.





**MSECB Certification - ISO/IEC 27001:2022, ISO/IEC 27018:2019 and CSA STAR Certification**

*Management System Audit Report*

*of* **Company ABC**

**DISTRIBUTION**

The content of this report must not be disclosed to a third party without the agreement of the MSECB Client.

**DISCLAIMER**

This report has been prepared by MSECB in respect of a client's application for assessment by MSECB. The purpose of the report is to verify the Client's conformance with the management system standard(s) or other criteria specified. The content of this report applies only to matters, which were evident to MSECB at the time of the audit within the audit scope. MSECB does not warrant or otherwise comment upon the suitability of the contents of the report or the certificate for any particular purpose or use. MSECB accepts no liability whatsoever for consequences to, or actions taken by, third parties as a result of or in reliance upon information contained in this report or certificate.

This audit is based on a sampling process of the available information and the auditors nor MSECB can guarantee that all, if any, non-conformities have been discovered.

1. Audit information 4

1.1. Organization information 5

1.2. Audit information 5

1.3. Audit Scope 6

2. Audit preparation and methodology 7

2.1. Audit objectives 7

2.2. Audit criteria 7

2.3. Audit methodology 8

2.4. Previous audit results 8

2.5. Audit planning 9

2.6. Key people interviewed 9

2.7. MSECB complaint and appeal process 9

3. Significant audit trails followed 10

4. Audit findings 70

4.1. Audit finding definition 70

4.2. Major nonconformities (see also Annex A) 71

4.3. Minor nonconformities (see also Annex A) 71

4.4. Observations 71

4.5. Opportunities for improvement 71

4.6. Agreed follow-up activities 71

4.7. Uncertainty / obstacles that could affect the reliability of audit conclusions 71

4.8. Unresolved diverging opinions between the audit team & auditee 71

5. Audit conclusions and audit recommendation 72

5.1. System management conformance and capability 72

5.2. Audit conclusions 72

5.3. Recommendation 72

6. Annex A: Nonconformity report 73

6.1. Nonconformity Report 73

7. Annex B: Certification Information 74

8. Annex C: Surveillance Plan 75

**Executive Summary**

I have audited the Management System (MS) of Company ABC (Organization Name) from May 12th to May 15th 2022.The main objective of this audit was to assess if the MS has been successfully implemented and effective, as well as to evaluate the conformance of the organization to the ISO/IEC 27001:2022, ISO/IEC 27018:2019 and CSA Star requirements. Based on these assessments and evaluations, a decision has been made whether or not to recommend your organization for certification against ISO/IEC 27001:2022, ISO/IEC 27018:2019 and CSA Star Certification.

The audit team has conducted the audit based on the organization’s defined processes in correspondence with the audit plan. The audit conducted by a professional team was a process-based audit with a focus on the significant aspects, risks and objectives.

The CSA STAR Certification is an independent third-party audit of a cloud service provider's (CSP) security that combines ISO/IEC 27001 criteria with the CSA Cloud Controls Matrix (CCM). The following table was used to assess the maturity level for each CCM control and overall domain with a score from 1 to 15:

|  |  |
| --- | --- |
| **Score** | **Descriptor** |
| 1-3 | No Formal Approach |
| 4-6 | Reactive Approach |
| 7-9 | Proactive Approach |
| 10-12 | Improvement-Based Approach |
| 13-15 | Optimizing Approach |

In order to make it possible for an assessor to consistently apply a score to the control area, the grid below outlines what would be required of an organization to achieve each score.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Score** | **1 to 3** | **4 to 6** | **7 to 9** | **10 to 12** | **12 to 15** |
|  | **No formal approach** | **Reactive** | **Proactive** | **Improving** | **Optimizing** |
| **Evidence/definition** | 1. There is noevidence of asystem in place tomanage thecontrol area. | 4. There isevidence of asystem in placeto cover the keyoperations in thecontrol area.Where required,the system isdocumented. | 7. There isevidence of arobust system inplace that coversall routineoperations in thecontrol area. | 10. There isevidence thesystem formanaging thecontrol area iscapable ofmanagingcontingencyevents as well asroutine activity.r | 13. Control areaowners candemonstrate thatthey activelyreview bestpractice fromtheir industry andacross theirorganization andapply it to thecontrol area. |
| **Managed** | 2. There is someevidence of eithera documentedsystem or anaccepted way ofworking is inplace. | 5. There is aclearly identifiedowner for thecontrol area whounderstands theirscope ofresponsibility. | 8. There isevidence that thecontrol area isactivelymonitored andmeasured andaction evaluatedbased on theevidence. | 11. Input from avariety of sourcesis considered todecide how tomanage risk andimprove operationsin thiscontrol area. | 14. Control areaowners activelyshare bestpractice tosupport developmentin otherareas of theorganizationbased on theirexperience in thiscontrol area. |
| **Followed/effective** | 3. There is someevidence of anaccepted way ofworking that isbroadly understoodandfollowed. | 6. There isevidence thesystem isunderstood androutinelyfollowed. | 9. There isevidence thatcritical peopleoperating in thecontrol area areappropriatelytrained/skilled tomanage routineoperations in thecontrol area. | 12. There isevidence thatinputs from arange ofstakeholders andmonitoring andmeasuringsystems havebeen taken intoaccount whenimprovingoperations in thecontrol area. | 15. Changes inthe control areaare evaluatedagainst thestrategicobjective of theorganization. |

Depending on the capability level the client achieves their audit report will categories there performance against the maturity model as either:

|  |  |
| --- | --- |
| **Overall Score** | **Award** |
| Less than 3 | No Award |
| 3-6 | Bronze Award |
| 6-9 | Silver Award |
| Greater than 9 | Gold Award |

If the organization has an average score between 3 and 6, they will get a bronze level. If the organization has an average score between 6 and 9 they will get a silver level. If the organization has an average score greater than 9 they will get a gold level. According to CSA STAR guidelines, if a major nonconformity were noted in a control domain, the maximum possible score would be 6; if a minor nonconformity were noted in a control domain, the maximum possible score would be 9.

# Audit information

## Organization information

|  |  |
| --- | --- |
| Company name: |  |
| Contract number: |  |
| Phone number: |  |
| Website: |  |
| Total number of employees: |  |
| Total number of employees within the scope:Please provide justification for the employees that are not included in the certification scope. |  |
|  |
| Contact name: |  |
| Contact email: |  |
| Contact phone: |  |

|  |
| --- |
| Sites: |
| **Site #** | **Street Address** | **City** | **State, Province, Country** | **Zip Code** | **# of Employees** |
| 1 (main) |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |

## Audit information

|  |  |
| --- | --- |
| Audit standard(s): |  |
| Audit type: | [ ]  Initial Audit | [ ]  Surveillance 1 |
| [ ]  Recertification | [ ]  Surveillance 2 |
| [ ]  Other: |
| Date(s) of audit(s): |  |
| Duration: |  |
| Audit team leader: |  |
| Additional team member(s): |  |
| Additional attendees and roles: |  |

|  |  |
| --- | --- |
| **Site #** | **Sites Audited** |
| 1 (main) | [ ]  |
| 2 | [ ]  |
| 3 | [ ]  |
| 4 | [ ]  |

## Audit Scope

|  |  |
| --- | --- |
| Certification audit scope: |  |
| Date and version of scope statement: |  |
| Has scope changed since last audit?  |  |
| All scope exclusions are appropriate and justified:Important Note\* Excluded clauses in the audited Management System shall be put in the certificate |  |

# Audit preparation and methodology

## Audit objectives

The main purpose of this audit is to evaluate the implementation and effectiveness of the Information Security Management (ISMS) including evaluation of conformity to the requirements of ISO/IEC 27001:2022, ISO/IEC 27018:2019 and CSA Star requirements.

The specific objectives of this audit are to confirm that:

* The organization has determined the boundaries and applicability of the MS in scope;
* The management system conforms with all the requirements of the audit standard (Clause 4 to 10 of ISO/IEC 27001:2022, ISO/IEC 27018:2019 and CSA Star requirements);
* The management system conforms with all applicable legal and regulatory requirements;
* The management system is capable of achieving the objectives of the organization’s policies;
* The organization has established, implemented, maintained and continually improved its MS, including the processes needed and their interactions, in accordance with the requirements of the ISO/IEC 27001:2022, ISO/IEC 27018:2019 and CSA Star requirements*.*

## Audit criteria

The audit criteria (the set of requirements) for this audit are all normative clauses of ISO/IEC 27001:2022, ISO/IEC 27018:2019 and CSA Star requirements:

* Clause 4 – Context of the organization
* Clause 5 – Leadership
* Clause 6 – Planning
* Clause 7 – Support
* Clause 8 – Operation
* Clause 9 – Performance Evaluation
* Clause 10 – Improvement
* Annex A – Control objectives and controls
* Additional requirements
	+ Use of logo and trademark
* Documentation and processes defined in the management system developed by the client

***CSA STAR***

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

## Audit methodology

[Please explain the methodology used by the audit team to perform this audit, similar to the sample below]

The audit team has conducted a process-based audit focusing on the significant aspects, risks and objectives. The auditors have used audit procedures to collect evidence in sufficient quantity and quality to validate the conformity of the management system of the organization. The use of audit procedures in a systematic way reduces the audit risk and reinforces the objectivity of the audit conclusions.

The audit team has used a combination of evidence collection procedures to create their audit test plan. The audit methods used consisted of interviews, observations of activities, review of documentation and records, technical tests and analysis of sampling.

The analysis procedure allows the audit team to draw conclusions concerning a whole by examining a part. It allows the auditor to estimate characteristics of a population by directly observing a part of the whole population. The sampling method used during this audit was a systematic sampling (or interval sampling) technique with a margin error of 3 to 5 %.

Technical tests, including testing of the effectiveness of a process or control have not been performed by the auditors themselves. The operations have always been performed by the personnel of the auditee.

## Previous audit results

The results of the last audit of this system have been reviewed, in preparation for this audit in particular to assure appropriate correction and corrective action have been implemented to address any nonconformity identified. This review has concluded that:

[ ]  any nonconformity identified during previous audits has been corrected and the corrective action continues to be effective

[ ]  any nonconformity identified during previous audits hasn’t been addressed adequately and the specific issue has been re-defined in the nonconformity section of this report

[ ]  N/A (no previous audits or no nonconformities during the previous audit)

## Audit planning

[Please describe how the audit was planned by the audit team. Please check the example below]

*The team leader of the audit has established an initial contact with the auditee to make arrangement for this audit, including scheduling the dates. The team leader has validated the feasibility of the audit, the audit objectives, the audit scope, the location and the audit criteria.*

*The audit plan was sent to the auditee and it was confirmed before the opening meeting between the audit team and the auditee.*

*The onsite audit was started with an opening meeting which has been attended by the general manager and the ISMS responsible. The MSECB profile, audit purpose, methodology, reporting system, appeal process and confidentiality were briefly presented to the client during the opening meeting.*

## Key people interviewed

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Title** | **Department / Process** | **Opening Meeting (Yes or No)** | **Closing Meeting (Yes or No)** | **Date of interviewing** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## MSECB complaint and appeal process

Any client may appeal any decision made by the audit team. Appeals must be in writing and are addressed using MSECB’ procedure for handling appeals and disputes. If MSECB fails to resolve the appeal to the organization’s satisfaction, the appeal can be escalated to MSECB Advisory Board.

MSECB Complaint and Appeal Procedure: [www.msecb.com](http://www.msecb.com)

# Significant audit trails followed

**Notes on usage by the auditor:**

*Under the column “Status”, please use the following key to record your assessment result for each clause:*

***A*** *= Acceptable,*

***N/A*** *= Not Applicable (Out of Scope),*

***MaNC*** *= Major Nonconformity*

***MiNC*** *= Minor Nonconformity*

***OBS*** *= Observation*

***OFI*** *= Opportunity for improvement*

*\*nonconformities are explained in “Section 4: Audit Findings”.*

*Evidence should be provided also for ‘Acceptable’ clauses.*

*If nonconformity is identified (Minor or Major), please include the number of the nonconformity in the column “No. of NC”. Detailed description of the nonconformity should be provided in Annex A – Nonconformity Report.*

*If OBS or OFI is identified, please explain in detail the finding(s) in section 4.4 and 4.5.*

| **Clause****Requirement** | **Status** | **Audit Evidence** | **No. of NC** |
| --- | --- | --- | --- |
|  |  | Findings/justification of findings/specifics/notes |  |
| **4 Context of the organization** |
| 4.1 | Understanding the organization and its context |  |  |  |
| 4.2 | Understanding the needs and expectations of interested parties |  |  |  |
| 4.3 | Determining the scope of the ISMS |  |  |  |
| 4.4 | Information security management system |  |  |  |
| **5 Leadership** |
| 5.1  | Leadership and commitment |  |  |  |
| 5.2 | Policy |  |  |  |
| 5.3  | Organizational roles, responsibilities and authorities |  |  |  |
| **6 Planning** |
| 6.1 | Actions to address risks and opportunities |  |  |  |
| 6.1.1 | General |  |  |  |
| 6.1.2 | Information security risk assessment |  |  |  |
| 6.1.3 | Information security risk treatment |  |  |  |
| 6.2 | Information security objectives and planning to achieve them |  |  |  |
| 6.3 | Planning of changes |  |  |  |
| **7 Support** |
| 7.1 | Resources |  |  |  |
| 7.2 | Competence |  |  |  |
| 7.3 | Awareness |  |  |  |
| 7.4 | Communication |  |  |  |
| 7.5 | Documented information |  |  |  |
| 7.5.1 | General |  |  |  |
| 7.5.2 | Creating and updating |  |  |  |
| 7.5.3 | Control of documented information |  |  |  |
| **8 Operation** |
| 8.1 | Operational planning and control |  |  |  |
| 8.2 | Information security risk assessment |  |  |  |
| 8.3 | Information security risk treatment |  |  |  |
| **9 Performance evaluation** |
| 9.1 | Monitoring, measurement, analysis and evaluation |  |  |  |
| 9.2 | Internal audit |  |  |  |
| 9.2.1 | General |  |  |  |
| 9.2.2 | Internal audit progra |  |  |  |
| 9.3 | Management review |  |  |  |
| 9.3.1 | General |  |  |  |
| 9.3.2 | Management review inputs |  |  |  |
| 9.3.3 | Management review results |  |  |  |
| **10 Improvement** |
| 10.1 |  Continual improvement |  |  |  |
| 10.2 |  Nonconformity and corrective |  |  |  |

|  |
| --- |
| **11. Additional requirements** |
| Use of logo and trademark |  |  |  |
| List of documents included in the audited MS |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Control Objective and Controls** | **Status** | **Audit Evidence** | **No. of NC** |
|  |
| **A.5 Organizational controls** |
| A 5.1 | **Policies for information security.** Control. Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur. |  |  |  |
| Control 5.1.and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. sector-specific guidance also applies for:- Public cloud PII protection implementation guidance- Other information for public cloud PII protection(27018) |
| A 5.2 | **Information security roles and responsibilities.** Control. Information security roles and responsibilities shall be defined and allocated according to the organization needs. |  |  |  |
| Control 5.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies:- Public cloud PII protection implementation guidance(27018) |
| A 5.3 | **Segregation of duties**Control. Conflicting duties and conflicting areas of responsibility shall be segregated. |  |  |  |
| A 5.4 | **Management responsibilities**Control. Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization. |  |  |  |
| A 5.5 | **Contact with authorities.**Control. The organization shall establish and maintain contact with relevant authorities. |  |  |  |
| A 5.6 | **Contact with special interest groups.**Control. The organization shall establish and maintain contact with special interest groups or other special security forums and professional associations. |  |  |  |
| A 5.7 | **Threat intelligence**Control. Information relating to information security threats shall be collected and analyzed to produce threat intelligence |  |  |  |
| A 5.8 | **Information security in project management** Control. Information security shall be integrated into project management. |  |  |  |
| A 5.9 | **Inventory of information and other associated assets**Control. An inventory of information and other associated assets, including owners, shall be developed and maintained. |  |  |  |
| A 5.10 | **Acceptable use of information and other associated assets**Control. Rules for the acceptable use and procedures for handling information and other assets shall be identified, documented and implemented. |  |  |  |
| A 5.11 | **Return of assets**Control. Personnel and other interested parties as appropriate shall return all the organization’s assets in their possession upon change or termination of their employment, contract or agreement. |  |  |  |
| A 5.12 | **Return of assets**Control. Personnel and other interested parties as appropriate shall return all the organization’s assets in their possession upon change or termination of their employment, contract or agreement. |  |  |  |
| A 5.13 | **Labelling of information** Control. An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization. |  |  |  |
| A 5.14 | **Information transfer**Control. Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties. |  |  |  |
| Control 5.14 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies:- Public cloud PII protection implementation guidance (27018) |
| A 5.15 | **Access control**Control. Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements. |  |  |  |
| A 5.16 | **Identity management**Control. The full life cycle of identities shall be managed. |  |  |  |
| A 5.17 | **Authentication information**Control. Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information. |  |  |  |
| A 5.18 | **Access rights**Control. Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization’s topic-specific policy on and rules for access control. |  |  |  |
| A 5.19 | **Information security in supplier relationships** Control. Processes and procedures shall be defined and implemented to manage the information security risk associated with the use of supplier’s products or services. |  |  |  |
| A 5.20 | **Addressing information security within supplier agreements**Control. Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship. |  |  |  |
| A 5.21 | **Managing information security in the information and communication technology (ICT) supply chain**Control. Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain. |  |  |  |
| A 5.22 | **Monitoring, review and change management of supplier services.**Control. The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery. |  |  |  |
| A 5.23 | **Information security for use of cloud services**Control. Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization’s information security requirements. |  |  |  |
| A 5.24 | **Information security incident management planning and preparation**Control. The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities. |  |  |  |
| A 5.25 | **Assessment and decision on information security events** Control. The organization shall assess information security events and decide if they are to be categorized as information security incidents. |  |  |  |
| A 5.26 | **Response to information security incidents**Control. Information security incidents shall be responded to in accordance with the documented procedures. |  |  |  |
| A 5.27 | **Response to information security incidents**Control. Information security incidents shall be responded to in accordance with the documented procedures. |  |  |  |
| A 5.28 | **Collection of evidence**Control. The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events. |  |  |  |
| A 5.29 | **Information security during disruption**Control. The organization shall plan how to maintain information security at an appropriate level during disruption. |  |  |  |
| A 5.30 | **ICT refines for business continuity.**Control. ICT Readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements. |  |  |  |
| A 6.31 | **Legal, statutory, regulatory and contractual requirements** Control. Legal, statutory, regulatory and contractual requirements related to information security and the organization’s approach to meet these requirements shall be identified, documented and kept up to date. |  |  |  |
| A 5.32 | **Intellectual property rights**Control. The organization shall implement appropriate procedures to protect intellectual property rights. |  |  |  |
| A 5.33 | **Protection of records**Control. Record shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release. |  |  |  |
| A 5.34 | **Privacy protection of personal identifiable information (PII)**Control. The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements. |  |  |  |
| A 5.35 | **Independent review of information security**Control. The organization’s approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur. |  |  |  |
| Control 5.35 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies.- Public cloud PII protection implementation guidance (27018) |
| A 5.36 | **Compliance with policies, rules and standards for information security**Control. Compliance with the organization’s information security policy, topic-specific policies, rules and standards shall be regularly reviewed. |  |  |  |
| A 5.37 | **Documented operating procedures.**Control. Operating procedures for information processing facilities shall be documented and made available to personnel who need them. |  |  |  |
| **A.6 People controls** |
| A 6.1 | **Screening**Control. Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks |  |  |  |
| A 6.2 | **Terms and conditions of employment**Control. The employment contractual agreements shall state the personnel’s and the organization’s responsibilities for information security. |  |  |  |
| A 6.3 | **Information security awareness education and training**Control. Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization’s information security policy, topic-specific policies and procedures, as relevant for their job function. |  |  |  |
| Control 6.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies:-Public cloud PII protection implementation guidance-Other information for public cloud PII protection(27018) |
| A 6.4 | **Disciplinary process** Control. A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation. |  |  |  |
| A 6.5 | **Responsibilities after termination or change of employment.**Control. Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties. |  |  |  |
| A 6.6 | **Confidentiality or non-disclosure agreements** Control. Confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties. |  |  |  |
| A 6.7  | **Remote working**Control. Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization’s premises. |  |  |  |
| A 6.8 | **Information security event reporting**Control. The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in timely manner. |  |  |  |
| **A.7 Physical controls** |
| A 7.1 | **Physical security perimeters**Control. Security perimeters shall be defined and used to protect areas that contain information and other associated assets. |  |  |  |
| A 7.2 | **Physical entry**Control. Secure areas shall be protected by appropriate entry controls and access points. |  |  |  |
| A 7.3 | **Securing offices, rooms and facilities**Control. Physical security for offices, rooms and facilities shall be designed and implemented |  |  |  |
| A 7.4 | **Physical security monitoring**Control. Premises shall be continuously monitored for unauthorized physical access. |  |  |  |
| A 7.5 | **Protecting against physical and environmental threats**Control. Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented. |  |  |  |
| A 7.6 | **Working in secure areas**Control. Security measures for working in secure areas shall be designed and implemented. |  |  |  |
| A 7.7 | **Clear desk and clear screen**Control. Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced. |  |  |  |
| A 7.8 | **Equipment siting and protection**Control. Equipment shall be sited securely and protected. |  |  |  |
| A 7.9 | **Security of assets off-premises**Control, Off-site assets shall be protected. |  |  |  |
| A 7.10 | **Storage media**Control. Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization’s classification scheme and handling requirements. |  |  |  |
| A 7.11 | **Supporting utilities**Control. Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities. |  |  |  |
| A 7.12 | **Cabling security**Control. Cables varying power, data or supporting information services shall be protected from interception, interference or damage. |  |  |  |
| A 7.13 | **Equipment maintenance**Control. Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information. |  |  |  |
| A 7.14 | **Secure disposal or re-use of equipment**Control. Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use. |  |  |  |
| Control 7.14 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies:- Public cloud PII protection implementation guidance (27018) |
| **A.8 Technological controls** |
| A 8.1 | **User end point devices**Control. Information stored on, processed by or accessible via user end point devices shall be protected. |  |  |  |
| A 8.2 | **Privileged access rights**Control. The allocation and use of privileged access rights shall be restricted and managed. |  |  |  |
| A 8.3 | **Information access restriction** Control. Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control. |  |  |  |
| A 8.4 | **Access to source code** Control. Read and write access to source code, development tools and software libraries shall be appropriately managed. |  |  |  |
| A 8.5 | **Secure authentication**Control. Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control. |  |  |  |
| A 8.6 | **Capacity management**Control. The use of resources shall be monitored and adjusted in line with current and expected capacity requirements. |  |  |  |
| A 8.7 | **Protection against malware**Control. Protection against malware shall be implemented and supported by appropriate user awareness. |  |  |  |
| A 8.8 | **Management of technical vulnerabilities**Control. Information about technical vulnerabilities of information systems in use shall be obtained, the organization’s exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken. |  |  |  |
| A 8.9 | **Configuration management**Control. Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed. |  |  |  |
| A 8.10 | **Information deletion**Control. Information stored in information systems, devices or in any other storage media shall be deleted when no longer required. |  |  |  |
| A 8.11 | **Data masking**Control. Data masking shall be used in accordance with the organization’s topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration. |  |  |  |
| A 8.12 | **Data leakage prevention** Control. Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information. |  |  |  |
| A 8.13 | **Information backup**Control. Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup. |  |  |  |
| Control 8.13 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies:- Public cloud PII protection implementation guidance (27018) |
| A 8.14 | **Redundancy of information processing facilities**Control. Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements. |  |  |  |
| A 8.15 | **Logging**Control. Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analyzed. |  |  |  |
| Control 8.15 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies:- Public cloud PII protection implementation guidance (27018) |
| A 8.16 | **Monitoring activities** Control. Networks, systems and applications shall be monitored for anomalous behavior and appropriate actions taken to evaluate potential information security incidents. |  |  |  |
| A 8.17 | **Clock synchronization**Control. The clock of information processing systems used by the organization shall be synchronized to approved time sources. |  |  |  |
| A 8.18 | **Use of privileged utility programs**Control. The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled. |  |  |  |
| A 8.19 | **Installation of software on operational systems**Control. Procedures and measures shall be implemented to securely manage software installation on operational systems. |  |  |  |
| A 8.20 | **Networks security** Control. Networks and network devices shall be secured, managed and controlled to protect information in systems and applications. |  |  |  |
| A 8.21 | **Security of network services** Control. Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored. |  |  |  |
| A 8.22 | **Segregation of networks**Control. Groups of information services, users and information systems shall be segregated in the organization’s networks. |  |  |  |
| A 8.23 | **Web filtering**Control. Access to external websites shall be managed to reduce exposure to malicious content. |  |  |  |
| A 8.24 | **Use of cryptography**Control. Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented. |  |  |  |
| Contol 8.24 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The Sector-specific guidance also applies:- Public cloud PII protection implementation guidance (27018) |
| A 8.25 | **Secure development life cycle**Control. Rules for the secure development of software and systems shall be established and applied. |  |  |  |
| A 8.26 | **Application security requirements**Control. Information security requirements shall be identified, specified and approved when developing or acquiring applications. |  |  |  |
| A 8.27 | **Secure system architecture and engineering principles** Control. Principles for engineering secure systems shall be established, documented, maintained, and applied to any information system development activities. |  |  |  |
| A 8.28 | **Secure coding**Control. Secure coding principles shall be applied to software development. |  |  |  |
| A 8.29 | **Security testing in development and acceptance** Control. Security testing processes shall be defined and implemented in development life cycle. |  |  |  |
| A 8.30 | **Outsourced development** Control. The organization shall direct, monitor and review the activities related to outsourced system development. |  |  |  |
| A 8.31 | **Separation of development, test and production environments** Control. Development, testing and production environments shall be separated and secured. |  |  |  |
| Contol 8.31 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. Sector-specific guidance also applies:- Public cloud PII protection implementation guidance (27018) |
| A 8.32 | **Change management**Control. Changes to information processing facilities and information systems shall be subject to change management procedures. |  |  |  |
| A 8.33 | **Test information**Control. Test information shall be appropriately selected, protected and managed. |  |  |  |
| A 8.34 | **Protection of information systems during audit testing**Control. Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management. |  |  |  |

**Annex A**(normative)
**Public cloud PII processor extended control set for PII protection**

|  |  |  |  |
| --- | --- | --- | --- |
| **Controls Requirements** | **Status** | **Audit Evidence** | **No. of NC** |

|  |  |
| --- | --- |
| **ISO 27018 - Public cloud PII processor extended control set for PII protection** |   |
| **A.1** | **General (No additional controls in the standard)** |  |
| **A 2** | **Consent and choice** |   |
| A.2.1 | **Obligation to co-operate regarding PII principals’ rights** Control. The public cloud PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals’ rights to access, correct and/or erase PII pertaining to them. |  |  |  |
| **A.3** | **Purpose legitimacy and specification** |   |
| A.3.1 | **Public cloud PII processor’s purpose** Control. PII to be processed under a contract should not be processed for any purpose independent of the instructions of the cloud service customer. |  |  |  |
| A.3.2 | **Public cloud PII processor's commercial use** Control. PII processed under a contract should not be used by the public cloud PII processor for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving the service. |  |  |  |
| **A.4** | **Collection limitation (No additional controls are relevant to this privacy principle).** |
| **A.5** | **Data Minimization** |  |
| A.5.1  | **Secure erasure of temporary files** Control. Temporary files and documents should be erased or destroyed within a specified, documented period. |  |  |  |
| **A.6**  | **Use, retention and disclosure limitation** |  |
| A.6.1 | **PII disclosure notification** Control. The contract between the public cloud PII processor and the cloud service customer should require the public cloud PII processor to notify the cloud service customer, in accordance with any procedure and time periods agreed in the contract, of any legally binding request for disclosure of PII by a law enforcement authority, unless such a disclosure is otherwise prohibited. |  |  |  |
| A.6.2 | **Recording of PII disclosures**Control. Disclosures of PII to third parties should be recorded, including what PII has been disclosed, to whom and at what time. |  |  |  |
| **A.7** | **Accuracy and quality (No additional controls are relevant to this privacy principle)** |
| **A.8** | **Openness, transparency and notice** |
| A.8.1 | **Disclosure of sub-contracted PII processing**Control. The use of sub-contractors by the public cloud PII processor to process PII should be disclosed to the relevant cloud service customers before their use. |  |  |  |
| **A.9** | **Individual participation and access (No additional controls are relevant to this privacy principle).** |
| **A.10** | **Accountability** |  |
| A.10.1 | **Notification of data breach involving PII** Control. The public cloud PII processor should promptly notify the relevant cloud service customer in the event of any unauthorized access to PII or unauthorized access to processing equipment or facilities resulting in loss, disclosure or alteration of PII. |  |  |  |
| A.10.2 | **Retention period for administrative security policies and guidelines** Control. Copies of security policies and operating procedures should be retained for a specified, documentedperiod on replacement (including updating). |  |  |  |
| A.10.3 | **PII return, transfer and disposal** Control. The public cloud PII processor should have a policy in respect of the return, transfer and/or disposal of PII and should make this policy available to the cloud service customer. |  |  |  |
| **A.11** | **Information security** |  |
| A.11.1 | **Confidentiality or non-disclosure agreements** Control. Individuals under the public cloud PII processor’s control with access to PII should be subject to a confidentiality obligation. |  |  |  |
| A.11.2 | **Restriction of the creation of hardcopy material** Control. The creation of hardcopy material displaying PII should be restricted. |  |  |  |
| A.11.3 | **Control and logging of data restoration** Control. There should be a procedure for, and a log of, data restoration efforts. |  |  |  |
| A.11.4 | **Protecting data on storage media leaving the premises** Control. PII on media leaving the organization's premises should be subject to an authorization procedure and should not be accessible to anyone other than authorized personnel (e.g. by encrypting the data concerned). |  |  |  |
| A.11.5 | **Use of unencrypted portable storage media and devices** Control. Portable physical media and portable devices that do not permit encryption should not be used except where it is unavoidable, and any use of such portable media and devices should be documented. |  |  |  |
| A.11.6 | **Encryption of PII transmitted over public data-transmission networks** Control. PII that is transmitted over public data-transmission networks should be encrypted prior totransmission. |  |  |  |
| A.11.7 | **Secure disposal of hardcopy materials** Control. Where hardcopy materials are destroyed, they should be destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc. |  |  |  |
| A.11.8 | **Unique use of user IDs** Control. If more than one individual has access to stored PII, then they should each have a distinct user ID for identification, authentication and authorization purposes. |  |  |  |
| A.11.9 | **Records of authorized users** Control. An up-to-date record of the users or profiles of users who have authorized access to the information system should be maintained. |  |  |  |
| A.11.10 | **User ID management** Control. De-activated or expired user IDs should not be granted to other individuals. |  |  |  |
| A.11.11 | **Contract measures** Control. Contracts between the cloud service customer and the public cloud PII processor should specify minimum technical and organizational measures to ensure that the contracted security arrangements are in place and that data are not processed for any purpose independent of the instructions of the controller. Such measures should not be subject to unilateral reduction by the public cloud PII processor. |  |  |  |
| A.11.12  | **Sub-contracted PII processing** Control. Contracts between the public cloud PII processor and any sub-contractors that process PII should specify minimum technical and organizational measures that meet the information security and PII protection obligations of the public cloud PII processor. Such measures should not be subject to unilateral reduction by the sub-contractor. |  |  |  |
| A.11.13  | **Access to data on pre-used data storage space** Control. The public cloud PII processor should ensure that whenever data storage space is assigned to a cloud service customer, any data previously residing on that storage space is not visible to that cloud service customer. |  |  |  |
| **A.12**  | **Privacy compliance** |  |
| A.12.1  | **Geographical location of PII** Control. The public cloud PII processor should specify and document the countries in which PII can possibly be stored. |  |  |  |
| A.12.2  | **Intended destination of PII** Control. PII transmitted using a data-transmission network should be subject to appropriate controls designed to ensure that data reaches its intended destination. |  |  |  |

# CSA STAR Requirements

The CSA STAR Certification leverages the requirements of the ISO/IEC 27001 together with the CSA Cloud Controls Matrix (CCM) v4.0. MSECB evaluated the maturity level across each control domain.

|  |  |  |
| --- | --- | --- |
| **Control Domain** | **Audit Evidence** | **Score** |
| Audit & Assurance (A&A) |  |  |
| Application & Interface Security (AIS) |  |  |
| Business Continuity Management and Operational Resilience (BCR) |  |  |
| Change Control and Configuration Management (CCC) |  |  |
| Cryptography, Encryption and Key Management (CEK) |  |  |
| Datacenter Security (DCS) |  |  |
| Data Security and Privacy Lifecycle Management (DSP) |  |  |
| Governance, Risk Management and Compliance (GRC) |  |  |
| Human Resources (HRS) |  |  |
| Identity and Access Management (IAM) |  |  |
| Interoperability and Portability (IPY) |  |  |
| Infrastructure and Virtualization Security (IVS) |  |  |
| Logging and Monitoring (LOG) |  |  |
| Security Incident Management, E-Discovery, and Cloud Forensics (SEF) |  |  |
| Supply Chain Management, Transparency, and Accountability (STA) |  |  |
| Threat and Vulnerability Management (TVM) |  |  |
| Universal Endpoint Management (UEM) |  |  |

| **Control Objective and Controls** | **Control Title** | **Score** |
| --- | --- | --- |
| **Audit & Assurance (A&A)** |
| A&A-01 | **Control:**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 | Audit and Assurance Policy and Procedures |  |
| A&A-02 | **Control:** Conduct independent audit and assurance assessments according to relevant standards at least annually. | Independent Assessments |  |
| A&A-03 | **Control:**Perform independent audit and assurance assessments according to risk-based plans and policies. | Risk Based Planning Assessment |  |
| A&A-04 | **Control:**Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit. | Requirements Compliance |  |
| A&A-05 | **Control:**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. | Audit Management Process |  |
| A&A-06 | **Control:**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. | Remediation |  |
| **Application & Interface Security (AIS)** |
| AIS-01 | **Control:**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. | Application and Interface Security Policy and Procedures  |  |
| AIS-02 | **Control:**Establish, document and maintain baseline requirements for securing different applications. | Application Security Baseline Requirements  |  |
| AIS-03 | **Control:**Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations. | Application Security Metrics |  |
| AIS-04 | **Control:**Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization. | Secure Application Design and Development |  |
| AIS-05 | **Control:**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. | Automated Application Security Testing |  |
| AIS-06 | **Control:**Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible. | Automated Secure Application Deployment |  |
| AIS-07 | **Control:**Define and implement a process to remediate application security vulnerabilities, automating remediation when possible. | Application Vulnerability Remediation |  |
| **Business Continuity Management & Operational Resilience (BCR)** |
| BCR-01 | **Control:**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. | Business Continuity Management Policy and Procedures |  |
| BCR-02 | **Control:**Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities. | Risk Assessment and Impact Analysis |  |
| BCR-03 | **Control:**Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite. | Business Continuity Strategy |  |
| BCR-04 | **Control:**Establish, document, approve, communicate, apply, evaluate and maintain a business continuity plan based on the results of the operational resilience strategies and capabilities. | Business Continuity Planning |  |
| BCR-05 | **Control:**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. | Documentation |  |
| BCR-06 | **Control:**Exercise and test business continuity and operational resilience plans at least annually or upon significant changes. | Business Continuity Exercises |  |
| BCR-07 | **Control:**Establish communication with stakeholders and participants in the course of business continuity and resilience procedures. | Communication |  |
| BCR-08 | **Control:**Periodically backup data stored in the cloud. Ensure the confidentiality, integrity and availability of the backup, and verify data restoration from backup for resiliency. | Backup |  |
| BCR-09 | **Control:**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. | Disaster Response Plan |  |
| BCR-10 | **Control:**Exercise the disaster response plan annually or upon significant changes, including if possible local emergency authorities. | Response Plan Exercise |  |
| BCR-11 | **Control:**Supplement business-critical equipment with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards. | Equipment Redundancy |  |
| **Change Control & Configuration Management (CCC)** |
| CCC-01 | **Control:**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. | Change Management Policy and Procedures |  |
| CCC-02 | **Control:**Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards. | Quality Testing |  |
| CCC-03 | **Control:**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). | Change Management Technology |  |
| CCC-04 | **Control:**Restrict the unauthorized addition, removal, update, and management of organization assets. | Unauthorized Change Protection |  |
| CCC-05 | **Control:**Include provisions limiting changes directly impacting CSCs owned environments/tenants to explicitly authorized requests within service level agreements between CSPs and CSCs. | Change Agreements |  |
| CCC-06 | **Control:**Establish change management baselines for all relevant authorized changes on organization assets. | Change Management Baseline |  |
| CCC-07 | **Control:**Implement detection measures with proactive notification in case of changes deviating from the established baseline. | Detection of Baseline Deviation |  |
| CCC-08 | **Control:**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. | Exception Management |  |
| CCC-09 | **Control:**Define and implement a process to proactively roll back changes to a previously known good state in case of errors or security concerns. | Change Restoration |  |
| **Cryptography, Encryption & Key Management (CEK)** |
| CEK-01 | **Control:**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. | Encryption and Key Management Policy and Procedures |  |
| CEK-02 | **Control:**Define and implement cryptographic, encryption and key management roles and responsibilities. | CEK Roles and Responsibilities |  |
| CEK-03 | **Control:**Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards. | Data Encryption |  |
| CEK-04 | **Control:**Use encryption algorithms that are appropriate for data protection, considering the classification of data, associated risks, and usability of the encryption technology.  | Encryption Algorithm |  |
| CEK-05 | **Control:**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. | Encryption Change Management |  |
| CEK-06 | **Control:**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. | Encryption Change Cost Benefit Analysis |  |
| CEK-07 | **Control:**Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback. | Encryption Risk Management |  |
| CEK-08 | **Control:**CSPs must provide the capability for CSCs to manage their own data encryption keys. | CSC Key Management Capability |  |
| CEK-09 | **Control:**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). | Encryption and Key Management Audit |  |
| CEK-10 | **Control:**Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used. | Key Generation |  |
| CEK-11 | **Control:**Manage cryptographic secret and private keys that are provisioned for a unique purpose. | Key Purpose |  |
| CEK-12 | **Control:**Rotate cryptographic keys in accordance with the calculated cryptoperiod, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements. | Key Rotation |  |
| CEK-13 | **Control:**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. | Key Revocation |  |
| CEK-14 | **Control:**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. | Key Destruction |  |
| CEK-15 | **Control:**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. | Key Activation |  |
| CEK-16 | **Control:**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. | Key Suspension |  |
| CEK-17 | **Control:**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. | Key Deactivation |  |
| CEK-18 | **Control:**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. | Key Archival |  |
| CEK-19 | **Control:**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. | Key Compromise |  |
| CEK-20 | **Control:**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. | Key Recovery |  |
| CEK-21 | **Control:**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. | Key Inventory Management |  |
| **Datacenter Security (DCS)** |
| DCS-01 | **Control:**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. | Off-Site Equipment Disposal Policy and Procedures |  |
| DCS-02 | **Control:**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. | Off-Site Transfer Authorization Policy and Procedures |  |
| DCS-03 | **Control:**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. | Secure Area Policy and Procedures |  |
| DCS-04 | **Control:**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. | Secure Media Transportation Policy and Procedures |  |
| DCS-05 | **Control:**Classify and document the physical, and logical assets (e.g., applications) based on the organizational business risk. | Assets Classification |  |
| DCS-06 | **Control:**Catalogue and track all relevant physical and logical assets located at all of the CSP’s sites within a secured system. | Assets Cataloguing and Tracking |  |
| DCS-07 | **Control:**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. | Controlled Access Points |  |
| DCS-08 | **Control:**Use equipment identification as a method for connection authentication. | Equipment Identification |  |
| DCS-09 | **Control:**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. | Secure Area Authorization |  |
| DCS-10 | **Control:**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. | Surveillance System |  |
| DCS-11 | **Control:**Train datacenter personnel to respond to unauthorized ingress or egress attempts. | Unauthorized Access Response Training |  |
| DCS-12 | **Control:**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. | Cabling Security |  |
| DCS-13 | **Control:**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. | Environmental Systems |  |
| DCS-14 | **Control:**Secure, monitor, maintain, and test utilities services for continual effectiveness at planned intervals. | Secure Utilities |  |
| DCS-15 | **Control:**Keep business-critical equipment away from locations subject to high probability for environmental risk events. | Equipment Location |  |
| **Data Security & Privacy Lifecycle Management (DSP)** |
| DSP-01 | **Control:**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. | Security and Privacy Policy and Procedures |  |
| DSP-02 | **Control:**Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means. | Secure Disposal |  |
| DSP-03 | **Control:**Create and maintain a data inventory, at least for any sensitive data and personal data. | Data Inventory |  |
| DSP-04 | **Control:**Classify data according to its type and sensitivity level. | Data Classification |  |
| DSP-05 | **Control:**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. | Data Flow Documentation |  |
| DSP-06 | **Control:**Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually. | Data Ownership and Stewardship |  |
| DSP-07 | **Control:**Develop systems, products, and business practices based upon a principle of security by design and industry best practices. | Data Protection by Design and Default |  |
| DSP-08 | **Control:**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. | Data Privacy by Design and Default |  |
| DSP-09 | **Control:**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. | Data Protection Impact Assessment |  |
| DSP-10 | **Control:**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. | Sensitive Data Transfer |  |
| DSP-11 | **Control:**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. | Personal Data Access, Reversal, Rectification and Deletion |  |
| DSP-12 | **Control:**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. | Limitation of Purpose in Personal Data Processing |  |
| DSP-13 | **Control:**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. | Personal Data Sub-processing |  |
| DSP-14 | **Control:**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. | Disclosure of Data Sub-processors |  |
| DSP-15 | **Control:**Obtain authorization from data owners, and manage associated risk before replicating or using production data in non-production environments. | Limitation of Production Data Use |  |
| DSP-16 | **Control:**Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations. | Data Retention and Deletion |  |
| DSP-17 | **Control:**Define and implement processes, procedures and technical measures to protect sensitive data throughout its lifecycle. | Sensitive Data Protection |  |
| DSP-18 | **Control:**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. | Disclosure Notification |  |
| DSP-19 | **Control:**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. | Data Location |  |
| **Governance, Risk Management and Compliance (GRC)** |
| GRC-01 | **Control:**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. | Governance Program Policy and Procedures |  |
| GRC-02 | **Control:**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. | Risk Management Program |  |
| GRC-03 | **Control:**Review all relevant organizational policies and associated procedures at least annually or when a substantial change occurs within the organization. | Organizational Policy Reviews |  |
| GRC-04 | **Control:**Establish and follow an approved exception process as mandated by the governance program whenever a deviation from an established policy occurs. | Policy Exception Process |  |
| GRC-05 | **Control:**Develop and implement an Information Security Program, which includes programs for all the relevant domains of the CCM. | Information Security Program |  |
| GRC-06 | **Control:**Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs. | Governance Responsibility Model |  |
| GRC-07 | **Control:**Identify and document all relevant standards, regulations, legal/contractual, and statutory requirements, which are applicable to your organization. | Information System Regulatory Mapping |  |
| GRC-08 | **Control:**Establish and maintain contact with cloud-related special interest groups and other relevant entities in line with business context. | Special Interest Groups |  |
| **Human Resources (HRS)** |
| HRS-01 | **Control:**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. | Background Screening Policy and Procedures |  |
| HRS-02 | **Control:**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 | Acceptable Use of Technology Policy and Procedures |  |
| HRS-03 | **Control:**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. | Clean Desk Policy and Procedures |  |
| HRS-04 | **Control:**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. | Remote and Home Working Policy and Procedures |  |
| HRS-05 | **Control:**Establish and document procedures for the return of organization-owned assets by terminated employees. | Asset returns |  |
| HRS-06 | **Control:**Establish, document, and communicate to all personnel the procedures outlining the roles and responsibilities concerning changes in employment. | Employment Termination |  |
| HRS-07 | **Control:**Employees sign the employee agreement prior to being granted access to organizational information systems, resources and assets. | Employment Agreement Process |  |
| HRS-08 | **Control:**The organization includes within the employment agreements provisions and/or terms for adherence to established information governance and security policies. | Employment Agreement Content |  |
| HRS-09 | **Control:**Document and communicate roles and responsibilities of employees, as they relate to information assets and security. | Personnel Roles and Responsibilities |  |
| HRS-10 | **Control:**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. | Non-Disclosure Agreements |  |
| HRS-11 | **Control:**Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organization and provide regular training updates. | Security Awareness Training |  |
| HRS-12 | **Control:**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. | Personal and Sensitive Data Awareness and Training |  |
| HRS-13 | **Control:**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. | Compliance User Responsibility |  |
| **Identity & Access Management (IAM)** |
| IAM-01 | **Control:**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. | Identity and Access Management Policy and Procedures |  |
| IAM-02 | **Control:**Establish, document, approve, communicate, implement, apply, evaluate and maintain strong password policies and procedures. Review and update the policies and procedures at least annually. | Strong Password Policy and Procedures |  |
| IAM-03 | **Control:**Manage, store, and review the information of system identities, and level of access. | Identity Inventory |  |
| IAM-04 | **Control:**Employ the separation of duties principle when implementing information system access. | Separation of Duties |  |
| IAM-05 | **Control:**Employ the least privilege principle when implementing information system access. | Least Privilege |  |
| IAM-06 | **Control:**Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets. | User Access Provisioning |  |
| IAM-07 | **Control:**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. | User Access Changes and Revocation |  |
| IAM-08 | **Control:**Review and validate user access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance. | User Access Review |  |
| IAM-09 | **Control:**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. | Segregation of Privileged Access Roles |  |
| IAM-10 | **Control:**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. | Management of Privileged Access Roles |  |
| IAM-11 | **Control:**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. | CSCs Approval for Agreed Privileged Access Roles |  |
| IAM-12 | **Control:**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. | Safeguard Logs Integrity |  |
| IAM-13 | **Control:**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. | Uniquely Identifiable Users |  |
| IAM-14 | **Control:**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. | Strong Authentication |  |
| IAM-15 | **Control:**Define, implement and evaluate processes, procedures and technical measures for the secure management of passwords. | Passwords Management |  |
| IAM-16 | **Control:**Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized. | Authorization Mechanisms |  |
| **Interoperability & Portability (IPY)** |
| IPY-01 | **Control:**Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for:a. Communications between application interfacesb. Information processing interoperabilityc. Application development portabilityd. Information/Data exchange, usage, portability, integrity, and persistenceReview and update the policies and procedures at least annually. | Interoperability and Portability Policy and Procedures |  |
| IPY-02 | **Control:**Provide application interface(s) to CSCs so that they programmatically retrieve their data to enable interoperability and portability. | Application Interface Availability |  |
| IPY-03 | **Control:**Implement cryptographically secure and standardized network protocols for the management, import and export of data. | Secure Interoperability and Portability Management |  |
| IPY-04 | **Control:**Agreements must include provisions specifying CSCs access to data upon contract termination and will include:a. Data formatb. Length of time the data will be storedc. Scope of the data retained and made available to the CSCsd. Data deletion policy | Data Portability Contractual Obligations |  |
| **Infrastructure & Virtualization Security (IVS)** |
| IVS-01 | **Control:**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 | Infrastructure and Virtualization Security Policy and Procedures |  |
| IVS-02 | **Control:**Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business. | Capacity and Resource Planning |  |
| IVS-03 | **Control:**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. | Network Security |  |
| IVS-04 | **Control:**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. | OS Hardening and Base Controls |  |
| IVS-05 | **Control:**Separate production and non-production environments. | Production and Non-Production Environments |  |
| IVS-06 | **Control:**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. | Segmentation and Segregation |  |
| IVS-07 | **Control:**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 | Migration to Cloud Environments |  |
| IVS-08 | **Control:**Identify and document high-risk environments. | Network Architecture Documentation |  |
| IVS-09 | **Control:**Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks. | Network Defense |  |
| **Logging and Monitoring (LOG)** |
| LOG-01 | **Control:**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. | Logging and Monitoring Policy and Procedures |  |
| LOG-02 | **Control:**Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs. | Audit Logs Protection |  |
| LOG-03 | **Control:**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. | Security Monitoring and Alerting |  |
| LOG-04 | **Control:**Restrict audit logs access to authorized personnel and maintain records that provide unique access accountability. | Audit Logs Access and Accountability |  |
| LOG-05 | **Control:**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. | Audit Logs Monitoring and Response |  |
| LOG-06 | **Control:**Use a reliable time source across all relevant information processing systems. | Clock Synchronization |  |
| LOG-07 | **Control:**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. | Logging Scope |  |
| LOG-08 | **Control:**Generate audit records containing relevant security information. | Log Records |  |
| LOG-09 | **Control:**The information system protects audit records from unauthorized access, modification, and deletion. | Log Protection |  |
| LOG-10 | **Control:**Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures, and controls. | Encryption Monitoring and Reporting |  |
| LOG-11 | **Control:**Log and monitor key lifecycle management events to enable auditing and reporting on usage of cryptographic keys. | Transaction/Activity Logging |  |
| LOG-12 | **Control:**Monitor and log physical access using an auditable access control system. | Access Control Logs |  |
| LOG-13 | **Control:**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. | Failures and Anomalies Reporting |  |
| **Security Incident Management, E-Discovery, & Cloud Forensics (SEF)** |
| SEF-01 | **Control:**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. | Security Incident Management Policy and Procedures |  |
| SEF-02 | **Control:**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. | Service Management Policy and Procedures |  |
| SEF-03 | **Control:**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. | Incident Response Plans |  |
| SEF-04 | **Control:**Test and update as necessary incident response plans at planned intervals or upon significant organizational or environmental changes for effectiveness. | Incident Response Testing |  |
| SEF-05 | **Control:**Establish and monitor information security incident metrics. | Incident Response Metrics |  |
| SEF-06 | **Control:**Define, implement and evaluate processes, procedures and technical measures supporting business processes to triage security-related events. | Event Triage Processes |  |
| SEF-07 | **Control:**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. | Security Breach Notification |  |
| SEF-08 | **Control:**Maintain points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities. | Points of Contact Maintenance |  |
| **Supply Chain Management, Transparency, and Accountability (STA)** |
| STA-01 | **Control:**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. | SSRM Policy and Procedures |  |
| STA-02 | **Control:**Apply, document, implement and manage the SSRM throughout the supply chain for the cloud service offering. | SSRM Supply Chain |  |
| STA-03 | **Control:**Provide SSRM Guidance to the CSC detailing information about the SSRM applicability throughout the supply chain. | SSRM Guidance |  |
| STA-04 | **Control:**Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM for the cloud service offering. | SSRM Control Ownership |  |
| STA-05 | **Control:**Review and validate SSRM documentation for all cloud services offerings the organization uses. | SSRM Documentation Review |  |
| STA-06 | **Control:**Implement, operate, and audit or assess the portions of the SSRM which the organization is responsible for. | SSRM Control Implementation |  |
| STA-07 | **Control:** Develop and maintain an inventory of all supply chain relationships. | Supply Chain Inventory |  |
| STA-08 | **Control:**CSPs periodically review risk factors associated with all organizations within their supply chain. | Supply Chain Risk Management |  |
| STA-09 | **Control:**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 | Primary Service and Contractual Agreement |  |
| STA-10 | **Control:**Review supply chain agreements between CSPs and CSCs at least annually. | Supply Chain Agreement Review |  |
| STA-11 | **Control:** 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. | Internal Compliance Testing |  |
| STA-12 | **Control:**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. | Supply Chain Service Agreement Compliance |  |
| STA-13 | **Control:**Periodically review the organization’s supply chain partners’ IT governance policies and procedures. | Supply Chain Governance Review |  |
| STA-14 | **Control:**Define and implement a process for conducting security assessments periodically for all organizations within the supply chain. | Supply Chain Data Security Assessment |  |
| **Threat & Vulnerability Management (TVM)** |
| TVM-01 | **Control:**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. | Threat and Vulnerability Management Policy and Procedures |  |
| TVM-02 | **Control:**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. | Malware Protection Policy and Procedures |  |
| TVM-03 | **Control:**Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk. | Vulnerability Remediation Schedule |  |
| TVM-04 | **Control:**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. | Detection Updates |  |
| TVM-05 | **Control:**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. | External Library Vulnerabilities |  |
| TVM-06 | **Control:**Define, implement and evaluate processes, procedures and technical measures for the periodic performance of penetration testing by independent third parties. | Penetration Testing |  |
| TVM-07 | **Control:**Define, implement and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organizationally managed assets at least monthly. | Vulnerability Identification |  |
| TVM-08 | **Control:**Use a risk-based model for effective prioritization of vulnerability remediation using an industry recognized framework. | Vulnerability Prioritization |  |
| TVM-09 | **Control:**Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification. | Vulnerability Management Reporting |  |
| TVM-10 | **Control:**Establish, monitor and report metrics for vulnerability identification and remediation at defined intervals. | Vulnerability Management Metrics |  |
| **Universal Endpoint Management (UEM)** |
| UEM-01 | **Control:**Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. Review and update the policies and procedures at least annually. | Endpoint Devices Policy and Procedures |  |
| UEM-02 | **Control:**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. | Application and Service Approval |  |
| UEM-03 | **Control:**Define and implement a process for the validation of the endpoint device compatibility with operating systems and applications. | Compatibility |  |
| UEM-04 | **Control:**Maintain an inventory of all endpoints used to store and access company data. | Endpoint Inventory |  |
| UEM-05 | **Control:**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. | Endpoint Management |  |
| UEM-06 | **Control:**Configure all relevant interactive-use endpoints to require an automatic lock screen. | Automatic Lock Screen |  |
| UEM-07 | **Control:**Manage changes to endpoint operating systems, patch levels, and/or applications through the company’s change management processes. | Operating Systems |  |
| UEM-08 | **Control:**Protect information from unauthorized disclosure on managed endpoint devices with storage encryption. | Storage Encryption |  |
| UEM-09 | **Control:**Configure managed endpoints with anti-malware detection and prevention technology and services. | Anti-Malware Detection and Prevention |  |
| UEM-10 | **Control:**Configure managed endpoints with properly configured software firewalls. | Software Firewall |  |
| UEM-11 | **Control:**Configure managed endpoints with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment. | Data Loss Prevention |  |
| UEM-12 | **Control:**Enable remote geo-location capabilities for all managed mobile endpoints. | Remote Locate |  |
| UEM-13 | **Control:**Define, implement and evaluate processes, procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices. | Remote Wipe |  |
| UEM-14 | **Control:**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. | Third-Party Endpoint Security Posture |  |
| **TOTAL SCORE** |  |

# Audit findings

The audit findings were communicated to the senior management of the organization during the closing meeting. The final conclusion of the audit results and recommendation by the audit team was also communicated to the management during the meeting.

## Audit finding definition

The evaluation of the audit findings is based on the following definitions:

**Major Nonconformities (MaNC)**

The **absence** or **total failure** of a **system** to meet a requirement. It may be either:

* A number of minor nonconformities against one requirement can represent a total failure of the system and thus be considered a major nonconformance; or
* Any nonconformance that would result in the probable shipment of a nonconforming product. A condition that may result in the failure or materially reduce the usability of the products or services for their intended purpose; or
* A nonconformance that judgment and experience indicate is likely either to result in the failure of the ISMS system or to materially reduce its ability to assure controlled processes and products.

**Minor Nonconformities (MiNC)**

A **nonconformance** that judgment and experience **indicate is not likely to result in the failure** of the ISMS system or **reduce its ability** to assure controlled processes or products. It may be either:

* A failure in some part of the supplier's documented ISMS system relative to a requirement; or
* A single observed lapse in following one item of a company’s ISMS system.

**Observations (OBS)**

Any issues which are **likely to become a NC,** if not treated until the next audit are marked as observations (OBS). No response is required.

**Opportunities for Improvement (OFI)**

If **certain aspects** which generally comply with the requirements of the standard should be improved, then they are marked as opportunities for improvement (OFI). These OFIs help to **improve the management system** as a whole or named processes. No response is required.

## Major nonconformities (see also Annex A)

Please explain if there are major non-conformities found during the audit.

## Minor nonconformities (see also Annex A)

Please explain if there are minor non-conformities found during the audit.

## Observations

Please list any noted observations or issues that can possibly turn to non-conformities.

## Opportunities for improvement

*Please list any noted opportunities for improvement without any specific recommendations for correction.*

## Agreed follow-up activities

Nonconformities detailed here need to be addressed through the organization’s corrective action process, in accordance with the relevant corrective action requirements of the audit standard, including actions to analyze the cause of the nonconformity, prevent recurrence, and complete the maintained records.

Corrective actions to address the identified major nonconformities, shall be carried out immediately and MSECB shall be notified of the actions taken within 30 days. To confirm the actions taken, evaluate their effectiveness, and determine whether certification can be granted or continued, a MSECB auditor will perform a follow up visit within 90 days.

Corrective actions to address the identified minor nonconformities shall be documented on an action plan and be sent for review by the client to the auditor within 30 days. If the actions are deemed to be satisfactory, they will be followed up during the next scheduled visit.

Nonconformities shall be addressed through the client’s corrective action process, including:

* Actions taken to determine the extent of and contain the specific nonconformance.
* Root Cause (results of an investigation to determine the most basic cause(s) of the nonconformance).
* Actions taken to correct the nonconformance and, in response to the root cause, to eliminate recurrence of the nonconformance.
* Corrective action response shall be submitted to the MSECB Lead Auditor.
* Client must maintain corrective action records, including objective evidence, for at least three (3) years.

## Uncertainty / obstacles that could affect the reliability of audit conclusions

Please specify.

## Unresolved diverging opinions between the audit team & auditee

Please specify.

# Audit conclusions and audit recommendation

## System management conformance and capability

*[Please describe if the management system has proven conformity with the requirements of the audit standard and provided adequate structure to support implementation and maintenance of the management system*

*i.e:*

* *demonstration of effective implementation and maintenance of MS*
* *demonstration of established and tracking of proper key performance objectives and targets*
* *implementation of internal audit programme etc. ]*

## Audit conclusions

|  |  |
| --- | --- |
| Has there been any serious deviation from the audit plan? (If yes, please specify) | Yes [ ]  No [ ]  |
| Are there any significant issues impacting the audit program? (If yes, please specify) | Yes [ ]  No [ ]  |
| Are there any significant changes affecting the management system since last audit took place? (If yes, please list the significant changes) | Yes [ ]  No [ ]  N/A [ ]  |
| Are there any unresolved issues affecting the management system since last audit took place? (If yes, please list the unresolved issues) | Yes [ ]  No [ ]  N/A [ ]  |
| The verification of the effectiveness of the corrective action taken regarding previously identified nonconformities has been performed and is satisfactory (please list any comments if needed) | Yes [ ]  No [ ]  N/A [ ]  |
| The management system is designed to achieve the organization’s policy objectives | Yes [ ]  No [ ]  |
| The management system is designed to meet statutory, regulatory and contractual requirements | Yes [ ]  No [ ]  |
| The internal audit and management review processes are in place and adequate | Yes [ ]  No [ ]  |
| The audit was successful in meeting the stated objectives | Yes [ ]  No [ ]  |
| STAR Certification requirements were applied  | Yes [ ]  No [ ]  |

## Recommendation

*Lead Auditor Recommendation:*

*(Please recommend whether the management system of the organization being audited, should be certified or not certified with ISO 27001 MS Certificate and CSA STAR Certification)*

# Annex A: Nonconformity report

## Nonconformity Report

Note: If more than one nonconformity identified, please add additional nonconformity reports

|  |
| --- |
| **NON CONFORMITY REPORT** |
| **TO BE COMPLETED BY AUDITOR** | **DATE** | **ORGANIZATION** | **NC ID** |
|  |  |  |
| **STANDARD:** ISO/IEC 27001:2022 |
| **NON CONFORMITY OBSERVED IN PROCESS/ AREA** |  |
| **REQUIREMENT OF THE STANDARD:**  | **CLAUSE:**  |
| **NON CONFORMITY – DESCRIPTION OF OBJECTIVE EVIDENCE** |
|  |
| **GRADE (Major/ Minor)** | **LEAD AUDITOR** | **AUDITOR** | **BUSINESS PROCESS REP.** |
|  |  |  |  |
| **TO BE COMPLETED BEFORE** |
|  |
| **TO BE COMPLETED BY THE ORGANIZATION** | **ROOT CAUSE ANALYSIS (What failed in the system to allow this NC to occur ?)** |
|  |
| **CORRECTION & CORRECTIVE ACTION (What is done to solve this problem and to prevent recurrence)** |
| CORRECTION: CORRECTIVE ACTION:  |
| **VERIFICATION OF CORRECTIVE ACTIONS** | **DATE OF COMPLETION** |  |
| **ORGANIZATION REPRESENTATIVE** |  |
| **TO BE COMPLETED BY AUDITOR**  | **VERIFICATION OF CORRECTIONS / CORRECTIVE ACTIONS** | **DATE** | **STATUS** | **LEAD AUDITOR** |
|  |  |  |
| **AUDITOR COMMENTS (including evidences verified to accept the corrections/ correcive actions)** |  |

# Annex B: Certification Information

|  |
| --- |
| **GENERAL INFORMATION** |
| **Number of Certificates** (for hardcopy) |  |
| **Languages** | [ ]  English | [ ]  French |
| **Name of the company** (to be put in the certificate) |  |
| **Address** (to be put in the certificate) |  |
| **Certification Scope Statement** (to be put in the certificate)**Important Note\*** Scope Statement should be concise and shall indicate **only** the processes and procedures within the management system that were assessed during the audit. Company’s name or address should not be written in this statement as they are mentioned in dedicated spaces. For ISO/IEC 27001, it is obligatory to put SoA version as well.  |  |
| **Excluded clauses in the audited Management System** (to be put in the certificate) |  |
| **DELIVERY ADDRESS**  |
| Title (Mr., Ms.) |  |
| First name |  |
| Last name |  |
| Address |  |
| City |  |
| Country |  |
| Province/State/Region |  |
| ZIP/Postal code |  |
| Email address |  |

# Annex C: Surveillance Plan

|  |
| --- |
| **Surveillance PlanISO/IEC 27001:2022 and ISO/IEC 27018:2019** |
| **1**: Initial Audit**2:** Surveillance 1 Audit**3**: Surveillance 2 Audit**4**: Recertification Audit | **Plan** |
| **1****(202X)** | **2** **(202X)** | **3****(202X)** | **4****(202X)** |
| **ISO/IEC 27001:2022 Clauses** |
| **4 Context of the organization** |
| **4.1** | Understanding the organization and its context |  |  |  |  |
| **4.2** | Understanding the needs and expectations of interested parties |  |  |  |  |
| **4.3** | Determining the scope of the information security management system |  |  |  |  |
| **4.4** | Information security management system |  |  |  |  |
| **5 Leadership** |
| **5.1** | Leadership and commitment |  |  |  |  |
| **5.2** | Policy |  |  |  |  |
| **5.3** | Organizational roles, responsibilities and authorities |  |  |  |  |
| **6 Planning** |
| **6.1** | Actions to address risks and opportunities |  |  |  |  |
| **6.2** | Information security objectives and planning to achieve them |  |  |  |  |
| **6.3** | Planning of changes |  |  |  |  |
| **7 Support** |
| **7.1** | Resources |  |  |  |  |
| **7.2** | Competence |  |  |  |  |
| **7.3** | Awareness |  |  |  |  |
| **7.4** | Communication |  |  |  |  |
| **7.5** | Documented information |  |  |  |  |
| **8 Operation** |
| **8.1** | Operational planning and control |  |  |  |  |
| **8.2** | Information security risk assessment |  |  |  |  |
| **8.3** | Information security risk treatment |  |  |  |  |
| **9 Performance Evaluation** |
| **9.1** | Monitoring, measurement, analysis and evaluation |  |  |  |  |
| **9.2** | Internal audit |  |  |  |  |
| **9.3** | Management review |  |  |  |  |
| **10 Improvement** |
| **10.1** | Continual improvement |  |  |  |  |
| **10.2** | Nonconformity and corrective action |  |  |  |  |
| **Control objectives and controls** |
| **A.5** | Organizational controls |  |  |  |  |
| **A.6** | People controls |  |  |  |  |
| **A.7** | Physical controls |  |  |  |  |
| **A.8** | Technological Controls  |  |  |  |  |
| **11. Additional requirements** |
|  | Use of Logo |  |  |  |  |
|  | List of documents included in the audited MS |  |  |  |  |
| **Notes and comments:** |  |

# 8. Annex D: Surveillance Plan

|  |
| --- |
| **Surveillance PlanCSA STAR Certification** |
| **1**: Initial Audit**2:** Surveillance 1 Audit**3**: Surveillance 2 Audit**4**: Recertification Audit | **Plan** |
| **1****(202X)** | **2** **(202X)** | **3****(202X)** | **4****(202X)** |
| **CSA STAR Requirements Certification**  |
| **A&A** | Audit and Assurance |  |  |  |  |
| **AIS** | Application & Interface Security |  |  |  |  |
| **BCR** | Business Continuity Management & Operational Resilience |  |  |  |  |
| **CCC** | Change Control & Configuration Management |  |  |  |  |
| **CEK** | Cryptography, Encryption & Key Management |  |  |  |  |
| **DCS** | Datacenter Security |  |  |  |  |
| **DSP** | Data Security & Privacy Lifecycle Management |  |  |  |  |
| **GRC** | Governance, Risk Management and Compliance |  |  |  |  |
| **HRS** | Human Resources  |  |  |  |  |
| **IAM** | Identity & Access Management |  |  |  |  |
| **IPY** | Interoperability & Portability |  |  |  |  |
| **IVS** | Infrastructure & Virtualization Security |  |  |  |  |
| **LOG** | Logging and Monitoring |  |  |  |  |
| **SEF** | Security Incident Management, E-Discovery, & Cloud Forensics |  |  |  |  |
| **STA** | Supply Chain Management, Transparency, and Accountability |  |  |  |  |
| **TVM** | Threat & Vulnerability Management |  |  |  |  |
| **UEM** | Universal Endpoint Management |  |  |  |  |

*For completed visits, mark “X” in the box for each clause/process covered.*

*For planned visits, mark “O” in the box for each clause/process to be covered.*