of such policy, technical controls, and their effectiveness.</td></tr>
<tr><td><b>Control Title</b>
Change Agreements</td><td><b>Control ID</b>
CCC-05</td><td><b>Control Specification</b>
Include 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"><b>Auditing Guidelines</b>
1. Examine policy and/or procedures related to change management to determine whether provisions are included for limiting changes directly impacting CSCs owned environments/tenants to explicitly authorized requests within service level agreements between CSPs and CSCs.
2. Examine relevant documentation, observe relevant processes, and/or interview the control owner(s), and/or relevant stakeholders, as needed, for change agreements and determine if the policy control requirements stipulated in the policy have been implemented.
3. Examine measures that evaluate the organization's change agreement policy and determine if these measures are implemented according to policy control requirements.</td></tr>
<tr><td><b>Control Title</b>
Change Management Baseline</td><td><b>Control ID</b>
CCC-06</td><td><b>Control Specification</b>
Establish change management baselines for all relevant authorized changes on organization assets.</td></tr>
<tr><td colspan="3"><b>Auditing Guidelines</b>
1. Examine policy and/or standards related to change management to determine if changes are formally controlled, documented and enforced to minimize the corruption of information systems.
2. Determine if the introduction of new systems and major changes to existing systems are formally documented, specified, tested, quality controlled, and the implementation managed.</td></tr>
<tr><td><b>Control Title</b>
Detection of Baseline Deviation</td><td><b>Control ID</b>
CCC-07</td><td><b>Control Specification</b>
Implement detection measures with proactive notification in case of changes deviating from the established baseline.</td></tr>
<tr><td colspan="3"><b>Auditing Guidelines</b>
1. Examine measures that evaluate the organization's compliance with the change management policy and determine if these measures are implemented according to policy control requirements.</td></tr>
</table>

Control Title	Control ID	Control Specification
Exception Management	CCC-08	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.

Auditing Guidelines

1. Verify that the organization establishes and documents mandatory configuration settings for information technology products employed within the information system, as determined by adoption of the latest suitable security configuration baselines.
2. Confirm that the process identifies, documents, and approves exceptions from the mandatory established configuration settings for individual components based on explicit operational requirements.
3. Determine that the organization monitors and controls changes to the configuration settings in accordance with organizational policy and procedures.

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

Auditing Guidelines

1. Examine policy and/or procedures related to change management and determine if roll back procedures are defined and implemented, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.
2. Examine relevant documentation, observe relevant processes, and/or interview the control owner(s) and/or relevant stakeholders, as needed to ensure that roll back procedures are defined and implemented and determine if the policy control requirements stipulated in the policy have been implemented. Select a sample of changes and examine the change management record to confirm that the change was assessed and included appropriate fallback procedures in the event of a failed change.
3. Examine measure(s) that evaluate(s) the organization’s compliance with the change management policy and determine if these measures are implemented according to policy control requirements.
4. Obtain and examine supporting documentation maintained as evidence of these metrics, measures, tests, or audits to determine if the office or individual responsible reviews the information and, if issues were identified, they were investigated and corrected.

2.5 Cryptography, Encryption & Key Management (CEK)

Control Title	Control ID	Control Specification
Encryption and Key Management Policy and Procedures	CEK-01	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.

Auditing Guidelines

1. Review cryptography, encryption, and key management policy and procedures and confirm that these have been approved by appropriate management.
2. Confirm that the policy and procedures are reviewed at least annually.

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

Auditing Guidelines

1. Obtain cryptographic, encryption policy, and key management procedures.
2. Verify, by interviews or otherwise, that employees and stakeholders are aware of their roles and responsibilities, and obtain supporting documentation evidencing that the responsibilities are being managed in-line with policy and procedures.

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.

Auditing Guidelines

1. Identify data flows within the organization that are in-transit.
2. Identify data storages within the organization that are at-rest.
3. Confirm that the identified data flows and data storages have been protected by an appropriate cryptographic algorithm aligned to cryptography, encryption, and key management policy and procedures.

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.

Auditing Guidelines

1. Identify the encryption algorithms in use.
2. Confirm that identified encryption algorithms have been reviewed and approved by appropriate management.
3. Confirm that the encryption algorithm approval process includes assessment of the appropriateness of the algorithm for the data it is protecting, any associated risks, and the algorithm's usability.

Control Title	Control ID	Control Specification
Encryption Change Management	CEK-05	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.

Auditing Guidelines

1. Examine policy and procedures and obtain evidence that these include the change management process.
2. Obtain representative samples of recent changes relating to cryptographic, encryption, and key management technology.
3. Confirm that sample changes have followed the organization change management procedures, including approval by appropriate individuals, communication of changes to relevant stakeholders, and assessment of the success of implementing changes with any required remediation actions being tracked.

Control Title	Control ID	Control Specification
Encryption Change Cost Benefit Analysis	CEK-06	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.

Auditing Guidelines

1. Obtain a copy of the change management policy and procedures. Confirm that these documents include assessment of impact on downstream effects, including residual risk, cost, and benefit analysis.
2. Examine recent changes made to cryptography-, encryption-, and key management-related systems (including policy and procedures), and confirm that these changes include an account of downstream effects of proposed changes, including residual risk, cost, and benefits analysis.
3. Confirm that the changes have been reviewed and approved by appropriate management.

Control Title	Control ID	Control Specification
Encryption Risk Management	CEK-07	Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.

Auditing Guidelines

1. Identify and confirm the existence of the organization's risk assessment process and obtain the risk register.
2. Confirm that the risk register includes as part of a regular process or control review encryption and key management.
3. Obtain evidence that demonstrates that a risk assessment is performed of the encryption and key management program and process.

<table>
<tr><td><b>Control Title</b>
CSC Key Management Capability</td><td><b>Control ID</b>
CEK-08</td><td><b>Control Specification</b>
CSPs must provide the capability for CSCs to manage their own data encryption keys.</td></tr>
<tr><td colspan="3"><b>Auditing Guidelines</b>
1. Identity CSC’s data key encryption policy and standards.
2. Review the implementation of the CSP key broker and key management services (KMS) and the cloud hardware security modules (HSMs).
3. Confirm that the configuration enables appropriate management of the key, e.g., customer-managed master key, CSP-managed master key, and CSP-owned master key.
4. Confirm that HSM meets internal compliance standards, e.g., FIPS 140-2.</td></tr>
<tr><td><b>Control Title</b>
Encryption and Key Management Audit</td><td><b>Control ID</b>
CEK-09</td><td><b>Control Specification</b>
Audit encryption and key management systems, policy 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).</td></tr>
<tr><td colspan="3"><b>Auditing Guidelines</b>
1. Examine the master audit plan to confirm that audits of encryption and key management systems, policy and processes are included in the plan.
2. Review previously completed audits and confirm that audits of encryption and key management systems, policy and processes have been completed and that any issues raised have been included in issue logs and tracked appropriately.</td></tr>
<tr><td><b>Control Title</b>
Key Generation</td><td><b>Control ID</b>
CEK-10</td><td><b>Control Specification</b>
Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used.</td></tr>
<tr><td colspan="3"><b>Auditing Guidelines</b>
1. Confirm that the organization has an approved process for the generation of cryptographic keys.
2. Identify the keys being used.
3. Observe the generation of an encryption key in a production-like sandbox or as a test tenant in production and confirm the keys have been generated according to the appropriate procedure and technical specifications.</td></tr>
<tr><td><b>Control Title</b>
Key Purpose</td><td><b>Control ID</b>
CEK-11</td><td><b>Control Specification</b>
Manage cryptographic secret and private keys that are provisioned for a unique purpose.</td></tr>
</table>

Auditing Guidelines

1. Obtain copies of the policy and procedures detailing the management of secret and private cryptographic keys.
2. Identify cryptographic secret and private keys that have been provisioned for a unique purpose.
3. Ascertain that these keys are being managed in accordance with policy and procedures.

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.

Auditing Guidelines

Consider the symmetric vs. asymmetric key rotation capabilities of CSPs and an appropriate rotation process adopted.

1. Confirm that policy and procedures include a requirement for regular key rotation.
2. Identify keys used within the organization. Confirm that these keys are part of the rotation process.
3. Review the key rotation process to confirm logging and monitoring of key rotation, tracking of date, time, encryption algorithm used, and authorization process used.

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.

Auditing Guidelines

1. Examine the organization procedures and confirm the existence of a key revocation process.
2. Identify a population of keys and confirm that they are captured within the key revocation process.
3. Confirm that a list of entities no longer part of the organization is maintained.

Control Title	Control ID	Control Specification
Key Destruction	CEK-14	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.

Auditing Guidelines

1. Confirm the existence of key destruction processes and procedures.
2. Review the access permissions for the destruction and restoration of keys and confirm that only appropriate individuals have access to these capabilities.
3. Review keys that have been destroyed and ascertain the appropriate process and procedure have been followed.
4. Establish documented criteria that determine when it is appropriate for a cryptographic key to be stored outside a secure environment.

Control Title	Control ID	Control Specification
Key Activation	CEK-15	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.

Auditing Guidelines

1. Confirm the existence of processes and procedures to generate keys.
2. Confirm that the access and permissions around the key creation process is restricted to appropriate individuals.
3. Identify the key management server and the key storage database.
4. Review the key attributes and confirm that these are appropriate for the key, e.g., activation data, instance, deletion ability, rollover, etc.
5. Confirm the key activation process, e.g., manual, on creation, at a future time.
6. Review the pre-activated keys.

Control Title	Control ID	Control Specification
Key Suspension	CEK-16	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.

Auditing Guidelines

1. Confirm the existence of processes and procedures to manage the transition state of keys.
2. Review the access and permissions regarding the transition state of keys and confirm that these are restricted to appropriate individuals.
3. Verify that it is possible to modify a key state and suspend/disable keys when required.

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.

Auditing Guidelines

1. Confirm the existence of processes and procedures to deactivate keys.
2. Review the access and permissions around the key deactivation process and confirm this is restricted to appropriate individuals.
3. Review key deactivation process and configurations. Confirm that they are in line with internal and external requirements.
4. Confirm the key deactivation process e.g. manual, on expiration, at a defined future time.

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.

Auditing Guidelines

1. Confirm the existence of a documented and valid process for key archival.
2. Verify that the key archival process implements least privilege throughout the key archival cycle.
3. Establish whether the storage medium is secure, as per internal and external requirements.

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.

Auditing Guidelines

1. Examine if the organization has defined processes, procedures and technical measures for secure handling of compromised keys.
2. Review if the process for secure usage of compromised keys fulfills the organization and external business / operational continuity requirements.
3. Evaluate the significance of technical and organizational measures defined and implemented for usage of compromised keys in a secure environment.

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.

Auditing Guidelines

1. Examine if the organization has defined processes and procedures for handling the operational risk of compromised keys.
2. Determine if the key recovery process fulfills the organization and external business / operational continuity requirements.
3. Evaluate the significance of technical and organizational measures as per the key management lifecycle.

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.

Auditing Guidelines

1. Examine if the organization has defined the key management processes.
2. Review the processes for key lifecycle management (creation, rotation, storage, disposal) with respect to organization and external (regulatory) requirements.
3. Evaluate if the processes and procedures for change management of key management systems provide an overall traceability of lifecycle steps.

2.6 Datacenter Security (DCS)

Control Title	Control ID	Control Specification
Off-Site Equipment Disposal Policy and Procedures	DCS-01	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 policy and procedures at least annually.

Auditing Guidelines

1. Examine the organization's policy and procedures related to data destruction.
2. Determine if the policy has been approved, communicated, and reviewed.
3. Determine if a policy exists that addresses the secure destruction of data and for conditions when equipment is reused as opposed to when equipment is destroyed.

Control Title	Control ID	Control Specification
Off-Site Transfer Authorization Policy and Procedures	DCS-02	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.

Auditing Guidelines

1. Examine the organization's policy and procedures related to relocation, transfer or retirement of assets.
2. Determine if policy has been approved, communicated, and reviewed.
3. Determine if the policy requires recorded authorisation of movements.

Control Title	Control ID	Control Specification
Secure Area Policy and Procedures	DCS-03	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.

Auditing Guidelines

1. Examine the organization's policy and procedures related to physical areas under the organisation's control.
2. Determine if policy has been approved, communicated, and reviewed.

Control Title	Control ID	Control Specification
Secure Media Transportation Policy and Procedures	DCS-04	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.

Auditing Guidelines

1. Examine the organization's policy and procedures for secure transportation of physical media.
2. Determine if policy has been approved, communicated, and reviewed.

Control Title	Control ID	Control Specification
Assets Classification	DCS-05	Classify and document the physical, and logical assets (e.g., applications) based on the organizational business risk.

Auditing Guidelines

1. Examine the policy relating to defining the organization's business risk.
2. Confirm that the physical and logical assets are being classified in accordance with defined policy and procedures.
3. Review the asset Inventory to determine if assets are catalogued and tagged according to the organization's business risk classification criteria.

<table>
<tr><td>**Control Title**
Assets Cataloguing and Tracking</td><td>**Control ID**
DCS-06</td><td>**Control Specification**
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">**Auditing Guidelines**
1. Examine the policy relating to defining asset location and disposition.
2. Examine the asset registers and determine if they are stored and accessed securely.</td></tr>
<tr><td>**Control Title**
Controlled Access Points</td><td>**Control ID**
DCS-07</td><td>**Control Specification**
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">**Auditing Guidelines**
1. Examine the policy relating to physical security perimeters.
2. Examine the lists of types of areas in the organisation, and the classification of each.
3. Determine if there are appropriate physical security barriers and if monitoring exists between areas.</td></tr>
<tr><td>**Control Title**
Equipment Identification</td><td>**Control ID**
DCS-08</td><td>**Control Specification**
Use equipment identification as a method for connection authentication.</td></tr>
<tr><td colspan="3">**Auditing Guidelines**
1. Examine the policy relating to equipment classification and identification
2. Determine if appropriate methods are implemented.
3. Confirm the existence of a process or procedure to track and maintain a list of appropriate equipment permitted for authorised connections.</td></tr>
<tr><td>**Control Title**
Secure Area Authorization</td><td>**Control ID**
DCS-09</td><td>**Control Specification**
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>
<tr><td colspan="3">**Auditing Guidelines**
1. Examine the policy and procedures relating to access to secure areas.
2. Determine if the policy includes ingress and egress points to service and delivery areas.
3. Determine if procedures include activities and actions against unauthorized personnel in the premises.
4. Confirm that existence, review, and retention of Access logs for secure areas are aligned with policy and procedures.</td></tr>
</table>

<table>
<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>Auditing Guidelines</b>
1. Examine the policy relating to data center surveillance.
2. Determine if the policy includes ingress, egress and external perimeter to detect unauthorized access.
3. Determine if procedures include activities and actions against unauthorized personnel in the premises.
4. Review and determine if items identified in surveillance system logs for the premises have been actioned in accordance with policy and procedures.
5. Determine if logs are maintained and reviewed appropriately.</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>Auditing Guidelines</b>
1. Examine the policy and procedures relating to activities and actions to perform in case of unauthorized access.
2. Examine the policy and procedures related to datacenter's personnel training.
3. Determine if the training content is appropriate and approved by the organization.
4. Ascertain that appropriate datacenter personnel have completed all relevant training through review of training plans and records. Confirm that these have been completed in accordance with policy and procedures.</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>Auditing Guidelines</b>
1. Examine the policy and procedures relating to cabling Infrastructure.
2. Determine if risk registers are maintained for cabling (For plant and ancillary equipment).</td></tr>
<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>
</table>

Auditing Guidelines

1. Confirm the existence of policy and procedures relating to environmental control in the datacenter.
2. Verify that the environment control systems are documented and operational in accordance with policy and procedures.
3. Determine if testing for operational control effectiveness is conducted at regular intervals.
4. Determine if environment system logs (e.g., temperature and humidity) are generated and if related monitoring controls are maintained.
5. Confirm that the system logs are reviewed on a periodic basis and items are disposed of in accordance with policy and procedures.

Control Title	**Control ID**	**Control Specification**
Secure Utilities	DCS-14	Secure, monitor, maintain, and test utilities services for continual effectiveness at planned intervals.

Auditing Guidelines

1. Confirm the existence of the policy and procedures relating to utilities services
2. Confirm that the control effectiveness of utilities services is conducted at periodic intervals.
3. Determine if utility services logs are maintained and reviewed periodically.
4. Determine if testing of the utilities services is included in the CSP contract with the customer.

Control Title	**Control ID**	**Control Specification**
Equipment Location	DCS-15	Keep business-critical equipment away from locations subject to high probability for environmental risk events.

Auditing Guidelines

1. Examine the policy relating to environmental risk.
2. Determine if locations are assessed and classified for probability of environmental risk.
3. Determine if business-critical equipment is identified.

2.7 Data Security & 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.

Auditing Guidelines

1. Examine the organization's policy and procedures related to data privacy. Determine if a framework exists to ensure that the organization monitors the regulatory and legislative environment for changes applicable to the organization. Confirm whether the organization has documented the roles and responsibilities that support the management of its policy.
2. Determine whether policy and procedure content is sufficient to direct the compliant and lawful management of personal data and to address non-compliance.
3. Confirm whether policy addresses the requirement that the organization's data is used only for authorized purposes and in compliance with legislation and regulation.
4. Examine if the policy and procedures are reviewed on an appropriate basis.
5. Examine the measure(s) that evaluate(s) compliance with the organization's data privacy and security policy and determine if the measure(s) address(es) implementation of the policy/control requirement(s) as stipulated.
6. Examine documentation to determine if the function responsible for data privacy compliance reviews the information to determine whether the organization is compliant with current legislation and regulation.
7. Confirm that the procedure exists for follow-up on deviation to current legislation and regulations and is up to date

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.

Auditing Guidelines

1. Examine the organization's procedures and technical requirements related to the secure disposal of data from storage media. Establish that this process and key controls comply with the organization's data privacy and security policy. Establish whether the organization has documented the roles and responsibilities for this process.
2. Select a sample of disposal requests and assess whether they have followed the process through to completion. Confirm that all evidence was formally documented and recorded.

3. Examine measure(s) that evaluate(s) this process and determine if the measure(s) address(es) implementation of the process/control requirement(s) as stipulated. Reviews, tests, or audits should be completed periodically by the organization to measure the effectiveness of the implemented controls and to verify that non-compliance and opportunities for improvement are identified, evaluated for risk, reported, and corrected in a timely manner.
4. Obtain and examine supporting documentation maintained as evidence of these metrics to determine if the office or individual responsible reviews the information and if identified issues were investigated and corrected. Determine if the individual or office is able to correct issues without the need to routinely escalate the issues to the next level of management. Examine related records to determine if the individual or office conducted any follow-ups on the deviations to verify they were corrected as intended.

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.

Auditing Guidelines

1. Examine the organization’s procedures and technical requirements for the population and management of its data inventory. Establish that this process and key controls comply with the organization’s data privacy and security policy. Establish whether the organization has documented the roles and responsibilities for this process.
2. Select a sample of entries to ensure they have been recorded correctly on the inventory. The sample must include a proportion of sensitive and personal data entries.
3. Assess whether management of the data inventory meets the organization’s expectations.
4. Examine measure(s) that evaluate(s) this process and determine if the measure(s) address(es) implementation of the process/control requirement(s) as stipulated. Reviews, tests, or audits should be completed periodically by the organization to measure the effectiveness of the implemented controls and to verify that non-compliance and opportunities for improvement are identified, evaluated for risk, reported, and corrected in a timely manner.
5. Obtain and examine supporting documentation maintained as evidence of these metrics to determine if the office or individual responsible reviews the information and if identified issues were investigated and corrected. Determine if the individual or office is able to correct issues without the need to routinely escalate the issues to the next level of management. Examine related records to determine if the individual or office conducted any follow-ups on the deviations to verify they were corrected as intended.

Control Title	**Control ID**	**Control Specification**
Data Classification	DSP-04	Classify data according to its type and sensitivity level.

Auditing Guidelines

1. Examine the organization’s procedures and technical requirements for classifying data. Establish that this process and key controls comply with the organization’s data privacy and security policy. Establish whether the organization has documented the roles and responsibilities for this process.
2. Establish if the organization’s data classification matrix is aligned with the organization’s data classification requirements.
3. Select a sample of data to confirm that each item has been classified appropriately.
4. Examine measure(s) that evaluate(s) this process and determine if the measure(s) address(es) implementation of the process/control requirement(s) as stipulated. Reviews, tests, or audits should be completed periodically by the organization to measure the effectiveness of the implemented controls and to verify that non-compliance and opportunities for improvement are identified, evaluated for risk, reported, and corrected in a timely manner.
5. Obtain and examine supporting documentation maintained as evidence of these metrics to determine if the office or individual responsible reviews the information and if identified issues were investigated and corrected. Determine if the individual or office is able to correct issues without the need to routinely escalate the issues to the next level of management. Examine related records to determine if the individual or office conducted any follow-ups on the deviations to verify they were corrected as intended.

Control Title	**Control ID**	**Control Specification**
Data Flow Documentation	DSP-05	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.

Auditing Guidelines

1. Examine the organization’s procedures and technical requirements for recording data flows and that a review is carried out at least annually. Establish that this process and key controls comply with the organization’s data privacy and security policy. Establish whether the organization has documented the roles and responsibilities for this process.
2. Select a sample of documents to check that they have been completed to the correct specifications and reviewed.
3. Review if data flow documentation includes assessment for accuracy, completeness, timeliness, and sustainability of data (flow).
4. Examine measure(s) that evaluate(s) this process and determine if the measure(s) address(es) implementation of the process/control requirement(s) as stipulated. Reviews, tests, or audits should be completed periodically by the organization to measure the effectiveness of the implemented controls and to verify that non-compliance and opportunities for improvement are identified, evaluated for risk, reported, and corrected in a timely manner.

5. Obtain and examine supporting documentation maintained as evidence of these metrics to determine if the office or individual responsible reviews the information and if identified issues were investigated and corrected. Determine if the individual or office is able to correct issues without the need to routinely escalate the issues to the next level of management. Examine related records to determine if the individual or office conducted any follow-ups on the deviations to verify they were corrected as intended.

Control Title	**Control ID**	**Control Specification**
Data Ownership and Stewardship	DSP-06	Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually.

Auditing Guidelines

1. Examine the organization's data owner process and roles and responsibilities documentation. Establish that this process and key controls comply with the organization's data privacy and security policy. Establish whether the organization has documented the roles and responsibilities for this process.
2. Establish that the organization maintains a source(s) of record of data owners and the records for which they are responsible. Establish that this must include personal data and sensitive data.
3. In the absence of a documented procedure, interview control owner(s) responsible for key staff involved in/with, and/or other relevant stakeholders impacted by the process/control requirement(s) and determine if the requirement(s) is/are understood. Evidence may be provided by observing individuals, systems and/or processes associated with data management to determine if the process requirements are generally understood and implemented consistently.
4. Select a range of entries to establish the information recorded is correct.
5. Assess whether oversight of the data ownership process meets the organization's expectations.
6. Examine if the documentation is reviewed on an annual basis.
7. Examine measure(s) that evaluate(s) this process and determine if the measure(s) address(es) implementation of the process/control requirement(s) as stipulated. Reviews, tests, or audits should be completed periodically by the organization to measure the effectiveness of the implemented controls and to verify that non-compliance and opportunities for improvement are identified, evaluated for risk, reported, and corrected in a timely manner.
8. Obtain and examine supporting documentation maintained as evidence of these metrics to determine if the office or individual responsible reviews the information and if identified issues were investigated and corrected. Determine if the individual or office is able to correct issues without the need to routinely escalate the issues to the next level of management. Examine related records to determine if the individual or office conducted any follow-ups on the deviations to verify they were corrected as intended.

Control Title	Control ID	Control Specification
Data Protection by Design and Default	DSP-07	Develop systems, products, and business practices based upon a principle of security by design and industry best practices.

Auditing Guidelines

1. Examine whether the organization's policy, standards, and procedures create a framework which fosters a culture and expectation of "security through design." Determine whether this content addresses the directive of the organization's culture and whether practices reflect security through design.
2. Examine whether the organization's governance framework, documents, controls, and metrics satisfy the organization and if its sub-processors comply with this requirement. Establish whether the organization has documented the roles and responsibilities involved.
3. Review the organization's data breaches log, the security incidents log, and project change failure records for examples where this requirement was not followed correctly. Further, confirm that action plans were identified and carried out.
4. Examine the measures that evaluate this organizational requirement and determine if the measures address implementation of process and control requirements as stipulated.
5. Obtain and examine supporting documentation maintained as evidence of these metrics to determine if the office or individual responsible reviews the information and if identified issues were investigated and remediated appropriately.

Control Title	Control ID	Control Specification
Data Privacy by Design and Default	DSP-08	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.

Auditing Guidelines

1. Examine whether the organization's policy, standards, processes, and controls create a framework that fosters a culture and expectation of "data privacy through design." Determine whether this content addresses the directive of the organization's culture and if practices reflect data privacy through design.
2. Examine whether the organization's governance framework, documents, controls, and metrics satisfy the organization and whether its sub-processors comply with this requirement. Establish whether the organization has documented the roles and responsibilities involved.
3. Review the organization's data breaches log, the security incidents log, and project change failure records for examples where this requirement was not followed correctly. Further, confirm that action plans were identified and carried out appropriately.

<table>
<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>Auditing Guidelines</b>
1. Examine procedures related to DPIA risk assessment and determine if once a requirement has been established, the organization identifies and grades the associated risks and reports and prioritizes the remediation of risks and non-compliance activities. Examine whether the DPIA process and templates align to the organization's risk methodology and taxonomy.
2. Establish whether the organization has documented the roles and responsibilities for this process.
3. Select a sample of DPIAs and examine evidence to confirm that each assessment was performed to identify associated risks. Further, confirm that any action plans were identified and carried out appropriately. Confirm that all relevant evidence was formally documented.</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>Auditing Guidelines</b>
1. Examine the organization's procedures and technical requirements for the secure and lawful transfer of personal data and sensitive data. Establish that this process and key controls comply with the organization's data privacy and security policy.
2. Establish whether the organization has documented the roles and responsibilities for this process.
3. Select a range of personal data transfers and a range of sensitive data transfers to confirm that each transfer adhered to the organization's policy, procedures, and controls. Confirm that all relevant evidence was formally documented.</td></tr>
<tr><td><b>Control Title</b>
Personal Data Access, Reversal, Rectification and Deletion</td><td><b>Control ID</b>
DSP-11</td><td><b>Control Specification</b>
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.</td></tr>
</table>

Auditing Guidelines

1. Examine whether the organization's policy and procedures related to data privacy addresses the requirement that authorized users must be able to access, modify, or delete personal data. Establish whether the organization has processes in place to manage and respond to data access requests from data subjects. Establish whether the organization has documented the roles and responsibilities for this process.
2. Select a range of data changes to confirm that only authorized users are able to successfully access, modify and delete personal data. Select a sample of data access requests to establish that these were completed correctly following the organization's processes. Confirm that all relevant evidence was formally documented.

Control Title	Control ID	Control Specification
Limitation of Purpose in Personal Data Processing	DSP-12	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.

Auditing Guidelines

1. Examine whether the organization's policy and procedures related to data privacy address the requirement that data the organization is responsible for is processed lawfully and used only for the purposes stated to data subjects.
2. Establish whether the organization has documented the roles and responsibilities for this process.
3. Review the organization's data breaches and confirm that action plans were identified and carried out appropriately. Confirm that all supporting evidence was formally documented.
4. Review the organization's processes that inform data subjects why the organization requests this data and what it will be used for. Confirm that any organization documentation (including web page content) is subject to formal periodic review for relevance and compliance to legislation and regulation.

Control Title	Control ID	Control Specification
Personal Data Sub-processing	DSP-13	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.

Auditing Guidelines

1. Examine the organization's contractual terms, procedures, roles and responsibility documents and technical requirements for the transfer of personal data and sensitive data to sub-processors and how sub-processors are to treat this data.
2. Establish whether the organization has documented the roles and responsibilities for this process.
3. Select a sample of data transfers to sub-processors to establish that the controls and reporting the sub-processor are in place and ensure that these comply with the organization's data privacy and security policy.
4. Examine the organization's contractual requirements for sub-processor compliance, reporting and non-compliance sanctions, and the organization's right to audit. Establish sub-processors' processes, controls and metrics to comply with those of the organization.

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.

Auditing Guidelines

1. Examine the organization's contractual requirements and procedures whereby sub-processors will disclose all occasions when personal or sensitive data was accessible by sub-processors prior to initiation of that processing.
2. Establish whether the organization has documented the roles and responsibilities for this process.
3. Select a sample of data transfers to sub-processors to establish that the controls and reporting the sub-processor are in place and ensure that these comply with the organization's data privacy and security policy.

Note: A real-life case will be rare. Should it not be possible to follow a real-life case, a theoretical case should be tested to establish that systems, processes, and controls are operating as designed and as agreed with the sub-processor.

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.

Auditing Guidelines

1. Examine the organization's procedures and technical requirements related to the use of production data in non-production environments or requests to replicate production data for use in non-production environments.
2. Establish whether the organization has documented the roles and responsibilities for this process.
3. Select a sample of requests and assess whether such requests have followed the approval and secure deployment processes through to completion. Confirm that all relevant evidence was formally documented and recorded.
4. Review the organization's data breaches for examples in which this requirement was not followed correctly. Further, confirm that any appropriate action plans were identified and carried out.

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.

Auditing Guidelines

1. Examine the organization’s procedures, technical requirements and other documentation for the retention, archiving and deletion of data.
2. Establish whether the organization has documented the roles and responsibilities for this process.
3. Establish that the organization maintains a source(s) of record of data types, owners, and retention periods. Select a range of entries to establish that the information recorded is correct.
4. Establish how the organization determines that its retention records are accurate and complete. Establish that the organization has documented its understanding of the extent of its remit in terms of its role as a supplier and the extent of its own supplier’s obligations to this requirement.
5. Confirm that the data retention process meets the organization’s requirements as detailed in policy and procedures.

Control Title	Control ID	Control Specification
Sensitive Data Protection	DSP-17	Define and implement processes, procedures and technical measures to protect sensitive data throughout its lifecycle.

Auditing Guidelines

1. Examine whether the organization’s policy and procedures related to data privacy address the requirement to manage and protect sensitive data throughout its lifecycle.
2. Establish whether the organization has documented the roles and responsibilities for this process.
3. Select a sample of sensitive data types to establish the systems, processes, and controls operating to manage sensitive data throughout its lifecycle. Select a sample to establish the examples following the organization’s processes.
4. Review the organization’s data breaches for examples for which this requirement was not followed correctly. Further, confirm that any relevant action plans were identified and carried out. Confirm that all relevant evidence was formally documented.

Control Title	Control ID	Control Specification
Disclosure Notification	DSP-18	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.

Auditing Guidelines

1. Examine the organization’s procedures and technical requirements related to personal data requests from law enforcement authorities.
2. Establish that processes and controls comply with the organization’s data privacy and security policy.
3. Establish whether the organization has documented the roles and responsibilities for this process.
4. Select a sample of requests and assess whether such requests have followed the approvals and secure communication processes through to completion. Confirm that all evidence was formally documented.
5. Review the organization’s data breaches for examples for which this requirement was not followed correctly. Further, confirm that relevant action plans were identified and carried out.

Control Title	Control ID	Control Specification
Data Location	DSP-19	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.

Auditing Guidelines

1. Examine the organization’s procedures, technical requirements, and other documentation to direct, manage and review the records of the organization’s data physical storage locations.
2. Establish whether the organization has documented the roles and responsibilities for this process.
3. Confirm that the organization’s policy and procedures include details of guidelines for the storage and processing of data within the designated countries/regions/zones/ jurisdictions.
4. Establish that the organization maintains a source(s) of record of its physical data storage locations and is able to trace data lineage. Select a range of entries to establish that the information is recorded appropriately.
5. Confirm that the data storage records are accurate and complete as detailed in policy and procedures.
6. Establish that the organization has documented its understanding of the extent of its remit in terms of its role as a supplier and the extent of its own supplier’s obligations to this requirement.
7. Confirm that the data storage process meets the organization’s requirements as detailed in policy and procedures.

2.8 Governance, Risk Management and Compliance (GRC)

Control Title	Control	Control Specification
Governance Program Policy and Procedures	GRC-01	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.

Auditing Guidelines

1. Examine the policy and/or procedures related to information governance programs to determine whether the organization has developed a comprehensive strategy for information governance.
2. Examine policies and procedures for evidence of review at least annually.

Control Title	Control ID	Control Specification
Risk Management Program	GRC-02	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.

Auditing Guidelines

1. Examine the policy and/or procedures related to the Enterprise Risk Management (ERM) program to determine whether the organization has developed a comprehensive strategy to manage risk to organizational operations and assets, and individuals.
2. Review ERM documentation, processes, and supporting evidence to confirm if the ERM program includes provisions for cloud security and privacy risk.
3. Examine measure(s) that evaluate(s) the organization's compliance with the risk management policy and determine if the measure(s) address(es) implementation of the policy/control requirement(s) as stipulated in the policy level.
4. Obtain and examine supporting evidence to determine if the office or individual responsible reviews the information and, if issues were identified, if they were investigated and remediated appropriately.

Control Title	Control ID	Control Specification
Organizational Policy Reviews	GRC-03	Review all relevant organizational policies and associated procedures at least annually or when a substantial change occurs within the organization.

Auditing Guidelines

1. Examine the policy and/or procedures related to the Enterprise Risk Management (ERM) program to determine if the organization reviews these documents at least annually or when a substantial change occurs within the organization.
2. Confirm that Policy reviews have taken place in compliance with the organizations review requirements and any exceptions identified are investigated and remediated.

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.

Auditing Guidelines

1. Examine the policy and/or procedures to determine if the policy exception process has been established.
2. Identify and confirm that exceptions to policies are tracked, authorised, and evidenced.
3. Confirm a review of policy exceptions takes place on a periodic basis by appropriate management.

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.

Auditing Guidelines

1. Examine the policy and/or procedures related to the Information Security Program to determine whether the organization has developed and implemented a comprehensive strategy to manage Information Security across the organization.
2. Review the details of the information security program and establish if this covers the CCMv4 relevant domains.
3. Confirm that identified gaps/issues are being tracked, monitored, and remediated with appropriate escalation where required.

Control Title	Control ID	Control Specification
Governance Responsibility Model	GRC-06	Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs.

Auditing Guidelines

1. Confirm the organization has established a governance framework which details roles, responsibilities, and accountability.
2. Evidence that governance meetings are reported and documented appropriately.
3. Confirm that individuals/groups responsible for governance are tracking and monitoring progress against the governance program.

<table>
<tr><td><b>Control Title</b>
Information System Regulatory Mapping</td><td><b>Control ID</b>
GRC-07</td><td><b>Control Specification</b>
Identify and document all relevant standards, regulations, legal/contractual, and statutory requirements, which are applicable to your organization.</td></tr>
<tr><td colspan="3"><b>Auditing Guidelines</b>
1. Confirm that policy and procedures include provisions to identify and document all relevant standards, regulations, legal/contractual, and statutory requirements.
2. Establish that the organization maintains an inventory of CCM controls and relevant regulatory information is mapped across to the CCM inventory.
3. Identify and examine any metrics and supporting evidence to provide assurance that the information system regulatory mapping is reviewed on a periodic basis, and that any gaps in the mapping are appropriately actioned.</td></tr>
<tr><td><b>Control Title</b>
Special Interest Groups</td><td><b>Control ID</b>
GRC-08</td><td><b>Control Specification</b>
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"><b>Auditing Guidelines</b>
1. Examine the organization’s policy and procedures related to contact with cloud-related special interest groups to determine if membership is required and actively maintained.
2. Identify relevant individuals responsible for contacting cloud-related special interest groups and determine if the policy requirements stipulated in the policy level have been implemented.</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.

Auditing Guidelines

1. Examine policy for adequacy, currency, communication, and effectiveness.
2. Examine the process for selection of local laws, regulations, ethics, and contractual constraints, and for review of its output.
3. Verify that the background verification required is mapped to the risks and data classification.
4. Examine the policy and procedures for evidence of review at least annually.
5. Examine Human Resources tickets upon hire which trigger background review and final confirmation from third party conducting background reviews showing it has been completed and how exceptions or failed checks have been addressed.

Control Title	Control ID	Control Specification
Acceptable Use of Technology Policy and Procedures	HRS-02	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.

Auditing Guidelines

1. Examine policy for adequacy, currency, communication, and effectiveness.
2. Verify that a definition of organizationally-owned or managed assets exists, and is implemented.
3. Verify, via Interviews or otherwise, that the policy is communicated to users.
4. Examine policy and procedures for evidence of review at least annually.

Control Title	Control ID	Control Specification
Clean Desk Policy and Procedures	HRS-03	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.

Auditing Guidelines

1. Examine policy for adequacy, currency, communication, and effectiveness.
2. Verify that secure and unsecure work areas are defined and demarcated.
3. Verify that confidential data is classified appropriately, and that the classification is available at point-of-use.
4. Verify, via Interviews or otherwise, that the policy is communicated to users.
5. Examine policy and procedures for evidence of review at least annually.

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.

Auditing Guidelines

1. Examine policy for adequacy, currency, communication, and effectiveness.
2. Verify, via Interviews or otherwise, that remote sites and locations, especially those not under the control of the organization, are defined and demarcated.
3. Verify, via Interviews or otherwise, that the policy and procedures are communicated to users.
4. Examine policy and procedures for evidence of review or at least annually.

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

Auditing Guidelines

1. Examine policy for adequacy, currency, communication, and effectiveness.
2. Verify that a definition of organizationally-owned assets exists, and is implemented.
3. Verify that a definition of terminated employees exists, and is implemented.
4. Examine policy and procedures for evidence of review at least annually.

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.

Auditing Guidelines

1. Examine policy for adequacy, currency, communication, and effectiveness.
2. Verify that organisation charts are maintained and available as appropriate.
3. Verify that a definition of terminated employees exists, and is implemented.
4. Examine policy and procedures for notification of stakeholders upon changes in employment, or of roles, and the appropriate activities are triggered, i.e. access changes, asset return, etc.

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.

Auditing Guidelines

1. Verify that the organization has defined formats and templates of employment agreements.
2. Verify, if more than one Agreement is used, that they are mapped to appropriate roles and job descriptions.
3. Examine the policy and procedures that mandate the signing of such Agreement before access is granted.

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.

Auditing Guidelines

1. Verify that the organization has defined formats and templates of Employment Agreements.
2. Verify that the Agreements include references to the organization's Information Security Management System (ISMS), and that they mandate compliance.

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.

Auditing Guidelines

1. Verify that organisation charts are maintained and available as appropriate.
2. Verify that the Role or Job Descriptions refer to the appropriate ISMS requirements.
3. Verify, by Interviews or otherwise, that employees and stakeholders are aware of the roles or job descriptions, and that these are reviewed.

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.

Auditing Guidelines

1. Examine if the organisation has identified its requirements for non-disclosure and confidentiality.
2. Determine the planned interval for review.
3. Verify that the requirements are reviewed at such planned intervals.

<table>
<tr><td><b>Control Title</b>
Security Awareness Training</td><td><b>Control ID</b>
HRS-11</td><td><b>Control Specification</b>
Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organization and provide regular training updates.</td></tr>
<tr><td colspan="3"><b>Auditing Guidelines</b>
1. Examine the security awareness training program for adequacy, currency, communication, and effectiveness.
2. Verify, by Interviews or otherwise, that the training program has been implemented.
3. Verify that the scope of the training program extends to all employees.
4. Examine policy and procedures for evidence of review.</td></tr>
<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>Auditing Guidelines</b>
1. Examine the security awareness training program for adequacy, currency, communication, and effectiveness.
2. Verify that a definition of sensitive organizational and personal data exists, and is implemented.
3. Verify, by Interviews or otherwise, that the training program has been implemented.
4. Verify that the scope of the training program extends to all employees with access to such data.
5. Examine policy and procedures for evidence of review.</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>Auditing Guidelines</b>
1. Examine the process for selection of applicable legal, statutory, or regulatory compliance obligations, and for review of its output.
2. Verify, by Interviews or otherwise, that employees are aware of their roles and responsibilities with respect to such obligations.</td></tr>
</table>

2.10 Identity & Access Management (IAM)

Control Title	**Control ID**	**Control Specification**
Identity and Access Management Policy and Procedures	IAM-01	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.

Auditing Guidelines

1. Examine policy and/or procedures related to identity and access management to determine if policy and/or procedure content:
    a. addresses the provisioning, modification and deprovisioning of logical access.
    b. establishes password complexity and management requirements.
    c. addresses authorization concept following separation of duties and least privilege.
    d. addresses privileged access management and access reviews.
    e. includes roles and responsibilities for provisioning, modifying and deprovisioning of logical access.
    f. understands the delineation of identity and access management control responsibility in relation to the shared responsibility model.
2. Determine if the policy is clearly communicated and available to stakeholders.
3. Examine if policy and procedures are reviewed and updated at least annually.

Control Title	**Control ID**	**Control Specification**
Strong Password Policy and Procedures	IAM-02	Establish, document, approve, communicate, implement, apply, evaluate and maintain strong password policies and procedures. Review and update the policies and procedures at least annually.

Auditing Guidelines

1. Examine policy and/or procedures related to passwords to determine if minimum password complexity requirements are defined.
2. Determine if the organization enforces minimum password complexity requirements as defined in policy.
3. Examine policy and procedures for evidence of review at least annually.

Control Title	**Control ID**	**Control Specification**
Identity Inventory	IAM-03	Manage, store, and review the information of system identities, and level of access.

Auditing Guidelines

1. Determine if the organization has defined acceptable storage methods and locations of system identities.
2. Evaluate if the organization is consistently utilizing approved methods and locations to store system identities.
3. Evaluate if access to stored identities is managed following established processes.

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

Auditing Guidelines

1. Determine if divisions of responsibility and separation of duties are defined and documented.
2. Determine if information system access authorizations are established to support separation of duties.

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

Auditing Guidelines

1. Examine the policy to determine the least privilege required for each role or user.
2. Evaluate the effectiveness of the implementation and review of policy.

Control Title	Control ID	Control Specification
User Access Provisioning	IAM-06	Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets.

Auditing Guidelines

1. Determine if personnel required to approve system access requests are identified and documented.
2. Evaluate if access requests are documented and approved by required personnel prior to access provisioning.

Control Title	Control ID	Control Specification
User Access Changes and Revocation	IAM-07	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.

Auditing Guidelines

1. Determine if a process is established for removing logical access when users leave the organization or when access is no longer appropriate.
2. Determine if a timeframe for access removal and access modification is defined.
3. Verify that a process is established for removing existing system access and assigning appropriate access or for modifying existing access after internal transfer or change of job functions.
4. Determine if established processes for access removal and modification, within the defined time frame, are followed in practice.

Control Title	**Control ID**	**Control Specification**
User Access Review	IAM-08	Review and validate user access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance.

Auditing Guidelines

1. Determine if the required frequency for review of accounts is established.
2. Determine if accounts are reviewed for compliance, including the level of access and conflicting access, following the principle of least privilege and consideration of separation of duties.
3. Determine if accounts are reviewed at the organization-defined frequency.

Control Title	**Control ID**	**Control Specification**
Segregation of Privileged Access Roles	IAM-09	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.

Auditing Guidelines

1. Determine if processes, procedures and technical measures for the separation of privileged access are defined and include requirements for separation of administrative access to data, encryption, key management and logging capabilities.
2. Evaluate if established processes, procedures and technical measures for the separation of privileged access are implemented and followed in practice.

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.

Auditing Guidelines

1. Determine if an access process, that includes requirements for limiting the time period of privileged access roles and rights, is defined.
2. Determine if procedures address the prevention of culmination of segregated privileged access.
3. Evaluate if an access process, that includes requirements for limiting the time period of privileged access roles and rights, is implemented and consistently followed in practice.
4. Evaluate if procedures that address the prevention of culmination of segregated privileged access is implemented and consistently followed in practice.

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.

Auditing Guidelines

1. Determine if 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 are defined, implemented and consistently followed in practice.

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.

Auditing Guidelines

1. Determine if processes, procedures and technical measures are defined for log management.
2. Determine if processes, procedures and technical measures for log management include the following two requirements:
    a. the logging infrastructure is read-only for all with write access, including privileged access roles.
    b. the ability to disable and/or modify logs is controlled following separation of duties and established break glass procedures.
3. Evaluate if the processes, procedures and technical measures for log management are implemented and consistently followed in practice.

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.

Auditing Guidelines

1. Determine if processes, procedures and technical measures are defined and require that users are identifiable through unique IDs or by association of individuals to the usage of user IDs.
2. Determine if the established processes, procedures and technical measures are implemented and consistently followed in practice.

Control Title	**Control ID**	**Control Specification**
Strong Authentication	IAM-14	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.

<table>
<tr><td colspan="3"><b>Auditing Guidelines</b>
1. Determine if processes, procedures and technical measures for authenticating access to systems, applications and sensitive data are defined and maintained.
2. Determine if processes, procedures and technical measures for authenticating access to systems, applications and sensitive data include organization-defined requirements for specific use cases of multifactor authentication, digital certificates and/or alternative security measures.
3. Determine if processes, procedures and technical measures for authenticating access to systems, applications and sensitive data are implemented and consistently followed in practice.</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>Auditing Guidelines</b>
1. Determine if processes, procedures and technical measures for the secure management of passwords are defined.
2. Determine if processes, procedures and technical measures for the secure management of passwords are implemented and consistently followed in practice.</td></tr>
<tr><td><b>Control Title</b>
Authorization Mechanisms</td><td><b>Control ID</b>
IAM-16</td><td><b>Control Specification</b>
Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.</td></tr>
<tr><td colspan="3"><b>Auditing Guidelines</b>
1. Determine if processes, procedures and technical measures, for verification of access authorization to data and system functions, are defined.
2. Determine if processes, procedures and technical measures, for verification of access authorization to data and system functions, are implemented and consistently followed in practice.</td></tr>
</table>

2.11 Interoperability & 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>Auditing Guidelines</b>
1. Examine policy for adequacy, currency, communication, and effectiveness.
2. Examine the inventory of documentation that establishes the requirements and communication of this control.
3. Examine policy and procedures for evidence of review at least annually.</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>Auditing Guidelines</b>
1. Examine the list of Application Programming Interfaces (API) available to Cloud Service Consumers.
2. Determine if such list and usable documentation is made available to Cloud Service Consumers.</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>Auditing Guidelines</b>
1. Examine the policy for the secure transmission of requests and data.
2. Inspect the requirements, with respect to any security domains defined.
3. Examine the policy that specifies protocols for transmission, with respect to standardization.</td></tr>
</table>

Control Title	Control ID	Control Specification
Data Portability Contractual Obligations	IPY-04	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

Auditing Guidelines

1. Examine the standard form of contract for offboarding the Cloud Service Consumers.
2. Determine if non-standard clauses allow the Cloud Service Consumers to waive such rights.
3. Determine if there are requests for data in unsupported formats.
4. Examine the policy regarding deletion of resources no longer in the control of a client, and determine if such policy corresponds to the contractual data retention.

2.12 Infrastructure & Virtualization Security (IVS)

Control Title	Control ID	Control Specification
Infrastructure and Virtualization Security Policy and Procedures	IVS-01	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.

Auditing Guidelines

1. Interview the team to determine if policy and procedures have been documented.
2. Evaluate the documented policy to determine if it has been approved and communicated to the relevant internal and external teams.
3. Determine if the policy has been applied to the infrastructure and virtualization security operations and if relevant procedures have been drafted.
4. Determine if the procedures are periodically evaluated and if they are maintained, up to date, and relevant.
5. Determine if policy and procedures are reviewed and updated on an annual basis. Policy may contain segregation of environments and roles, change management requirements and continuous exercising.

Control Title	Control ID	Control Specification
Capacity and Resource Planning	IVS-02	Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business.

Auditing Guidelines

1. Determine if the business requirements for system performance are available.
2. Determine if evidence exists that points to planning and monitoring of the availability, quality and capacity of resources.
3. Determine if evidence exists that establishes that the plan is appropriate and adequate to meet the expectations of the business requirements established in the first guideline.

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.

Auditing Guidelines

1. Examine the policy for communication between environments.
2. Examine the criteria for business justification of communication, and reviews.
3. Determine if the inventory of allowed communication has been reviewed, at least annually.
4. Evaluate the effectiveness of the monitoring and encryption of such communication.
5. Evaluate the details of business justification, and its review.

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.

Auditing Guidelines

1. Determine if the host and the guest OS has been hardened as per best practices.
2. Determine if the hypervisor or infrastructure control planes are hardened as per best practices.
3. Determine if appropriate technical controls exist that ensure that the hardening is done.
4. Determine if a security baseline has been set up.
5. Determine if the security baseline contains information about the hardening done.

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

Auditing Guidelines

1. Verify if production and non-production environments are appropriately segregated.
2. Verify if the segregation is reviewed and managed during change management.
3. Verify the classification of data contained in each environment.

<table>
<tr><td>Control Title
Segmentation and Segregation</td><td>Control ID
IVS-06</td><td>Control Specification
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.</td></tr>
<tr><td colspan="3">Auditing Guidelines
1. Review evidence to verify that the design and development of applications and infrastructure ensure appropriate best practices such as hardening, segmentation, and segregation is incorporated and the shared responsibility model between the CSP and CSC is maintained.
2. Review evidence to verify that the deployment and configuration of applications and infrastructure follow appropriate hardening, segmentation, and segregation is incorporated and the shared responsibility model between the CSP and CSC is maintained.
3. Review evidence to determine that segmentation and segregation is monitored.
4. Review evidence to determine that the tenants are isolated from each other.</td></tr>
<tr><td>Control Title
Migration to Cloud Environments</td><td>Control ID
IVS-07</td><td>Control Specification
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">Auditing Guidelines
1. Examine the list of environments that will be the target of migrations.
2. Examine the criteria for maintaining a list of approved protocols.
3. Examine the records of migrations.</td></tr>
<tr><td>Control Title
Network Architecture Documentation</td><td>Control ID
IVS-08</td><td>Control Specification
Identify and document high-risk environments.</td></tr>
<tr><td colspan="3">Auditing Guidelines
1. Examine the criteria for identifying high-risk environments.
2. Examine the inventory of high-risk environments, and periodicity of review.</td></tr>
<tr><td>Control Title
Network Defense</td><td>Control ID
IVS-09</td><td>Control Specification
Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks.</td></tr>
</table>

Auditing Guidelines

1. Interview the team to evaluate if they have defined processes and procedures for protection, detection and timely response to address network based attacks.
2. Review evidence to establish that the defined processes and procedures have been implemented.
3. Review evidence to establish that the processes and procedures are evaluated and validated periodically.
4. Review evidence to establish that the processes and procedures are based upon a defense-in-depth.
5. Review evidence to support the effective activation of incident response plans when necessary including the associated communication protocols.

2.13 Logging and Monitoring (LOG)

Control Title	Control ID	Control Specification
Logging and Monitoring Policy and Procedures	LOG-01	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.

Auditing Guidelines

1. Examine policy and procedures for adequacy, approval, communication, and effectiveness as applicable to planning, delivery and support of the organization's logging and monitoring requirements.
2. Examine policy and procedures for evidence of review at least annually.

Control Title	Control ID	Control Specification
Audit Logs Protection	LOG-02	Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs.

Auditing Guidelines

1. Examine the organisation's log retention requirements.
2. Evaluate the policy and technical measures with respect to effectiveness.

Control Title	Control ID	Control Specification
Security Monitoring and Alerting	LOG-03	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.

<table>
<tr><td colspan="3"><b>Auditing Guidelines</b>
1. Examine policy related to the security monitoring and alerting, and determine if security-related events within applications and the underlying infrastructure are identified.
2. Examine processes related to identifying responsible stakeholders for the purpose of alerting.
3. Evaluate the implementation with respect to effectiveness, and conduct a review of metrics.</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>Auditing Guidelines</b>
1. Examine policy related to the protection of log information.
2. Determine if the control requirements stipulated in the policy have been implemented.
3. Examine policy related to the maintenance of access records.</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>Auditing Guidelines</b>
1. Examine policy for the monitoring of audit logs.
2. Determine if policy and patterns have been established for anomalous activities.
3. Examine policy for the review of, and timely action on anomalies.</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>
<tr><td colspan="3"><b>Auditing Guidelines</b>
1. Examine policy that establishes the time scale and epoch, or traceability, of time across systems.
2. Evaluate the process that ensures synchronization of time on relevant systems.</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>Auditing Guidelines</b>
1. Examine policy for the identification of loggable events, applications, or systems.
2. Examine the outputs of such identification, with respect to review and approval.
3. Examine scope for evidence of review at least annually.</td></tr>
</table>

Control Title	Control ID	Control Specification
Log Records	LOG-08	Generate audit records containing relevant security information.

Auditing Guidelines

1. Examine policy related to audit logging and determine if it includes requirements to generate audit records containing relevant security information.
2. Examine audit records and determine if they adequately reflect the policy.

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

Auditing Guidelines

1. Examine policy for the protection of audit records.
2. Evaluate the use of technical measures in the protection of audit records.

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.

Auditing Guidelines

1. Examine policy related to the monitoring and reporting of operations of cryptographic policy.
2. Examine the process to identify such a policy.
3. Evaluate the effectiveness of such reporting capability.

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.

Auditing Guidelines

1. Examine policy for logging and monitoring usage of cryptographic key usage lifecycle events.
2. Examine the process to identify such events.
3. Evaluate the review of these logs.

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

Auditing Guidelines

1. Examine policy for logging and monitoring physical access.
2. Examine the process to identify such events.
3. Evaluate the review of these logs.

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.

Auditing Guidelines

1. Examine the policy for reporting of anomalies and failures of the monitoring system.
2. Examine the process for identifying accountable parties.

2.14 Security Incident Management, E-Discovery, & 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.

Auditing Guidelines

1. Examine policy for adequacy, approval, communication, and effectiveness as applicable to planning, delivery and support of the organization's Security Incident Management, E-Discovery and Cloud Forensics.
2. Examine policy and procedures for evidence of review at least annually.

Control Title	Control ID	Control Specification
Service Management Policy and Procedures	SEF-02	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.

Auditing Guidelines

1. Examine the policy for adequacy, approval, communication, and effectiveness as applicable to planning, delivery and support of the organization's Security Incident Management, with respect to timely management.
2. Examine the policy and procedures for evidence of review at least annually.

Control Title	Control ID	Control Specification
Incident Response Plans	SEF-03	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.

Auditing Guidelines

1. Examine the policy for adequacy, approval, communication, and effectiveness as applicable to planning, delivery and support of the organization’s Security Incident Management, with respect to timely management.
2. Examine the processes to identify impacted stakeholders.
3. Determine if this plan meets stakeholder requirements.

Control Title	**Control ID**	**Control Specification**
Incident Response Testing	SEF-04	Test and update as necessary incident response plans at planned intervals or upon significant organizational or environmental changes for effectiveness.

Auditing Guidelines

1. Verify if there is a calendar of exercises available, if exercises are performed at planned intervals and when there are significant changes within the organization or the context in which it operates.
2. Verify if the organization has reviewed and acted upon the results of its exercising and testing to implement changes and improvements.

Control Title	**Control ID**	**Control Specification**
Incident Response Metrics	SEF-05	Establish and monitor information security incident metrics.

Auditing Guidelines

1. Verify that metrics have been established to measure information security incidents.
2. Verify that metrics together demonstrate the efficacy, effectiveness and success of the information security incident response plan to address incidents as they happen.
3. Verify that the metrics are measured and reported to stakeholders.

Control Title	**Control ID**	**Control Specification**
Event Triage Processes	SEF-06	Define, implement and evaluate processes, procedures and technical measures supporting business processes to triage security-related events.

Auditing Guidelines

1. Verify if operational processes that help the organization to prepare for, identify, detect, protect, respond to and recover from information security incidents in a step-by-step manner exist.
2. Verify if tools that support these organizational procedures to triage security related events complement the ability of the teams to detect, review, monitor and quickly decide upon the context and the possible impact of the incident as it happens and over time.

Control Title	**Control ID**	**Control Specification**
Security Breach Notification	SEF-07	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.

Auditing Guidelines

1. Examine policy for adequacy, approval, communication, and effectiveness as applicable to planning, delivery and support of the organization's Security Breach Notification management.
2. Verify if there is a formal program that documents the breach notification requirements for all regulatory or contractual domains that the organization asserts adherence to.
3. Verify if there is a periodic awareness program to ensure all those associated with information security incident response are aware of the procedures involved for their roles, responsibilities and authorities.
4. Determine if the organization has established breach notification Time Objectives for information security breaches that meet the minimum expectation of the applicable regulation and verify if those time objectives are reflected in all internal and external service level expectations.

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.

Auditing Guidelines

1. Examine the process used to determine applicable points of contact, and the procedure for reviewing the list/documentation that contains them.
2. Verify if the organization has updated the list of points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.
3. Examine when the last updates were done and if there is a schedule for reviewing and updating these contacts.

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

Control Title	Control ID	Control Specification
SSRM Policy and Procedures	STA-01	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.

Auditing Guidelines

1. Examine policy for adequacy, approval, communication, currency, and effectiveness.
2. Examine policy and procedures for evidence of review at least annually.

Control Title	Control ID	Control Specification
SSRM Supply Chain	STA-02	Apply, document, implement and manage the SSRM throughout the supply chain for the cloud service offering.

Auditing Guidelines

1. Examine the policy for provisions related to service delivery.
2. Evaluate the process for communication of requirements and service levels to vendors and other third-parties.
3. Determine if a review of effectiveness is in place, especially with respect to contractual requirements.

Control Title	**Control ID**	**Control Specification**
SSRM Guidance	STA-03	Provide SSRM Guidance to the CSC detailing information about the SSRM applicability throughout the supply chain.

Auditing Guidelines

1. Examine whether SSRM guidance documentation has been approved by management and communicated to CSCs.
2. Examine the process for review of SSRM Guidance if required.

(Note: This control applies to an Organization that is in the role of a CSP).

Control Title	**Control ID**	**Control Specification**
SSRM Control Ownership	STA-04	Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM for the cloud service offering.

Auditing Guidelines

1. Examine the policy for assessing, demarcating, and documenting the interfaces at the edges of the organisation’s responsibility.
2. Determine if the delineation has been done, and is current.
3. Examine the process for communicating the security responsibility boundaries to third-parties.

(Note: This control applies to an Organization that is in the role of a CSP).

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

Auditing Guidelines

1. Examine the policy for assessing, demarcating, and documenting the interfaces at the edges of the Organisation’s responsibility.
2. Examine the process for validating the boundaries for cloud services used.
3. Examine the process for validating the seamlessness of controls for cloud services used.

(Note: This control applies to an Organization that is in the role of a CSC).

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.

Auditing Guidelines

1. Examine the policy related to addressing security in third-party agreements and determine if organizations employ formal contracts.
2. Determine if written procedures exist for addressing security in third-party agreements and whether or not the procedure(s) address(es) each element of the policy/control requirement(s) stipulated in the policy level.
3. Examine relevant documentation, observe relevant processes, and/or interview the control owner(s), and/or relevant stakeholders, as needed, for addressing security in third-party agreements and determine if the policy/control requirements stipulated in the policy level have been implemented.
4. Examine measure(s) that evaluate(s) the organization's compliance with the third-party management policy and determine if the measure(s) address(es) implementation of the policy/control requirement(s) as stipulated in the policy level.

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

Auditing Guidelines

1. Determine if there is an inventory maintained of all supply chain relationships.
2. Establish ownership for maintaining this inventory.
3. Examine the inventory's records to establish whether CSP/CSC relationships are maintained in this inventory.
4. Determine whether this inventory is subject to review.

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.

Auditing Guidelines

1. Examine the policy related to identification of risks related to external parties and determine if the organization conducts due diligence of the external party.
2. Determine if the policy/control requirements stipulated in the policy level have been implemented.
3. Determine the periodicity of review of risk factors.

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

Auditing Guidelines

1. Examine the policy for inclusion of the Control in third party agreements.
2. Examine the policy related to the review of third-party services to determine if the organization incorporates compliance by third parties.

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

Auditing Guidelines

1. Determine if a documented review schedule of CSP-CSC supply chain agreements exists on an annual basis and is operating.
2. Examine the organization's implementation of its third-party management policy.

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.

Auditing Guidelines

1. Examine the process for determining the standards and policy that service level agreements must conform to.
2. Examine the process to determine contractual, legal, and technical requirements applicable to service level agreements
3. Determine if internal assessments are defined, planned, and executed, at least annually.

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.

Auditing Guidelines

1. Examine the policy for incorporation of requirements into contractual documents throughout the CSP's supply chain.
2. Determine if requirements have been incorporated in contracts.
3. Evaluate if the right to audit is protected, where required.

Control Title	Control ID	Control Specification
Supply Chain Governance Review	STA-13	Periodically review the organization's supply chain partners' IT governance policies and procedures.

Auditing Guidelines

1. Examine the policy for review of supply chain partners governance of IT.
2. Determine if the right to review is incorporated contractually.
3. Evaluate whether such a review cycle is operating within the organization.

Control Title	Control ID	Control Specification
Supply Chain Data Security Assessment	STA-14	Define and implement a process for conducting security assessments periodically for all organizations within the supply chain.

Auditing Guidelines

1. Examine the policy related to the security assessments of the supply chain.
2. Examine the policy related to identification of risks related to external parties.
3. Determine if procedures exist for identification of risks related to external parties
4. Evaluate evidence of the conduct of assessments of organisations within the supply chain, periodically as required by the policy.

2.16 Threat & Vulnerability Management (TVM)

Control Title	Control ID	Control Specification
Threat and Vulnerability Management Policy and Procedures	TVM-01	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.

Auditing Guidelines

1. Examine policy for adequacy, currency, communication, and effectiveness.
2. Examine policy and procedures for evidence of review at least annually.

<table>
<tr><td>Control Title
Malware Protection Policy and Procedures</td><td>Control ID
TVM-02</td><td>Control Specification
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>
<tr><td colspan="3">Auditing Guidelines
1. Examine policy for adequacy, currency, communication, and effectiveness.
2. Examine policy and procedures for evidence of review at least annually.</td></tr>
<tr><td>Control Title
Vulnerability Remediation Schedule</td><td>Control ID
TVM-03</td><td>Control Specification
Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk.</td></tr>
<tr><td colspan="3">Auditing Guidelines
1. Examine policy for adequacy, currency, and effectiveness.
2. Determine if technical measures are evaluated for effectiveness.</td></tr>
<tr><td>Control Title
Detection Updates</td><td>Control ID
TVM-04</td><td>Control Specification
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.</td></tr>
<tr><td colspan="3">Auditing Guidelines
1. Examine policy for adequacy, currency, and effectiveness.
2. Determine if technical measures are evaluated for effectiveness.
3. Determine if updates and reviews of indicators are conducted at least weekly.</td></tr>
<tr><td>Control Title
External Library Vulnerabilities</td><td>Control ID
TVM-05</td><td>Control Specification
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.</td></tr>
<tr><td colspan="3">Auditing Guidelines
1. Examine policy for adequacy, currency, and effectiveness.
2. Determine if a process exists to identify third-party libraries, and to evaluate their impact on the organization’s vulnerability management.</td></tr>
<tr><td>Control Title
Penetration Testing</td><td>Control ID
TVM-06</td><td>Control Specification
Define, implement and evaluate processes, procedures and technical measures for the periodic performance of penetration testing by independent third parties.</td></tr>
</table>

Auditing Guidelines

1. Examine policy for adequacy, currency, and effectiveness.
2. Determine if the process for defining frequency of penetration testing is defined.
3. Determine if the process for selection of independent third parties is defined, and evaluated.

Control Title	Control ID	Control Specification
Vulnerability Identification	TVM-07	Define, implement and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organizationally managed assets at least monthly.

Auditing Guidelines

1. Examine policy for adequacy, currency, and effectiveness.
2. Determine if vulnerability detection is undertaken as required, and at least monthly.

Control Title	Control ID	Control Specification
Vulnerability Prioritization	TVM-08	Use a risk-based model for effective prioritization of vulnerability remediation using an industry recognized framework.

Auditing Guidelines

1. Examine policy and procedures related to prioritization of vulnerabilities detected.
2. Determine if an industry recognized or widely used framework is implemented.
3. Examine how the output of risk assessment of the vulnerabilities is used to inform prioritization of remediation.
4. Determine if the process is evaluated for effectiveness.

Control Title	Control ID	Control Specification
Vulnerability Management Reporting	TVM-09	Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification.

Auditing Guidelines

1. Examine policy and procedures related to tracking and reporting of vulnerabilities.
2. Examine the process to identify stakeholders.
3. Determine if the process is implemented.

Control Title	Control ID	Control Specification
Vulnerability Management Metrics	TVM-10	Establish, monitor and report metrics for vulnerability identification and remediation at defined intervals.

Auditing Guidelines

1. Verify that metrics have been established to measure vulnerabilities.
2. Examine the process for reporting metrics, including identification of recipients.
3. Determine if reports are sent at the defined intervals.

2.17 Universal Endpoint Management (UEM)

<table>
<tr><td>**Control Title**
Endpoint Devices Policy and Procedures</td><td>**Control ID**
UEM-01</td><td>**Control Specification**
Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. Review and update the policies and procedures at least annually.</td></tr>
<tr><td colspan="3">**Auditing Guidelines**
1. Examine policy for adequacy, currency, communication, and effectiveness.
2. Examine policy and procedures for evidence of review, at least annually.</td></tr>
<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">**Auditing Guidelines**
1. Determine if a list of approved services, applications and sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data have been identified and documented.
2. Determine if the identified and documented list of approved services, applications and sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data have been enforced.
3. Examine how endpoints are monitored for unauthorized services and the process to remove or terminate use of non-sanctioned resources.</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">**Auditing Guidelines**
1. Examine the process for endpoint compatibility validation.
2. Determine if the process produces a published compatibility matrix.</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">**Auditing Guidelines**
1. Examine the asset register, with reference to endpoints.
2. Determine if endpoints that store and access company data are tagged and included in the asset inventory.</td></tr>
</table>

<table>
<tr><td>**Control Title**
Endpoint Management</td><td>**Control ID**
UEM-05</td><td>**Control Specification**
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">**Auditing Guidelines**
1. Examine procedures for adequacy, currency, communication, and effectiveness.
2. Determine the extent and applicability of the processes, procedures, and technical measures over applicable endpoints, as identified.
3. Examine policy and procedures for evidence of review, with respect to effectiveness.</td></tr>
<tr><td>**Control Title**
Automatic Lock Screen</td><td>**Control ID**
UEM-06</td><td>**Control Specification**
Configure all relevant interactive-use endpoints to require an automatic lock screen.</td></tr>
<tr><td colspan="3">**Auditing Guidelines**
1. Determine the organisation's definition of interactive-use endpoints.
2. Examine the processes and technical measures in place to enforce automatic lock screens.</td></tr>
<tr><td>**Control Title**
Operating Systems</td><td>**Control ID**
UEM-07</td><td>**Control Specification**
Manage changes to endpoint operating systems, patch levels, and/or applications through the company's change management processes.</td></tr>
<tr><td colspan="3">**Auditing Guidelines**
1. Examine the organisation's change management policy for controls related to changes on endpoints.
2. Determine if such controls are in place for making changes to production and infrastructure systems and if the controls are evaluated as effective.</td></tr>
<tr><td>**Control Title**
Storage Encryption</td><td>**Control ID**
UEM-08</td><td>**Control Specification**
Protect information from unauthorized disclosure on managed endpoint devices with storage encryption.</td></tr>
<tr><td colspan="3">**Auditing Guidelines**
1. Examine the organisation's asset disposal policy for end-of-life security requirements.
2. Examine the organisation's policy on encryption or otherwise protection of data at rest on endpoints.
3. Determine if such controls are in place and evaluated as effective.</td></tr>
<tr><td>**Control Title**
Anti-Malware Detection and Prevention</td><td>**Control ID**
UEM-09</td><td>**Control Specification**
Configure managed endpoints with anti-malware detection and prevention technology and services.</td></tr>
<tr><td colspan="3">**Auditing Guidelines**
1. Examine the organisation's anti-malware policy.
2. Determine if such controls are in place and evaluated as effective.</td></tr>
</table>

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

Auditing Guidelines

1. Examine the organisation's software firewall and other endpoint network protection policy.
2. Examine the policy on configuration of such controls.
3. Determine if such controls are in place and evaluated as effective.

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.

Auditing Guidelines

1. Examine the organisation's data loss policy.
2. Examine the policies on configuration of such controls.
3. Determine if such controls are driven by risk assessments.
4. Determine if such controls are in place and evaluated as effective.

Control Title	Control ID	Control Specification
Remote Locate	UEM-12	Enable remote geo-location capabilities for all managed mobile endpoints.

Auditing Guidelines

1. Examine the organisation's remote geo-location for managed mobile endpoints policy.
2. Determine if such controls are in place.

Control Title	Control ID	Control Specification
Remote Wipe	UEM-13	Define, implement and evaluate processes, procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices.

Auditing Guidelines

1. Examine procedures for adequacy, currency, communication, and effectiveness.
2. Determine the extent and applicability of the processes, procedures, and technical measures over managed endpoints, as identified.
3. Examine policy and procedures for evidence of review, with respect to effectiveness.

Control Title	Control ID	Control Specification
Third-Party Endpoint Security Posture	UEM-14	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.

Auditing Guidelines

1. Examine procedures for adequacy, currency, communication, and effectiveness.
2. Determine the organisation's definition of third-party endpoints.
3. Determine the extent and applicability of the processes, procedures, and technical measures over third-party endpoints.
4. Examine policy and procedures for evidence of review, with respect to effectiveness.

Acronyms

API	Application Programming Interface
CAIQ	Consensus Assessments Initiative Questionnaire
CSC	Cloud Service Customer
CSP	Cloud Service Provider
DLP	Data Loss Prevention
DPIA	Data Protection Impact Assessment
ERM	Enterprise Risk Management
HSM	Hardware Security Modules
IaaS	Infrastructure as a Service
ISO/ IEC	International Organization for Standardization and the International Electrotechnical Commission
KMS	Key Management Services
MFA	Multi Factor Authentication
OS	Operating System
PaaS	Platform as a Service
PII	Personally Identifiable Information
SaaS	Software as a Service
SDLC	Software Development Life Cycle
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SSRM	Shared Security Responsibility Model

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.

Business continuity planning (BCP)
It is a broad disaster recovery approach whereby enterprises plan for recovery of the entire business process. This includes a plan for workspaces, telephones, workstations, servers, applications, network connections and any other resources required in the business process.

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 the 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 keys.

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 codebased entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

Management System
It is a set of policies, processes and procedures used by an organization to ensure that it can fulfill the tasks required to achieve its objectives. These objectives cover many aspects of the organization's operations (including financial success, safe operation, product quality, client relationships, legislative and regulatory conformance and worker management).

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.

Operational resilience
Is defined as initiatives that expand business continuity management programs to focus on the impacts, connected risk appetite and tolerance levels for disruption of product or service delivery to internal and external stakeholders (such as employees, customers, citizens and partners).

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.