الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Guide to Cloud Cybersecurity Controls – Cloud Service Providers Implementation

(GCCC-CSP – 1: 2023)

TLP: white

Document Classification: Public

Disclaimer: This Guide has been developed by the National Cybersecurity Authority to assist organizations in implementing Cloud Cybersecurity Controls (CCC–1:2022) for Cloud Service Providers (CSPs). The National Cybersecurity Authority disclaims responsibility for relying solely on this document and emphasizes the importance of considering the organization's specific requirements and environment. The National Cybersecurity Authority clarifies that this guide serves as an illustrative model and does not necessarily mean that this is the only method of implementing Cloud Cybersecurity Controls, as long as alternative methods align with the National Cybersecurity Authority. This document contains some illustrative deliverables related to the implementation of Cloud Cybersecurity Controls. The assessor or auditor has the right to request other evidences as deemed necessary to ensure that proper implementation of all Cloud Cybersecurity Controls.

In the Name of Allah,

The Most Gracious,

The Most Merciful

TLP: White

Document Classification: Public

Traffic Light Protocol (TLP):

This marking protocol is widely used around the world. It has four colors (traffic lights):

Red – Personal, Confidential and for Intended Recipient Only

The recipient has no rights to share information classified in red with any person outside the defined range of recipients, either inside or outside the organization, beyond the scope specified for receipt.

Amber – Restricted Sharing

The recipient may share information classified in amber only with intended recipients inside the organization and with recipients who are required to take action related to the shared information.

Green – Sharing within The Same Community

The recipient may share information classified in green with other recipients inside the organization or outside it, within the same sector or related to the organization. However, it is not allowed to exchange or publish this information on public channels.

White – No Restriction

Table of Contents

Introduction 6
Objectives 6
Scope of Work 6
Cloud Cybersecurity Controls Domains and Structure 7
Structure of the Guideline 8
CCC Implementation Guidance for Cloud Service Providers 9
CCC Implementation Guidance for Cloud Service Providers 10

List of Figures

Figure 1: CCC Domains and Subdomains **7**
Figure 2: CCC Implementation Guideline Structure **8**

TLP: White

Document Classification: Public

Introduction

The National Cybersecurity Authority (referred to in this document as "NCA") developed this guideline for implementing the cybersecurity controls stated in the Cloud Cybersecurity Controls (CCC–1:2020) for Cloud Service Providers (CSPs), to enable national organizations to implement the requirements to comply with the Cloud Cybersecurity Controls (CCC–1:2020). This guideline was developed based on the information and experiences that NCA has collected and analyzed since the publication of the controls and was aligned with cybersecurity best practices to facilitate the implementation of the controls across national entities.

Objectives

The main objective of this guide is to enable national entities to fulfill compliance requirements for the Cloud Cybersecurity Controls (CCC–1:2020) implementation, strengthen their cybersecurity, and reduce cybersecurity risks that may arise from internal and external cybersecurity threats.

Scope of Work

This guideline's scope of work applies to the CSPs as stated in the Cloud Cybersecurity Controls (CCC–1:2020), which is:

- The cybersecurity controls shall apply to the CSPs and CSTs. These controls represent the minimum cybersecurity requirements for cloud computing.
- CSPs within the scope of CCC are any CSP which provides cloud computing services to the CSTs within the scope of work.
- CSTs within the scope of CCC are any government organization in the Kingdom of Saudi Arabia inside or outside the Kingdom (including ministries, authorities, establishments and others) and its companies and entities, as well as private sector organizations owning, operating or hosting Critical National Infrastructures (CNIs) that currently use or planning to use any cloud service.
- The NCA strongly encourages all other organizations in the Kingdom to leverage these controls to implement best practices to improve and enhance their cloud cybersecurity.

Cloud Cybersecurity Controls Domains and Structure

Figure 1 below shows the CCC domains and subdomains.

1	حوكمة الأمن السيبراني Cybersecurity Governance	1-1	أدوار ومسؤوليات الأمن السيبراني Cybersecurity Roles and Responsibilities	1-2	إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management
		1-3	الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني Compliance with Cybersecurity Standards, Laws and Regulations	1-4	الأمن السيبراني المتعلق بالموارد البشرية Cybersecurity in Human Resources
		1-5	الأمن السيبراني ضمن إدارة التغيير Cybersecurity in Change Management		
2	تعزيز الأمن السيبراني Cybersecurity Defense	2-1	إدارة الأصول Asset Management	2-2	إدارة هويات الدخول والصلاحيات Identity and Access Management
		2-3	حماية الأنظمة وأجهزة معالجة المعلومات Information System and Processing Facilities Protection	2-4	إدارة أمن الشبكات Networks Security Management
		2-5	أمن الأجهزة المحمولة Mobile Devices Security	2-6	حماية البيانات والمعلومات Data and Information Protection
		2-7	التشفير Cryptography	2-8	إدارة النسخ الاحتياطية Backup and Recovery Management
		2-9	إدارة الثغرات Vulnerability Management	2-10	اختبار الاختراق Penetration Testing
		2-11	إدارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management	2-12	إدارة حوادث وتهديدات الأمن السيبراني Cybersecurity Incident and Threat management
		2-13	الأمن المادي Physical Security	2-14	حماية تطبيقات الويب Web Application Security
		2-15	إدارة المفاتيح Key Management	2-16	أمن تطوير الأنظمة System Development Security
		2-17	أمن وسائط التخزين Storage Media Security		
3	صمود الأمن السيبراني Cybersecurity Resilience	3-1	جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال Cybersecurity Resilience Aspects of Business Continuity Management (BCM)		
4	الأمن السيبراني المتعلق بالأطراف الخارجية Third-Party Cybersecurity	4-1	الأمن السيبراني المتعلق بسلسلة الإمداد والأطراف الخارجية Supply Chain and Third-Party Cybersecurity		

Figure 1: CCC Domains and Subdomains

TLP: White

Document Classification: Public

Structure of the Guideline

Figure 2 below shows the structure of the Implementation Guideline for Cloud Cybersecurity Controls.

<table>
<tr><td colspan="2">
</td><td>Name of Main Domain</td></tr>
<tr><td colspan="2">Reference number of the Main Domain</td><td></td></tr>
<tr><td colspan="2">Reference No. of the Subdomain</td><td>Name of Subdomain</td></tr>
<tr><td colspan="3">Objective</td></tr>
<tr><td colspan="3">Controls</td></tr>
<tr><td rowspan="3">Control Reference Number</td><td colspan="2">Control Clauses</td></tr>
<tr><td colspan="2">Guidelines:</td></tr>
<tr><td colspan="2">Expected deliverables:</td></tr>
</table>

Figure 2: CCC Implementation Guideline Structure

CCC Implementation Guidance for Cloud Service Providers

General guidelines
• Identify the cloud services that are provided by the organization, and determine the degree of classification of the data that is processed or stored by the services in accordance with the cloud cybersecurity controls document (CCC-1:2020), while also considering related laws and regulations. • Inventorying assets and cloud technology systems within the organization, reviewing them, and updating them annually. • Inventorying user accounts with sensitive privileges, who have the ability to manage cloud services within the organization, and reviewing them periodically • Identify and document the cloud cybersecurity requirements, along with associated roles and responsibilities, and having them authorized by the authorizing official, reviewing them periodically. • Review the ECC guidelines and implement CCC related to CSPs. • Develop a plan to implement CCC for CPSs, and monitoring it continuously.

TLP: White

Document Classification: Public

CCC Implementation Guidance for Cloud Service Providers

The below outlines implementation guideline for the CCC

1 (Cybersecurity Governance)

1-1	Cybersecurity Roles and Responsibilities	
Objective	To ensure that roles and responsibilities are defined for all parties participating in implementing the cloud cybersecurity controls, including the roles and responsibilities of the head of the CSP and CST or his/her delegate, referred to in this controls as "Authorizing Official".	
Controls		
1-1-P-1	In addition to the ECC control 1-4-1, the Authorizing Official shall also identify, document and approve the following:	
	1-1-P-1-1	Cybersecurity Roles and RACI assignment for all stakeholders of the cloud services including Authorizing Official's roles and responsibilities.
		Related cybersecurity tools: • Template for Cybersecurity Roles and Responsibilities • Template for Cybersecurity Organizational Structure **Guidelines:** • Identify cloud services (e.g. based on the Cloud Service portfolio) offered and related cybersecurity stakeholders both internal and external (e.g. Cloud Cybersecurity Architecture, Engineering, Operations teams, 3rd party Cloud Security Managed Services, Authorizing Office, CSTs, etc.).
		Expected deliverables: • Cloud Cybersecurity Roles and Responsibilities and RACI matrix documented and approved within the related Service Level Agreements (SLAs) between CSP and CSTs.
1-2	Cybersecurity Risk Management	
Objective	To ensure managing cybersecurity risks in a methodological approach in order to protect the CSP's and CST's information and technology assets as per organizational policies and procedures, and related laws and regulations.	
Controls		

1-2-P-1	Cybersecurity risk management methodology mentioned in the ECC Subdomain 1-5, shall also include for the CSP, as a minimum:	
	1-2-P-1-1	Defining acceptable risk levels for the cloud services and clarifying them to the CST if the risk was related to him/her.
		Related cybersecurity tools: • Template for Risk Management Policies **Guidelines:** In addition to the ECC control 1-5 implementation guidelines: • Identify offered cloud services and analyse their business impact in a defined process (e.g. Business Impact Analysis) to understand and assess risks (for example, service disruption, data leak, unauthorized access, etc.) and the damage one cloud issue may cause. • Define risk levels for cloud services (e.g.: critical, high, medium, low), and the acceptable risk levels. • Communicate acceptable risk levels with CSTs (e.g.: sharing a Risk Assessment/Threat Analysis of cloud services provided to the CST).
		Expected deliverables: • Defined acceptable risk levels of cloud services documented and communicated with the concerned and relevant stakeholders, including the CSTs.
	1-2-P-1-2	Considering data and information classification in cybersecurity risk management methodology.
		Related cybersecurity tools: • Template for Cybersecurity Risk Management Policies • Template for Cybersecurity Risk Management Procedure • Template for Risk Register **Guidelines:** • Identify types of data and information processed/stored in the cloud services and classify it into agreed upon categories with the CST (e.g. public, restricted, secret, top secret) based on value and criticality to the CST, and include them in the cybersecurity risk management methodology when dealing with the cybersecurity risks related to cloud services.
		Expected deliverables: • Cybersecurity Risk Management Methodology includes clear procedure to deal with data based on its classification levels.
	1-2-P-1-3	Developing cybersecurity risk register for cloud services and monitoring it periodically according to the risks.

TLP: White

Document Classification: Public

		Related cybersecurity tools: • Template for Cybersecurity Risk Management Policies • Template for Cybersecurity Risk Management Procedures • Template for Risk Register **Guidelines:** • Identify cybersecurity risks related to cloud services and CSTs and assess them based on the approved methodology. • Maintain the Cloud Services Risk Register that includes all sufficient information to analyse risk, take informed decision about how to respond to risks and track associated actions. • Review the Risk Register periodically, based on an approved plan, considering the identified risks and their criticality.
		Expected deliverables: • Cybersecurity Cloud Services Risk Register. • Cybersecurity Cloud Services Risk Register review plan. • Cybersecurity Cloud Services Risk Register review reports.
1-3	**Compliance with Cybersecurity Standards, Laws and Regulations**	
Objective	To ensure that the CSPs' and CSTs' cybersecurity program is in compliance with related laws and regulations.	
Controls		
1-3-P-1	In addition to the ECC control 1-7-1, the CSP legislative and regulatory compliance should include as a minimum with the following requirements:	
	1-3-P-1-1	Continuous compliance with all laws, regulations, instructions, decisions, regulatory frameworks and controls, and mandates regarding cybersecurity in KSA.
		Related cybersecurity tools: • Template for Compliance with Laws and Regulations Policy • Template for Reviewing and Auditing Policy • Template for Audit Plan Log **Guidelines:** • Identify Periodically (e.g. annually or when a change occurs) all laws, regulations, instructions, decisions, regulatory frameworks and controls, and mandates regarding cybersecurity that are being applied within the KSA. • Monitor CSP's compliance with these requirements in a continuous manner (e.g. utilizing tools for daily or weekly verification).
		Expected deliverables:

		• List of all laws, regulations, instructions, decisions, regulatory frameworks and controls, and mandates regarding cybersecurity that are being applied within the KSA that are applicable to the CSP. • Reports clarifying the status of compliance with these requirements. • Reports clarifying periodic plans for monitoring compliance.
1-4	**Cybersecurity in Human Resources**	
Objective	To ensure that cybersecurity risks and requirements related to personnel (employees and contractors) are managed efficiently prior to employment, during employment and after termination/separation as per organizational policies and procedures, and related laws and regulations.	
Controls		
1-4-P-1	In addition to sub controls in the ECC controls 1-9-3 and 1-9-4, the following requirements should be covered prior and during the professional relationship of personnel with the CSP as a minimum:	
	1-4-P-1-1	Positions of cybersecurity functions in CSP's data centers within the KSA must be filled with qualified and suitable Saudi nationals.
		Related cybersecurity tools: • Template for Cybersecurity for Human Resources **Guidelines:** • Identify cybersecurity roles, positions and functions related to the data centres based in the KSA (e.g.: Cloud Security Engineer, Cybersecurity Monitoring Team, etc.). • Employ for these positions Saudi nationals with professional cybersecurity experience and certification relevant to the position and seniority. Consider cybersecurity industry recognized professional certifications (e.g.: CISSP, CISA, CCSK, CCSP). • Include data center cybersecurity staff in the cybersecurity training program to improve their skills and qualifications.
		Expected deliverables: • List of cybersecurity positions related to the data centers within the KSA and the requirements for each position. • List of employees filling these positions and their qualifications. • Cybersecurity training program and the provided training certificates based on it.
	1-4-P-1-2	Screening or vetting candidates of personnel working inside KSA who have access to Cloud Technology Stack, periodically.

TLP: White

Document Classification: Public

		Related cybersecurity tools: • Template for Cybersecurity for Human Resources **Guidelines:** • Review KSA-based job titles and descriptions for duties relevant to access to Cloud Technology Stack and make sure candidates for these jobs are under screening/vetting (e.g.: Cloud Engineer, Cloud Service Administrator, Key Vault Security Engineer, etc.) before employment and periodically.
		Expected deliverables: • Screening/Vetting process defined and implemented for candidates with access to Cloud Technology Stack including a plan for a periodic screening/vetting. • Reports of screening/vetting for these candidates. Information privacy and sensitivity must be in consideration when dealing with these reports.
	1-4-P-1-3	Cybersecurity policies as a prerequisite to access to Cloud Technology Stack, signed and appropriately approved.
		Related cybersecurity tools: • Template for Cybersecurity for Human Resources • Template for Cybersecurity Compliance **Guidelines:** • Make joiners/workers familiar with organization's cybersecurity policies before they are granted the access to Cloud Technology Stack by signing a formal form,
		Expected deliverables: • Cybersecurity policies acknowledgement and compliance form is signed by all personnel working on Cloud Technology Stack before having access.
1-4-P-2	In addition to sub controls in the ECC control 1-9-5, the following requirements should be in place, as a minimum, for the termination/completion of a human resource's professional relationship with the CSP:	
	1-4-P-2-1	Assurance that assets owned by the organization (especially those with security exposure) are accounted for and returned upon termination.
		Related cybersecurity tools: • Template for Cybersecurity for Human Resources **Guidelines:** • Include steps to validate the return of all organization's assets held by workers as part of the procedures for clearing a party upon termination of service. • Document validation process through an official form (e.g. a clearance form) and require employees to sign it.

		Expected deliverables: • Signed clearance forms include employees' acknowledgment to return all organization's assets, with validation by the concerned department.
1-5	**Cybersecurity in Change Management**	
Objective	To ensure that cybersecurity requirements are included in change management methodology and procedures in order to protect the confidentiality, integrity and availability of information and technology assets as per CSPs policies and procedures, and related laws and regulations.	
Controls		
1-5-P-1	Cybersecurity requirements for change management within the CSP shall be identified, documented and approved.	
	Related cybersecurity tools: • Template for Cybersecurity requirements checklist on IT and change management projects **Guidelines:** • Develop and document cybersecurity policy for Change Management (including planned and exceptional changes) that include for example requirements for: ○ Prioritize cybersecurity-related changes. ○ Testing before making changes to the production environment in pre-production and pre-development stages. ○ Define roles and responsibilities. ○ Ensure a roll-back of an unsuccessful change. ○ Allow only privileged users to implement a change. ○ Elevate and approve privileges for making changes. ○ Enable audit logs for change implementation. ○ Monitor user activities when implementing changes. • Document cybersecurity requirements for change management. • Approve cybersecurity requirements for change management both by representatives of cybersecurity and Change Management department. • Support the organization's policy by the executive management. This must be done through the approval of the representative.	
	Expected deliverables: • Cybersecurity change management policy approved by the organization (e.g., electronic copy or official hard copy). • Formal approval by the head of the organization or his/her deputy on the policy (e.g., via the organization's official e-mail, paper or electronic signature).	
1-5-P-2	Cybersecurity requirements for change management within the CSP shall be applied.	

TLP: White

Document Classification: Public

	Guidelines: • Implementing all cybersecurity requirements for change management in the organization, including, but not limited to: ○ Executing approved cybersecurity change management requirements within the organization. This includes secure implementation procedures for planned changes in production systems and exceptional cybersecurity-related change implementation procedures.	
	Expected deliverables: • Documents confirming the implementation of cybersecurity requirements for change management, as documented in the policy document. • Document that clarifies an action plan for implementing cybersecurity requirements for change management.	
1-5-P-3	Cybersecurity for change management in the CSP shall cover, as a minimum:	
	1-5-P-3-1	Processes and procedures to securely implement changes (planned works) in production systems, with priority given to cybersecurity observations.
		Related Cybersecurity Tools: • Template for Cybersecurity requirements checklist on IT and change management projects **Guidelines:** • Develop and document change management procedures for implementing planned changes in secure ways, including ensuring that related requirements are implemented and necessary approvals are obtained according to defined roles and responsibilities. • Ensure that the procedures prioritize changes related to cybersecurity observations.
		Expected deliverables: • Change management procedures that include prioritizing the implementation of changes related to cybersecurity. • Evidence demonstrating verification of secure procedures during the execution of changes.
	1-5-P-3-2	Process for the implementation of cybersecurity exceptional changes (e.g.: changes during incident restoration).

		Related Cybersecurity Tools: • Template for Cybersecurity requirements checklist on IT and change management projects **Guidelines:** • Develop and document change management procedures for implementing planned changes in secure ways, including ensuring that related requirements are implemented and necessary approvals are obtained according to defined roles and responsibilities. • Include principles and procedures for cybersecurity exceptional change implementation (e.g. user activity monitoring, four-eyes principle in place) to ensure necessary approvals before any change. • Define technical procedures for quick access (e.g. break glass process) based on approved requirements (e.g. temporal privileged access is granted automatically under specific conditions – when the scope of the change is related to a cybersecurity incident). • Build technical capabilities for that process (e.g. privileged interactive sessions available only through dedicated channels).
		Expected deliverables: • A document that contains procedures for implementing exceptional changes. • Evidence that shows technical capability for monitoring and control changes.
1-5-P-4	Cybersecurity requirements for change management within the CSP shall be applied and reviewed periodically.	
	Related Cybersecurity Tools: • Template for Cybersecurity Reviewing and Auditing Policies **Guidelines:** • Review and update cybersecurity requirements for change management in the organization periodically according to a documented and approved plan for review and based on a planned interval, at least annually, or in the event of changes in relevant laws and regulations. • Document and approve review and changes to the organization's cybersecurity requirements for change management by the head of the organization or his/ her deputy.	
	Expected deliverables: • Log of updates and changes to the cybersecurity requirements for change management. • An approved document that sets the policy's review schedule.	

TLP: White

Document Classification: Public

	• Policy indicating that it has been reviewed and updated, and that changes have been documented and approved by the head of the organization or his/her deputy. • Formal approval by the head of the organization or his/her deputy on the updated policy (e.g., via the organization's official e-mail, paper or electronic signature).

2 (Cybersecurity Defense)

2-1	Asset Management	
Objective	To ensure that the CSP and CST has an accurate and detailed inventory of information and technology assets in order to support the organization's cybersecurity and operational requirements to maintain the confidentiality, integrity and availability of information and technology assets.	
Controls		
2-1-P-1	In addition to controls in the ECC control 2-1, the CSP shall cover the following additional controls for cybersecurity requirements for cybersecurity event logs and monitoring management, as a minimum:	
	2-1-P-1-1	Inventory of all information and technology assets using suitable techniques such as Configuration Management Database (CMDB) or similar capability containing an inventory of all technical assets.
		Related Cybersecurity Tools: • Template for Asset Management Policies • Template for Asset Management that contains Classification guide **Guidelines:** • Identify types of information and technology assets in use (e.g. using Asset Discovery techniques, scans, etc.). • Identify types of information and technology assets used in the dedicated assets for cloud computing systems (such as virtual servers, cloud storage, application firewall, etc.). • Maintain CMDB-class technology to capture all information and technical assets. • Update Asset Inventory automatically to capture fluent changes in cloud asset landscape.
		Expected deliverables: • Asset inventory techniques are identified and utilized. • Document outlining the inventory of technical assets specific to cloud systems. • Organization's information and technology assets information is maintained within an asset inventory (e.g. CMDB).
	2-1-P-1-2	Identifying assets owners and involving them in the asset management lifecycle.

TLP: White

Document Classification: Public

		Related Cybersecurity Tools: • Template for Asset Management Policies **Guidelines:** • Identify duties and obligations (e.g.: regulatory, contractual) associated with assets (e.g.: approve changes related to assets, manage accesses to assets). • Define and document Roles and Responsibilities for assets in the asset management lifecycle (e.g.: create, deploy, manage, dispose) and communicate them with asset owners. • Assign owners to information and technology assets to ensure that all information or technology asset has an owner.
		Expected deliverables: • Document outlining asset inventory and owners assigned to the assets. • Evidence demonstrating that roles and responsibilities of asset owners are aligned with their respective assets.
2-2	**Identity and Access Management**	
Objective	To ensure the secure and restricted logical access to information and technology assets in order to prevent unauthorized access and allow only authorized access for users which are necessary to accomplish assigned tasks.	
Controls		
2-2-P-1	In addition to sub controls in the ECC control 2-2-3, the CSP shall cover the following additional sub controls for cybersecurity requirements for identity and access management requirements, as a minimum:	
	2-2-P-1-1	Identity and access management of generic accounts credentials for accountability cannot be assigned for a specific individual.
		Related Cybersecurity Tools: • Template for Identity and Access Management Standards, encompassing password management • Template for Identity and Access Management Policy • Template for Standards on Devices with Sensitive Privileges **Guidelines:** • Identify both privileged and non-privileged generic accounts (e.g.: service accounts, technical accounts, non-personal accounts). • Implementing technical restrictions on user accounts based on assigned permissions (e.g.: regularly update credential information,

		establishing a policy for acceptable account usage, specifying authorized access, usage scenarios, and permissible procedures)
		Expected deliverables: • Document outlining the list of users of generic accounts (service accounts, technical accounts, etc.). • Technical restrictions applied to the use and management of generic accounts.
	2-2-P-1-2	Secure session management, including session authenticity, session lockout, and session timeout termination.
		Related Cybersecurity Tools: • Template for Identity and Access Management Standards, encompassing password management • Template for Identity and Access Management Policy • Template for Standards on Devices with Sensitive Privileges **Guidelines:** • Tunnel sessions through authenticated proxies with capability to lockout sessions and terminate due to inactivity (e.g.: use of cloud native bastion services, when applicable) • Configure session management system for session lockouts and session timeouts (e.g.: the session lockout after 15 minutes and timeout after 10 minutes of inactivity)
		Expected deliverables: • Evidence demonstrating configurations applied to sessions, including authenticity, lockout, and timeout.
	2-2-P-1-3	Multi-factor authentication for privileged users, and candidates of personnel with access to Cloud Technology Stack.

TLP: White

Document Classification: Public

		Related Cybersecurity Tools: • Template for Identity and Access Management Standards, encompassing password management • Template for Identity and Access Management Policy • Template for Standards on Devices with Sensitive Privileges **Guidelines:** • Define privileged roles and identities that have access to Cloud Technology Stack (e.g. Engineers, Operators, Administrators) • Build a mandatory multi-factor authentication (e.g. using software tokens, SMS messages) policy and assign it to privileged users or groups of users.
		Expected deliverables: • List of privileged accounts with access to Cloud Technology Systems (CTS). • Multi-factor authentication technologies for access to privileged accounts that have access to cloud technology systems (CTS).
	2-2-P-1-4	Formal process to detect and prevent unauthorized access (e.g. unsuccessful login attempt threshold).
		Related Cybersecurity Tools: • Template for Identity and Access Management Standards, encompassing password management • Template for Identity and Access Management Policy • Template for Standards on Devices with Sensitive Privileges **Guidelines:** • Define and implement an Identity and Access Management (IAM) process that includes the purpose, and governance of how a CSP must address unauthorized access threat for their respective defined scope. The process description contains as minimum: ○ Accepted user authentication methods with configuration (e.g. password complexity policy, MFA usage). ○ Conditional access requiring certain criteria to be met before granting access. ○ User authentication monitoring for anomalies and suspicious behaviour (e.g. many unsuccessful logins in a row, impossible travel).

		○ Enable self-service password to reset and password management ○ Configure e-mail/mobile notifications for cloud account authentications to make sure the account owner is notified about account authentications
		Expected deliverables: • Authentication and monitoring of Accesses. • The number of allowed access attempts is limited and the account is temporarily closed if the limit is exceeded. • Sample of system configuration and monitoring report. • Access attempt alerts.
	2-2-P-1-5	Utilizing secure methods and algorithms for saving and processing passwords, such as: Secure Hashing functions.
		Related Cybersecurity Tools: • Template for Identity and Access Management Standards, encompassing password management • Template for Identity and Access Management Policy • Template for Standards on Devices with Sensitive Privileges **Guideline:** • Store passwords (both locally and centrally) in an irreversible form (e.g. using secure hashing functions). • Use approved cryptography hash functions. • Review these functions periodically to prevent compromised or insufficient functions. • Use cryptographic salt to create unique password hashes even if users choose the same passwords. • Utilizing the mentioned algorithms and functions in national encryption standards(advanced level)
		Expected deliverables: • Evidence that demonstrates a sample of stored passwords. • Document outlining the applied standard to the storage of passwords.

TLP: White

Document Classification: Public

		Secure management of third-party personnel's accounts.
	2-2-P-1-6	**Related Cybersecurity Tools:** • Template for Identity and Access Management Standards, encompassing password management • Template for Identity and Access Management Policy • Template for Standards on Devices with Sensitive Privileges **Guideline:** • Define and implement Identity and Access Management (IAM) restrictions for accounts of third parties such as service providers, contractors, etc. • Define and implement procedures for managing third party accounts, including creating, monitoring and revocation, and obtaining the necessary approvals for each phase. • Enable event logs for third-party accounts and monitor their related activities. • Use clear label for third party accounts. • Use Federated Identities and Authentication services and identities (e.g.: ADFS, SAML2, oAuth2) for third parties' accounts. • Periodic review of accounts and privileges according to a defined review plan.
		Expected deliverables: • Restrictions implemented to third party accounts based on approved standards. • Procedures adopted for managing third party accounts during their life cycle. • A sample of third party account requests showing obtaining the necessary approvals. • Sample of third-party account activity monitoring logs. • Defined labels for third party accounts. • Implemented Federated Identities and Authentication. • Third party's accounts and privileges review plan and reports.
	2-2-P-1-7	Access control enforced to management systems, and administrative consoles.

		Related Cybersecurity Tools: • Template for Identity and Access Management Standards, encompassing password management • Template for Identity and Access Management Policy • Template for Standards on Devices with Sensitive Privileges **Guidelines:** • Identify and inventory management systems and administrative consoles, and review them periodically. • Obtain the necessary approvals before assigning any access to the administrative and management systems. • Review access privileges to management systems and administrative consoles periodically. • Use Privilege Access Management (PAM) technology to control access to administrative and management systems and encrypt communication through the network. • Enable Multi-Factor Authentication (MFA) for access to management systems and administrative consoles. • Activate and monitor event logs on activities related to accessing management systems and administrative consoles, and record access sessions.
		Expected deliverables: • List of management systems and administrative consoles. • A sample of requests for access to management systems and administrative consoles. • A plan to review the access privileges to management systems and administrative consoles and review reports. • Evidence of using Privilege Access Management (PAM) technology to access management systems and administrative consoles. • Evidence of encryption of access communications through the network for management systems and administrative consoles and a list of activated encryption algorithms. • Evidence of Multi-Factor Authentication (MFA) implementation. • A sample of event monitoring and related alerts from Security Information and Event Management (SIEM).

TLP: White

Document Classification: Public

		• A sample of recording of sessions.
	2-2-P-1-8	Masking of displayed authentication inputs, especially passwords, to prevent shoulder surfing.
		Related Cybersecurity Tools: • Template for Identity and Access Management Standards, encompassing password management • Template for Identity and Access Management Policy • Template for Standards on Devices with Sensitive Privileges **Guidelines:** • Activate data masking features for sensitive data (e.g. passwords, mobile numbers, and email addresses) when displayed during password recovery/change requests.
		Expected deliverables: • Evidence that demonstrates the implementation of obfuscation and masking of sensitive and personal information.
	2-2-P-1-9	Getting CST's approval before accessing any CST-related asset by the CSP or CSP's third parties.
		Related Cybersecurity Tools: • Template for Identity and Access Management Standards, encompassing password management • Template for Identity and Access Management Policy • Template for Standards on Devices with Sensitive Privileges **Guidelines:** • Make CST's approval a prerequisite before allowing any access to its associated assets or data by the CSP, provided that obtaining consent must be through approved channels between the CST and the CSP.
		Expected deliverables: • The approved access request procedures to access the CST's assets or data approved by the CSP. • A sample of approval requests.
	2-2-P-1-10	Capability to immediately interrupt a remote access session and prevent any future access for a user.

		Related Cybersecurity Tools: • Template for Identity and Access Management Standards, encompassing password management • Template for Identity and Access Management Policy • Template for Standards on Devices with Sensitive Privileges **Guidelines:** • Tunnel remote sessions through an authenticated proxy. • Configure proxy to terminate immediately the session under defined conditions (e.g.: policy violation). • Configure a proxy to stop accepting connections from specific sources or users.
		Expected deliverables: • Establish controlled remote access sessions. • Sample of system/proxy configurations.
	2-2-P-1-11	Provision to CSTs of Multi-factor authentication services for privileged cloud users.
		Related Cybersecurity Tools: • Template for Identity and Access Management Standards, encompassing password management • Template for Identity and Access Management Policy • Template for Standards on Devices with Sensitive Privileges • Template for Standards on Network Detection and Response (NDR) **Guidelines:** • Identify privileged cloud service user roles and groups, and enable the functionality of MFA for these users.
		Expected deliverables: • Evidence demonstrating that cloud services are authenticated using MFA.
	2-2-P-1-12	Assurance of restricted and controlled access to storage systems and means (such as Storage Area Network (SAN)).

TLP: White

Document Classification: Public

		Related Cybersecurity Tools: • Template for Identity and Access Management Standards, encompassing password management • Template for Identity and Access Management Policy • Template for Standards on Devices with Sensitive Privileges • Template for Storage Media Security Policy **Guidelines:** • Define cybersecurity requirements for access to storage systems. • Identify and inventory storage systems, including their types, owners, and the users who have access to them. • Define and implement Access Policy dedicated to storage systems that include the purpose, and governance of how a CSP must address unauthorized access threats to these systems. • Segregate storage and computing systems physically and logically from other systems. • Restrict access to these systems and not allow access without obtaining the necessary approvals.
		Expected deliverables: • Access Policy for storage systems. • The asset register containing storage systems. • Sample of access policy for storage implementation. • Sample of architecture design of storage systems. • Sample access requests for storage systems.
2-3	**Information System and Information Processing Facilities Protection**	
Objective	To ensure the protection of information systems and information processing facilities (including workstations and infrastructures) against cyber risks.	
Controls		
2-3-P-1	In addition to sub controls in the ECC control 2-3-3, the CSP shall cover the following additional sub controls for cybersecurity requirements for information system and processing facilities protection requirements, as a minimum:	
	2-3-P-1-1	Ensuring that all configurations are applied in accordance with CSP's cybersecurity standards.

		Related Cybersecurity Tools: • Template for Server Security Policy • Template for Server Security Standards • Template for Virtual System Security Standards • Template for Proxy Server System Standards • Template for Configuration and Hardening Policy **Guidelines:** • Document and approve cybersecurity standards for information systems. • Configure information systems based on the approved standards before deployment and before implementing changes. • Verify periodically information systems configurations based on the approved standards. • Monitor changes to configurations. • Restrict modification rights of configurations to privileged roles. • Manage modifications of configurations in a formal Change Management process.
		Expected deliverables: • Approved cybersecurity standards for information systems. • Checklist for applying standards to configurations before deployment and before changes are applied. • Review plan for information systems configurations and review reports. • Sample event logs for monitoring changes to configurations. • Restrictions applied to modifying configurations and the list of workers with permission to change configurations. • A sample of configurations change requests.
	2-3-P-1-2	Assurance of separation and isolation of data, environments and information systems across CSTs, to prevent data commingling.
		Related Cybersecurity Tools: • Template for Server Security Policy • Template for Server Security Standards • Template for Virtual System Security Standards • Template for Proxy Server System Standards

TLP: White

Document Classification: Public

		• Template for Configuration and Hardening Policy • Template for Data Cybersecurity Policy • Template for Data Cyber Security Standards **Guidelines:** • Implement reliable mechanisms for separation and isolation of CSTs' data using virtualization hardware at the level of environments, servers, networks, and information processing systems (e.g.: Software Defined Network). • Periodically test isolation mechanisms (e.g. penetration tests).
		Expected deliverables: • Data and systems verified separation across CSTs.' data. • Test reports to validate the prevention of data commingling.
	2-3-P-1-3	Adopting of cybersecurity principles for technical system configurations adhering to the minimum functionality principle.
		Related Cybersecurity Tools: • Template for Server Security Policy • Template for Server Security Standards • Template for Virtual System Security Standards • Template for Proxy Server System Standards • Template for Configuration and Hardening Policy **Guidelines:** • Activate the "Minimum Functionality Principle" at the level of solution and systems architecture based on business needs and service providers' recommendations. • Define and implement minimum baseline requirements for the configuration and functionality of technologies, systems, software, and services. • Review configurations periodically to verify that excessive functions are not enabled.
		Expected deliverables: • Minimum functionality requirements defined at the level of configuration and functionality for technologies, systems, software and services, etc. • Configuration audit reports for compliance with specified requirements.

	2-3-P-1-4	The ability of the Cloud Technology Stacks to securely handle input validation, exceptions, and failures.
		Related Cybersecurity Tools: • Template for Server Security Policy • Template for Server Security Standards • Template for Virtual System Security Standards • Template for Proxy Server System Standards • Template for Configuration and Hardening Policy **Guidelines:** • Implement unified input validation technical framework across the Cloud Technology Stacks (e.g.: special characters, length, character sets, etc.). • Configure Cloud Technology Stacks to validate inputs. • Configure logging and monitoring to catch exceptions and failures.
		Expected deliverables: • A sample of the configuration for input validation. • A sample of enabling automatic monitoring and logging to catch exceptions and failures. • Evidence confirming the logging and monitoring of alerts/audit reports.
	2-3-P-1-5	Full isolation of security functions and applications from other functions and applications in the Cloud Technology Stack.
		Related Cybersecurity Tools: • Template for Server Security Policy • Template for Server Security Standards • Template for Virtual System Security Standards • Template for Authenticated Server Systems Standards **Guidelines:** • Deploy security solutions/tools and applications in dedicated physical or logical environments.
		Expected deliverables: • Document demonstrating that security functions and applications are isolated from other functions and applications in the Cloud Technology Stack.

TLP: White

Document Classification: Public

		• Architecture design documentation.
	2-3-P-1-6	Notify the CSTs of the cybersecurity requirements provided by the CSP and applicable for use by the CSTs.
		Related Cybersecurity Tools: • Template for Server Security Policy • Template for Server Security Standards • Template for Virtual System Security Standards • Template for Proxy Server System Standards **Guidelines:** • Define cybersecurity requirements for CSTs (e.g.: secure connection, secure integration protocol) • Send notifications to CSTs about security requirements provided by the service provider and the methods of activating them on the services used by subscribers.
		Expected deliverables: • A document of cybersecurity requirements provided by the service provider and methods of activating them on the services used by the subscribers. • Evidence that demonstrates the communication of requirements that can be activated according to the request of the subscribers, which have been shared with them.
	2-3-P-1-7	Detection and prevention of unauthorized changes to software, and systems.
		Related Cybersecurity Tools: • Template for Server Security Policy • Template for Server Security Standards • Template for Virtual System Security Standards • Template for Proxy Server System Standards **Guidelines:** • Identify and document Cybersecurity requirements for Change Management, Access Control, and Logging and Monitoring to detect and prevent unauthorized changes (e.g.: define roles and responsibilities to design, approve, and implement a change; allow only

		privileged users to implement a change; elevate privileges for making changes; enable audit logs for change implementation; monitor user activities when implementing changes) • Implement both administrative and technical controls to enforce these requirements (e.g. Change Management, Privileged Access Management systems, Logging and Monitoring systems)
		Expected deliverables: • Cybersecurity requirements for change management. • Provided evidence that confirms applied restrictions that prevent, detect, and remediate unauthorized changes. • Evidence illustrating system configuration for change prevention tools. • Documents demonstrating change monitoring report/alerts.
	2-3-P-1-8	Complete isolation and protection of multiple guest environments.
		Related Cybersecurity Tools: • Template for Server Security Policy • Template for Server Security Standards • Template for Virtual System Security Standards • Template for Proxy Server System Standards **Guidelines:** • Build and maintain the Threat Model for the virtualization technology. • Identify and respond to virtualization technology issues (e.g.: memory leak, escape to host). • Configure virtualization technology for guest isolation • Test virtualization technology for issues related to isolation and protection of guest environment.
		Expected deliverables: • Guest environments isolated. • Architectural design document for hosting environments illustrating isolation. • Sample of virtual environment threat model. • Sample of test report.

TLP: White

Document Classification: Public

	2-3-P-1-9	The community cloud services provided to CSTs (government organizations and CNI organizations) shall be isolated from any other cloud computing provided to organizations outside the scope of work.
		Related Cybersecurity Tools: • Template for Server Security Policy • Template for Server Security Standards • Template for Virtual System Security Standards • Template for Proxy Server System Standards **Guidelines:** • Define necessary procedures to ensure the physical and logical isolation and segregation of cloud services provided to government organizations and CNI organizations from any other cloud computing provided to organizations outside the scope of work. • Implement the isolation mechanisms between community cloud and public/private and other community clouds (e.g.: physical and logical barriers applied)
		Expected deliverables: • Architectural design documentation. • Sample of the Isolation mechanisms implemented between cloud services provided to government entities and sensitive infrastructure entities from any other cloud computing services provided to other external entities.
	2-3-P-1-10	Provide cloud computing services from within the KSA, including systems used for storage, processing, and disaster recovery centers.
		Related Cybersecurity Tools: • Template for Server Security Policy • Template for Server Security Standards • Template for Virtual System Security Standards • Template for Proxy Server System Standards **Guidelines:** • Build cloud computing and data storage and processing infrastructure (both main and disaster recovery) within the KSA (e.g. Data Centres located in the KSA, cloud operations team based in the KSA).
		Expected deliverables:

		• Cloud data centers are located in the KSA. • Architectural design document for storage systems, processing systems, and disaster recovery centers, with an explanation of their geographical location, whether leased or owned through contract. • Evidence illustrating the addresses of the centers' locations.
	2-3-P-1-11	Provide cloud computing services from within the KSA, including systems used for monitoring, and support.
		Related Cybersecurity Tools: • Server Security Policy Template • Server Security Standard Template • Template for Standards on Virtual System Security • Template for Standards on Proxy Server Systems **Guidelines:** • Build cloud computing monitoring and support infrastructure within KSA.
		Expected deliverables: • Evidence that illustrates the monitoring and cloud computing services support centers are based in the KSA. • Architectural design document for storage systems, processing systems, and disaster recovery centers, with an explanation of their geographical location. • Sample of contracts whether leased or owned. • Evidence illustrating the addresses of the centers' locations.
	2-3-P-1-12	Modern technologies, such as Endpoint Detection and Response (EDR) technologies, to ensure that the information servers and devices of CSP's information processing systems and devices of are ready for rapid response to incidents.
		Related Cybersecurity Tools: • Template for Endpoint Detection and Response (EDR) • Template for Advanced Persistent Threat (APT) Protection Standard • Template for Advanced Persistent Threat (APT) System Protection Standards • Template for Malware Protection Policy • Template for Malware Protection Standards • Template for Server Security Policy

TLP: White

Document Classification: Public

		• Template for Server Security Standard • Template for Virtual System Security Standards • Template for Proxy Server Systems Standards **Guidelines:** • Provide EDR techniques and mechanisms to detect, prevent, and protect against programs, suspicious activities, and malware. • Ensure that the technologies provided are up-to-date and contain advanced and persistent attacks (APT) protection. • Review the protection system periodically to ensure that the scope of the protection system is comprehensive for all users' devices, party systems, and servers through the control unit of the protection system. • Develop and implement a corrective action plan (when needed) to install the protection system on all devices. • Follow up the protection system periodically to ensure the updates are released on all users' devices, the party's systems and servers.
		Expected deliverables: • EDR systems implemented across all devices and servers. • EDR systems configurations review plan and reports. • EDR systems updates plan and reports.
2-4	**Networks Security Management**	
Objective	To ensure the protection of CSP's and CST's network from cyber risks.	
Controls		
2-4-P-1	In addition to sub controls in the ECC control 2-5-3, the CSP shall cover the following additional sub controls for cybersecurity requirements for networks security management requirements, as a minimum:	
	2-4-P-1-1	Monitoring of traffic across the external and internal networks to detect anomalies.

		Related Cybersecurity Tools: • Template for Network Security Standards • Template for Network Security Policy **Guidelines:** • Define scope for Network Anomaly Detection. • Identify all internal and external networks and network routes. • Establish methods and thresholds for effective Anomaly Detection considering low False Positives rates. • Implement a monitoring solution considering traffic volume. • Correlate network events with other security events. • Periodically review correlations rules. • Consider AI-based anomaly detection methods.
		Expected deliverables: • Inventory of network flows. • Anomaly detection rules defined on detection tools.
	2-4-P-1-2	Network isolation and protection of Cloud Technology Stack network from other internal and external networks.
		Related Cybersecurity Tools: • Template for Network Security Standards • Template for Network Security Policy **Guidelines:** • Identify potential risks related to Cloud Technology Stack network and apply relevant protection. • Isolate physically or logically (e.g.: Software Defined Networks) networks for Cloud Technology Stack and internal and external networks.
		Expected deliverables: • Threat Model for Cloud Technology Stack network. • Network-level controls implementation. • Architecture design documentation.
	2-4-P-1-3	Protection from denial-of-service attacks (including Distributed Denial of Service (DDoS)).

TLP: White

Document Classification: Public

		Related Cybersecurity Tools: • Template for Network Security Standards • Template for Network Security Policy • Template for Distributed Denial of Service (DDos) Protection Standard **Guidelines:** • Identify networks exposed to denial-of-service and distributed denial of service attacks. • Establish network monitoring to detect volumetric attacks. • Conduct deep packet analysis to detect bot-generated traffic for black-holing. • Utilize technologies and techniques to stop and prevent DDoS attacks.
		Expected deliverables: • A document or report demonstrating that Denial of Service threats are analysed, detected and mitigated.
	2-4-P-1-4	Protection of data transmitted through the network; from and to the Cloud Technology Stack network using cryptography primitives; for management and administrative access.
		Related Cybersecurity Tools: • Template for Network Security Standards • Template for Network Security Policy **Guidelines:** • Encrypt Cloud Technology Stack management and administrative network connection (both interactive and non-interactive - API) with strong encryption mechanisms using random number generators, entropy sources, and basic memory or math operations that are required by the cryptographic algorithms.
		Expected deliverables: • Evidence illustrating that Cloud Technology management networks are strongly encrypted.
	2-4-P-1-5	Access control between different network segments.
		Related Cybersecurity Tools: • Template for Network Security Standards • Template for Network Security Policy **Guidelines:** • Enforce only authenticated traffic between different network segments.

		• Assign the network connection to a user/identity who is responsible for data transfers between network segments. • Manage authorizations to establish connections across network segments.
		Expected deliverables: • Network connections assigned to authenticated users/identities. • Access control list.
	2-4-P-1-6	Isolation between cloud service delivery network, cloud management network and CSP enterprise network.
		Related Cybersecurity Tools: • Template for Network Security Standards • Template for Network Security Policy **Guidelines:** • Segregate physically or logically corporate networks from networks related to cloud services and cloud management and build isolation mechanisms (e.g.: Software Defined Networks) for these networks.
		Expected deliverables: • Isolation mechanisms for networks. • Architecture design documentation.
2-5	**Mobile Devices Security**	
Objective	To ensure the protection of mobile devices (including laptops, smartphones, and tablets) from cyber risks and to ensure the secure handling of the CSPs' and CSTs' information (including sensitive information) while utilizing mobile devices.	
Controls		
2-5-P-1	In addition to sub controls in the ECC control 2-6-3, the CSP shall cover the following additional sub controls for cybersecurity requirements for mobile device security, as a minimum:	
	2-5-P-1-1	Inventory of all end user and mobile devices.
		Related Cybersecurity Tools: • Template for User Devices, Mobile Devices, and Personal Devices Security Policy • Template for User Devices Security Standard • Template for Mobile Devices Security Standard **Guidelines:**

TLP: White

Document Classification: Public

		• Maintain the inventory of all end-user devices (e.g.: laptops, tablets) and mobile devices (e.g. smartphones, smartwatches) and their owners and users. Consider both CSP-owned and BYOD. • Periodically (e.g. annually) review the inventory
		Expected deliverables: • Maintained inventory of end-user and mobile devices. • Periodic reviews reports.
	2-5-P-1-2	Centralized mobile device security management.
		Related Cybersecurity Tools: • Template for User Devices, Mobile Devices, and Personal Devices Security Policy • Template for User Devices Security Standard • Template for Mobile Devices Security Standard **Guidelines:** • Define requirements for centralized platform to manage security of mobile devices (e.g.: apply security policy, enforce PIN to unlock device, wipe device) • Select and deploy centralized security management platform/product • On-board all mobile devices in business use to that platform
		Expected deliverables: • All mobile devices centrally managed in terms of security. • Sample of system configuration.
	2-5-P-1-3	Screen locking for end user devices.
		Related Cybersecurity Tools: • Template for Configuration and Hardening Policy • Template for User Devices, Mobile Devices, and Personal Devices Security Policy • Template for User Devices Security Standard • Template for Mobile Devices Security Standard • Plan for Cybersecurity Awareness Program **Guidelines:**

		• Define screen lock policy and relevant parameters (e.g. timeout, unlock methods). • Enforce that policy by configuring end user devices accordingly (e.g. using Active Directory GPO, end-point agents or MDM) • Make users aware to lock screen manually when they are not close to them.
		Expected deliverables: • Screen lock policy enforced to user devices. • Documents illustrating user awareness methods for manually locking the screen when they are not in proximity to their devices.
	2-5-P-1-4	Data sanitation and secure disposal for end-user devices, especially for those with exposure to the Cloud Technology Stack.
		Related Cybersecurity Tools: • Template for User Devices, Mobile Devices, and Personal Devices Security Policy • Template for User Devices Security Standard • Template for Mobile Devices Security Standard **Guidelines:** • Identify end-user devices and technologies exposed to the Cloud Technology Stack (e.g.: MS Windows, Linux, Apple iOS) • Select effective data sanitation and disposal methods relevant to these technologies. • Dispose securely these devices (and data) when necessary.
		Expected deliverables: • Approved and implemented data sanitation and device disposal tools and methods for Cloud Technology Stack - related end-user devices.
2-6	**Data and Information Protection**	
Objective	To ensure the confidentiality, integrity and availability of CSPs' and CSTs' data and information as per organizational policies and procedures, and related laws and regulations.	
Controls		
2-6-P-1	In addition to sub controls in the ECC control 2-7-3, the CSP shall cover the following additional sub controls for cybersecurity requirements for data and information protection requirements, as a minimum:	

	2-6-P-1-1	Prohibiting the use of Cloud Technology Stack's data in any environment other than production environment, except after applying strict controls for protecting that data, such as: data masking or data scrambling techniques.
		Guidelines: • Segregate physically or logically production and non-production environment. • Generate and use synthetic data in non-production environments • Build barriers to transfer data from/to production environment • Introduce an authorized channel/gateway to exchange data between environments that verifies data relevant to Cloud Technology Stack is masked/tokenized/scrambled in a way that ensures that original data cannot be reverse engineered.
		Expected deliverables: • Segregated production data with test data. • Architecture design documentation.
	2-6-P-1-2	Provision to CSTs of securely data storage processes, procedures, and technologies to comply with related legal and regulatory requirements.
		Guidelines: • Identify legal and regulatory requirements related to cloud data storage (e.g.: encryption of personal information) • Enable functionalities and technologies (and related processes) to let CSTs comply with these obligations (e.g. encryption mechanisms inbuilt in cloud services) • Communicate to CST these functionalities
		Expected deliverables: • List of applicable legal and regulatory requirements. • Data storage processes and technologies compliant to legal requirements.
	2-6-P-1-3	Disposal of CST's data should be performed in a secure manner on termination or expiry of the contract with the CSP.

		Guidelines: • Monitor contracts with CSTs regarding their expiration or termination. • Dispose CST's data as soon as possible when there is no valid contract. • Dispose CST's data using approved methods to ensure this process is irreversible considering used data storage technical methods and data recovery technical capabilities.
		Expected deliverables: • Contract statuses monitoring • Records of disposed CSTs data with specification of the disposal methods used.
	2-6-P-1-4	Commitment to maintain the confidentiality of the CST's data and information, according to related legal and regulatory requirements.
		Guidelines: • Identify and analyse legal and regulatory requirements for storing and processing CST's data (e.g.: data encryption).
		Expected deliverables: • Ensure storing and processing CST's data is subject to legal and regulatory regulations.
	2-6-P-1-5	Providing CSTs with secure means to export and transfer data and virtual infrastructure
		Guidelines: • Build cloud services with embedded functionalities to export and transfer data and virtual infrastructure out over a secured, encrypted connection or channel.
		Expected deliverables: • Secure data/assets export functionalities over an encrypted and secure channel or connection.
2-7	**Cryptography**	
Objective	To ensure the proper and efficient use of cryptography to protect information assets as per policies, procedures, and related laws and regulations.	
Controls		

TLP: White

Document Classification: Public

2-7-P-1	In addition to sub controls in the ECC control 2-8-3, the CSP shall cover the following additional sub controls for cryptography, as a minimum:	
	2-7-P-1-1	Technical mechanisms and cryptographic primitives for strong encryption, in according to the advanced level in the National Cryptographic Standards (NCS-1:2020).
		Related Cybersecurity Tools: • Template for Encryption Standard • Template for Encryption Key Management Standard • Template for Encryption Policy **Guidelines:** • Build encrypted cloud storage services compliant with the National Cryptographic Standards (NCS-1:2020)
		Expected deliverables: • NCS-1:2020 compliant data encryption mechanisms
	2-7-P-1-2	Certification authority and issuance capability in a secure manner, or usage of certificates from a trusted certification authority.
		Related Cybersecurity Tools: • Template for Encryption Standard • Template for Encryption Key Management Standard • Template for Encryption Policy **Guidelines:** • Build certification authority and issuance capability considering best practices in this area (e.g.: dedicated and isolated environment, strict access control, hardware security modules in place) • Review certificates in use if issued by trusted certification authority.
		Expected deliverables: • Installation and activation of a trusted source/authority for accreditation. • Trusted and certified certificates
2-8	**Backup and Recovery Management**	
Objective	To ensure the protection of CSPs' data and information including information systems and software configurations from cyber risks as per organizational policies and procedures, and related laws and regulations.	
Controls		

TLP: White

Document Classification: Public

2-8-P-1	In addition to sub controls in the ECC control 2-9-3, the CSP shall cover the following additional sub controls for cybersecurity requirements for backup and recovery management, as a minimum:	
	2-8-P-1-1	Securing access, storage and transfer of CST's data backups and its mediums, and protecting it against damage, amendment or unauthorized access.
		Related Cybersecurity Tools: • Template for Backup Policy • Template for Backup Standards • Template for Storage Media Security Standards **Guidelines:** • Identify risks related to access, storage and transfer of CST's data backups and its media, including those related to damage, amendment or unauthorized access (e.g.: accidental damage, theft, lost media) • Define security measures for secure access, storage and transfer of CST's data backups (e.g. access control, encryption) • Implement defined measures. • Periodically review implemented security measures to ensure its applicability.
		Expected deliverables: • List of identified risks. • Defined and applied security measures. • Regular review reports.
	2-8-P-1-2	Securing access, storage and transfer of Cloud Technology Stack backups and its mediums, and protecting it against damage, amendment or unauthorized access.
		Related Cybersecurity Tools: • Template for Backup Policy • Template for Backup Standards • Template for Storage Media Security Standards **Guidelines:** • Identify risks related to access, storage and transfer of CTS data backups and its media, including those related to damage, amendment or unauthorized access (e.g.: accidental damage, theft, lost media) • Define security measures for secure access, storage and transfer of CTS data backups (e.g. access control, encryption)

TLP: White

Document Classification: Public

		• Implement defined measures. • Periodically review implemented security measures to ensure its applicability.
		Expected deliverables: • List of identified risks. • Defined and applied security measures. • Regular review reports.
2-9	**Vulnerabilities Management**	
Objective	To ensure timely detection and effective remediation of technical vulnerabilities to prevent or minimize the probability of exploiting these vulnerabilities to launch cyber-attacks against the CSP and CST.	
Controls		
2-9-P-1	In addition to sub controls in the ECC control 2-10-3, the CSP shall cover the following additional sub controls for cybersecurity requirements for vulnerability management requirements, as a minimum:	
	2-9-P-1-1	Assessing and remediating vulnerabilities on external components of Cloud Technology Stack at least once every month, and at least once every three months for internal components of Cloud Technology Stack.

TLP: White

Document Classification: Public

		Related Cybersecurity Tools: • Template for Security Vulnerability Assessment Procedure, including a registry template for managing discovered vulnerabilities • Template for Vulnerability Log • Template for Vulnerability Management Policy • Template for Vulnerability Management Standard **Guidelines:** • Define and implement a Threat and Vulnerability Management policy that includes the intent, purpose, and governance of how a CSP must address threats and vulnerabilities for their respective scope under the Security Shared Responsibility Model. At a minimum, the policy should specify: ○ The frequency of assessments for external components of Cloud Technology Stack - monthly assessments. ○ The frequency of assessments for internal components of Cloud Technology Stack - quarterly assessments. ○ Remediation of threats and vulnerabilities for external components and internal components must be completed based on the severity of the identified threats and vulnerabilities. ○ Identify vulnerability detection methods that are in use. ○ What components to be covered under the scope considering applicable laws, regulations, and contractual requirements. ○ The vulnerability severity levels relevant to the organization. ○ When and how and to whom vulnerabilities should be reported and reviewed, especially significant vulnerabilities. ○ How remediating actions are tracked for timely and effective closure.
		Expected deliverables: • Threat and Vulnerability Management Policy. • Sample of assessments. • Sample of remediation's plans and actions.
	2-9-P-1-2	Notification to CSTs of identified vulnerabilities that may affecting them, and safeguards in place.

TLP: White

Document Classification: Public

		Related Cybersecurity Tools: • Template for Security Vulnerability Assessment Procedure, including a registry template for managing discovered vulnerabilities • Template for Vulnerability Log • Template for Vulnerability Management Policy • Template for Vulnerability Management Standard **Guidelines:** • Report immediately to CSTs detected vulnerabilities (that impact them) with sufficient information to analyse related risks and correlate Threat Response on CST side.
		Expected deliverables: • Reports sent to CSTs about detected vulnerabilities that impact them.
2-10	**Penetration Testing**	
Objective	To assess and evaluate the efficiency of the CSP's cybersecurity defense capabilities through simulated cyber-attacks to discover unknown weaknesses within the technical infrastructure that may lead to a cyber-breach.	
Controls		
2-10-P-1	In addition to sub controls in the ECC control 2-11-3, the CSP shall cover the following additional sub controls for cybersecurity requirements for penetration testing, as a minimum:	
	2-10-P-1-1	Scope of penetration tests must cover Cloud Technology Stack and must be conducted at least once every six months.
		Related Cybersecurity Tools: • Template for Penetration Testing Policy • Template for Penetration Testing Standard **Guidelines:** • Identify Cloud Technology Stack components. • Periodically (every six months) conduct penetration tests of all Clout Technology Stack components. • Verify completeness of scope for penetration tests of Cloud Technology Stack.
		Expected deliverables: • Penetration tests conducted to the entire Cloud Technology Stack
2-11	**Cybersecurity Event Logs and Monitoring Management**	

<table>
<tr><td>Objective</td><td colspan="2">Ensure timely collection, analysis and monitoring of cybersecurity event logs for the proactive detection and effective management of cyber-attacks to prevent or minimize the impact on the CSPs' and CSTs' business.</td></tr>
<tr><td colspan="3">Controls</td></tr>
<tr><td rowspan="4">2-11-P-1</td><td colspan="2">In addition to sub controls in the ECC control 2-12-3, the CSP shall cover the following additional sub controls for cybersecurity requirements for cybersecurity event logs and monitoring management, as a minimum:</td></tr>
<tr><td rowspan="3">2-11-P-1-1</td><td>Activating and protecting event logs and audit trails of Cloud Technology Stack.</td></tr>
<tr><td>Related Cybersecurity Tools:<ul><li>Template for Cybersecurity Event Logs and Monitoring Management Policy</li><li>Template for Cybersecurity Event Logs and Monitoring Management Standard</li></ul>Guidelines:<ul><li>Define and implement a Log Management policy that includes the intent, purpose, and governance of how a CSP must enable logging and monitoring of cybersecurity events for their respective scope under the Security Shared Responsibility Model. At a minimum, the policy should specify:<ul><li>The protection methods for logs where these are generated to prevent log tampering or logging technology evasion.</li><li>The protection methods for logs transmitted to the log repositories to ensure their confidentiality and integrity with encryption.</li></ul></li></ul></td></tr>
<tr><td>Expected deliverables:<ul><li>Log management policy.</li><li>Centralized and protected Log base.</li></ul></td></tr>
<tr><td rowspan="2">2-11-P-1-2</td><td>Activating and collecting login attempts history.</td></tr>
<tr><td>Related Cybersecurity Tools:<ul><li>Template for Cybersecurity Event Logs and Monitoring Management Policy</li><li>Template for Cybersecurity Event Logs and Monitoring Management Standard</li></ul>Guidelines:</td></tr>
</table>

TLP: White

Document Classification: Public

		• Configure authentication mechanisms for logging authentication attempts (e.g.: data, time, authentication method, system/application, user id/Identity) • Collect and store that information
		Expected deliverables: • Stored and recorded login attempts. • Evidence illustrating mechanisms for verifying login attempts.
	2-11-P-1-3	Activating and protecting all event logs of activities and operations performed by the CSP at the tenant level in order to support forensic analysis.
		Related Cybersecurity Tools: • Template for Cybersecurity Event Logs and Monitoring Management Policy • Template for Cybersecurity Event Logs and Monitoring Management Standard **Guidelines:** • Define requirements for logging of activities of CSP and CSTs that is sufficiently to support forensic analysis (e.g.: chain of custody) • Build logging functionality to capture these events/activities and protect logs (e.g.: ensure confidentiality, integrity and availability of these logs using encryption, HMAC and redundant storage.
		Expected deliverables: • CSP and CST event/activity log
	2-11-P-1-4	Protecting cybersecurity event logs from alteration, disclosure, destruction and unauthorized access and unauthorized release, in accordance with regulatory, or law requirements.

		Related Cybersecurity Tools: • Template for Cybersecurity Event Logs and Monitoring Management Policy • Template for Cybersecurity Event Logs and Monitoring Management Standard **Guidelines:** • Identify law and regulatory requirements regarding for audit logs. • Define and implement a Cybersecurity Log Management and Access Control policy that includes the intent, purpose, and governance of how a CSP must enable logging and monitoring of cybersecurity events for their respective scope under the Security Shared Responsibility Model. At a minimum, the policies should specify: ○ The protection methods for logs where these are generated to prevent log tampering or logging technology evasion. ○ The protection methods for logs transmitted to the log repositories to ensure their confidentiality and integrity with encryption. ○ Secure log destruction methods. ○ Restricted Access to logs ○ Read-only Access to logs
		Expected deliverables: • Cybersecurity event logs protected. • Restrictions applied to protect the logs. • Secured log destruction methods. • List of law and regulatory requirements for audit log.
	2-11-P-1-5	Continuous cybersecurity events monitoring using SIEM technique covering the full Cloud Technology Stack.
		Related Cybersecurity Tools: • Template for Cybersecurity Event Logs and Monitoring Management Policy • Template for Cybersecurity Event Logs and Monitoring Management Standard **Guidelines:** • Define requirements for cybersecurity events monitoring (e.g. capture of user authentications, privilege elevations, software execution)

TLP: White

Document Classification: Public

		• Define scope for cybersecurity events monitoring covering Cloud Technology Stack • Select and deploy SIEM-class system to monitor cybersecurity event logs. • Monitor cybersecurity event logs continuously (at least daily).
		Expected deliverables: • Cybersecurity logs monitored in SIEM • List of requirements for cybersecurity event monitoring. • Sample of monitoring reports/alerts.
	2-11-P-1-6	Reviewing cybersecurity event logs and audit trails periodically, covering CSP events in the Cloud Technology Stack.
		Related Cybersecurity Tools: • Template for Cybersecurity Event Logs and Monitoring Management Policy • Template for Cybersecurity Event Logs and Monitoring Management Standard **Guidelines:** • Define scope for CSP event logs reviews covering the Cloud Technology Stack. • Define criteria for reviews. • Select and assign skilled and independent reviewers of cybersecurity event logs/audit trails. • Review periodically cybersecurity event logs/audit trails.
		Expected deliverables: • Cybersecurity event logs reviewed by skilled and independent reviewers. • Sample of reports, alerts, use cases.
	2-11-P-1-7	Automated monitoring and logging of remote access sessions event logs.

		Related Cybersecurity Tools: • Template for Cybersecurity Event Logs and Monitoring Management Policy • Template for Cybersecurity Event Logs and Monitoring Management Standard **Guidelines:** • Log remote access sessions and relevant events. • Define markers, indicators and patterns for malicious remote accesses. • Monitor, detect and block automatically these remote sessions
		Expected deliverables: • Remote sessions automatically monitored
	2-11-P-1-8	Secure handling of user-related data found in the audit trails and the cybersecurity event logs.
		Related Cybersecurity Tools: • Template for Cybersecurity Event Logs and Monitoring Management Policy • Template for Cybersecurity Event Logs and Monitoring Management Standard **Guidelines:** • Detect user related data event logs/audit trails. • Anonymize that data using tokens.
		Expected deliverables: • Personally Identifiable Information anonymized in logs
2-12	**Cybersecurity Incident and Threat Management**	
Objective	Ensure timely identification and detection of cybersecurity incidents and their effective management and proactive response to cybersecurity threats to prevent or minimize the impact of the impacts resulting on the business of the CSPs.	
Controls		
2-12-P-1	In addition to sub controls in the ECC control 2-13-3, the CSP shall cover the following additional sub controls for cybersecurity requirements for cybersecurity incident and threat management, as a minimum:	
	2-12-P-1-1	Subscribing in authorized and specialized organizations and groups to stay up-to-date on cybersecurity threats, common practices and key know-how.

TLP: White

Document Classification: Public

		Related Cybersecurity tools: • Template for Cybersecurity Incident and Threat Management Policy • Template for Cybersecurity Incident and Threat Management Standards • Cybersecurity Incident Response Guidelines • Template for Cybersecurity Incident Response Detailed Plan **Guidelines:** • Select trusted external threat intelligence vendors (e.g. OSINT) • Monitor publications issued by the National Cybersecurity Authority (NCA) and relevant trusted authorities. • Analyse threat intelligence feeds and services for risks relevant to the CSP. • Confirm common and best practices in Threat Management with external cybersecurity advisors and consultants.
		Expected deliverables: • List of trusted external threat intelligence vendors. • Cybersecurity threat intelligence. • Knowledgebase of common and best practices in cybersecurity.
	2-12-P-1-2	Training for employees and third-party personnel to respond to cybersecurity incidents, in line with their roles and responsibilities.
		Related Cybersecurity tools: • Template for Cybersecurity Incident and Threat Management Policy • Template for Cybersecurity Incident and Threat Management Standards • Cybersecurity Incident Response Guidelines • Template for Cybersecurity Incident Response Detailed Plan **Guidelines:** • Establish a cybersecurity training program for employed and contracted personnel. • Train personnel in cybersecurity incident reporting and handling based on their roles and responsibilities (e.g.: what is a cybersecurity incident and how to report it). • Align the training program with roles and responsibilities of various groups.

		Expected deliverables: • Cybersecurity training program aligned with roles and responsibilities of the target groups. • Sample of training certificates/attendance.
	2-12-P-1-3	Periodically testing the incident response capability.
		Related Cybersecurity tools: • Template for Cybersecurity Incident and Threat Management Policy • Template for Cybersecurity Incident and Threat Management Standards • Cybersecurity Incident Response Guidelines • Template for Cybersecurity Incident Response Detailed Plan **Guidelines:** • Schedule regular reviews of incident response plans. • Define testing methodology and use appropriate testing method (e.g.: table top exercise, walkthrough, cut-over, incident simulation). • Make a Lesson Learnt a mandatory phase of testing methodology.
		Expected deliverables: • Incident response plan / procedure test schedule. • Report outlining the methodology for testing the cybersecurity incident response capabilities. • Lesson Learnt records.
	2-12-P-1-4	Root Cause Analysis of cybersecurity incidents and developing plans to address them.
		Related Cybersecurity tools: • Template for Cybersecurity Incident and Threat Management Policy • Template for Cybersecurity Incident and Threat Management Standards • Cybersecurity Incident Response Guidelines • Template for Cybersecurity Incident Response Detailed Plan **Guidelines:** • Make a Root Cause Analysis a mandatory phase of Incident Response to improve Incident Response Plans. • Gather, analyse, prioritize and address conclusions of Root Cause Analyses.

TLP: White

Document Classification: Public

		Expected deliverables: • Root Cause Analysis is mandatory part of Incident Response. • Root Cause Analysis conclusions are prioritized and addressed. • Incident Response Plan is constantly improved based on Root Cause Analysis conclusions. • Sample of root cause analysis.
	2-12-P-1-5	Support the CST in cases legal proceedings and forensics, protecting the chain of custody that falls under the management and responsibility of the CSP, in accordance with the related law and regulatory requirements.
		Related Cybersecurity tools: • Template for Cybersecurity Incident and Threat Management Policy • Template for Cybersecurity Incident and Threat Management Standards • Cybersecurity Incident Response Guidelines • Template for Cybersecurity Incident Response Detailed Plan **Guidelines:** • Analyse legal and regulatory requirements for CSTs. • Build legal and forensics capabilities to support CTSs in their legal obligations relevant to cloud services. • Build a process to track movement of evidence and ensure integrity of evidence during that movement and at rest.
		Expected deliverables: • Evidence demonstrating the knowledge and understanding of legal and regulatory requirements for CSTs. • Legal and forensics capabilities are built. • Movement of evidence are tracked, and their integrity ensured.
	2-12-P-1-6	Real-time reporting to the CST of incidents that may affect CST; if the incident is discovered.
		Related Cybersecurity tools: • Template for Cybersecurity Incident and Threat Management Policy • Template for Cybersecurity Incident and Threat Management Standards • Cybersecurity Incident Response Guidelines • Template for Cybersecurity Incident Response Detailed Plan

		Guidelines: • Analyse identified incidents for their impact on CSTs (e.g. how CST is using the impacted service). • Report such incidents immediately to CSTs with sufficient information to analyse related risks and track Incident Response on CSP side.
		Expected deliverables: • Impact on CSTs is analysed for all identified incidents. • Incidents impacting CTSs are immediately reported to CTSs with sufficient information. • Sample of incidents reported to CST.
	2-12-P-1-7	Support for CSTs to handle security incidents according to the agreement between the CSP and CST.
		Related Cybersecurity tools: • Template for Cybersecurity Incident and Threat Management Policy • Template for Cybersecurity Incident and Threat Management Standards • Cybersecurity Incident Response Guidelines • Template for Cybersecurity Incident Response Detailed Plan **Guidelines:** • Align incident handling process across CSP and CST before serving services (e.g.: Incident Response systems integration) • Report immediately to CSTs incidents (that impact them) with sufficient information to analyse related risks and correlate incident response on the CST side.
		Expected deliverables: • Incident handling process agreed between CSP and CST and formally recognized in contract. • Process of reporting to CTSs incidents impacting them established.
	2-12-P-1-8	Measuring and monitoring cybersecurity incident metrics and monitor compliance with contracts and legislative requirements

TLP: White

Document Classification: Public

		Related Cybersecurity tools: • Template for Cybersecurity Incident and Threat Management Policy • Template for Cybersecurity Incident and Threat Management Standards • Cybersecurity Incident Response Guidelines • Template for Cybersecurity Incident Response Detailed Plan • Template for Key Performance Indicator (KPIs) report **Guidelines:** • Define contractual and legislative requirements for Cybersecurity Incident Management. • Establish cybersecurity incident (compliance and effectiveness) metrics in form of KPI, KCI (e.g.: Mean Time to Detect, Mean Time to Response, Mean Time to Contain). • Test the metrics. • Formally approve the metrics by authorized person. • Establish dashboards and compliance reports to report the metrics. • Periodically review the dashboards and compliance reports.
		Expected deliverables: • Contractual and legislative requirements register. • Formally approved and tested cybersecurity incident metrics (KPI, KCI). • Metrics dashboards and compliance reports. • Records form dashboards and compliance reports review. • Sample of dashboard and compliance report.
2-13	**Physical Security**	
Objective	To ensure the protection of CSPs' information and technology assets from unauthorized physical access, loss, theft and damage.	
Controls		
2-13-P-1	In addition to sub controls in the ECC control 2-14-3, the CSP shall cover the following additional sub controls for cybersecurity requirements for physical security, as a minimum:	
	2-13-P-1-1	Continuous monitoring of access to CSP's sites and buildings.

		Related Cybersecurity tools: • Template for Physical Security Cybersecurity Policy • Template for Physical Security Standards **Guidelines:** • Identify all access points/gates to sites and buildings. • Define attack vectors against access points (consider piggy backing, reusing of stolen access tokens, tampering access prevention systems). • Define requirements for CSP's sites and building access monitoring. • Define a process for effective access monitoring and access violation detection. • Implement technical systems for effective access monitoring. • Involve trained Analysts when professional judgement is required in the monitoring process. • Keep monitoring records - access logs and who and when reviewed these logs for no less than six (6) months. • Record the dates and times of visitor entries and departures and supervise all visitors unless their access has been previously approved. • Monitor ingress and egress points to service and delivery areas and other points where unauthorized personnel may enter the premises. • Monitor access by reviewing access logs, access attempts and access recordings.
		Expected deliverables: • Inventory of sites' and buildings' gates and access points. • Documentation of defined attack vectors, access monitoring requirements and access monitoring process (procedure or instructions). • Access logs and records. • Access logs and records reviews.
	2-13-P-1-2	Preventing unauthorized access to devices in the Cloud Technology Stack.

TLP: White

Document Classification: Public

		Related Cybersecurity tools: • Template for Physical Security Cybersecurity Policy • Template for Physical Security Standards **Guidelines:** • Build physical security isolated perimeter for the data storage and processing facilities areas, including gates, physical authentication mechanisms, access control points and monitoring equipment. • Place the Cloud Technology Stack devices in secure area the perimeter in dedicated server room with access limited to authorized personnel. • Secure devices in the Cloud Technology Stack using rack cabinet enclosures to prevent damage or inserting external devices (e.g. USB flash drives, portable SSD drives, etc.).
		Expected deliverables: • Closed physical perimeter for servers and data storage with access control points. • Devices locked in secure racks preventing from damage and external portable devices insertions.
	2-13-P-1-3	Disposal of cloud infrastructure hardware storage equipment (external or internal), by adopting relevant legislation and best practices.
		Related Cybersecurity tools: • Template for Physical Security Cybersecurity Policy • Template for Physical Security Standards **Guidelines:** • Identify legal regulations and best practices for hardware disposal. • Define roles and responsibilities in the disposal process. • Select hardware sanitization methods (e.g. cryptographic erase, media degaussing, media physical destruction: pulverizing, burning, melting, etc. or industrial shredding) adequate to hardware type ensuring that data stored on these devices will not be recoverable. • Record the hardware disposal process.
		Expected deliverables: • Legal regulations and best practices for hardware disposal gathered. • Formally approved cloud infrastructure hardware disposal policy. • Hardware disposal records and tracking system.

2-14	Web Application Security	
Objective	Ensure the protection of external web applications of the CSP from cyber risks.	
Controls		
2-14-P-1	In addition to subcontrols in the ECC control 2-15-3, the CSP shall cover the following additional subcontrols for cybersecurity requirements for web application security, as a minimum:	
	2-14-P-1-1	Protecting information involved in application service transactions against possible risks (e.g.: incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure….).
		Related Cybersecurity tools: • Template for Web Application Security Policy • Template for Web Application Security Standard **Guidelines:** • Identify possible risks related to information involved in application service transactions. • Determine security measures that can be applied to protect information involved in application service transactions against identified risks. • Implement defined security measures. • Periodically review and update (or add new if relevant) identified risks and implemented measures to ensure its applicability. • Configure web application firewalls to inspect traffic, apply rules, and perform behavioural monitoring. • Deny access from known malicious or/and bad reputation sources. • Apply Transport Layer Security (TLS, SSL) or other data transmission encryption and integration protection layer. • Review Periodically the application exposure to the Internet to detect unintentional data exposures. • Deny default or common passwords for applications. • Monitor routing tables for malicious/unintentional changes or service redirections. • Establish ongoing monitoring of transactions in as near to real-time manner.

TLP: White

Document Classification: Public

		Expected deliverables: • Web application firewalls appropriately configured. • Traffic inspection and behavioural monitoring established. • Access from known malicious or/and bad reputation sources denied. • Data transmission encryption and integration protection layer (TLS, SSL) applied. • Regular application exposure to the Internet review and unintentional data exposure detection set. • Default or common passwords for applications denied. • Identification of malicious/unintentional changes or service redirections in routing tables implemented. • Ongoing monitoring of transactions established.
2-15	**Key Management**	
Objective	Ensure secure management of CSPs' and CSTs' cryptographic keys to protect confidentiality, integrity and availability of information and technical assets.	
Controls		
2-15-P-1	Cybersecurity requirements for key management process within the CSP shall be identified, documented and approved.	
	Related Cybersecurity tools: • Template for Encryption Policy • Template for Encryption Key Management Standard **Guidelines:** • Identify cybersecurity requirements for Key Management aspects (e.g.: key exchange, storage, usage, ownership) - use questionnaires and conduct workshops with relevant stakeholders. • Define Key Management standard to address cybersecurity requirements. • Formally approve the standard. • Periodically review the standard (e.g.: at least annually)	
	Expected deliverables: • Key Management standard that is formally approved and Periodically reviewed. • Regular review reports.	
2-15-P-2	Cybersecurity requirements for key management process within the CSP shall be applied.	
	Guidelines:	

	• Enforce defined Key Management standard (e.g. Key Management service hardening, access control restriction, monitoring) • Control the effective implementation of the standard. • Report violations to the standard. • Document and manage exceptions.	
	Expected deliverables: • Cybersecurity requirements for key management process are implemented and followed as per defined policy and related documentations.	
2-15-P-3	In addition to the ECC sub control 2-8-3-2, cybersecurity requirements for key management within the CSP shall cover, at minimum, the following:	
	2-15-P-3-1	Ensure well-defined ownership for cryptographic keys.
		Related Cybersecurity tools: • Template for Encryption Policy **Guidelines:** • Define responsibilities that come with cryptographic keys ownership during entire key lifecycle (e.g.: create a key, authorize to use the key, dispose the key) • Assign ownership for cryptographic keys to CSP employees. • Review Periodically cryptographic keys for orphans (every key must have an assigned active owner) • Assign owners to new cryptographic keys as a mandatory step when creating keys.
		Expected deliverables: • Identified Cryptographic keys and owners
	2-15-P-3-2	A secure cryptographic key retrieval mechanism in case of cryptographic key lost (such as backup of keys and enforcement of trusted key storage, strictly external to cloud).
		Related Cybersecurity tools: • Template for Encryption Policy **Guidelines:** • Develop and test cryptographic key recovery plans for cryptographic key loss or damage (e.g. print cryptographic keys, put into tagged envelopes and store in physical safes in trusted and safe external locations like deposit boxes or secure containers in banks)

TLP: White

Document Classification: Public

		Expected deliverables: • Cryptographic key retrieval plan
	2-15-P-3-3	Activating and monitoring of all audit trails of keys.
		Related Cybersecurity tools: • Template for Encryption Policy **Guidelines:** • Log key management activities (e.g.: Creation date, renewal date, expiration date, decommissioning date, key and certificate details, when the key was accessed by users and for what purpose, any additional details required by legal or regulatory requirements). • Build a SIEM-class monitoring capability for these logs
		Expected deliverables: • Compare the list of active cloud services to the list of monitored cloud services. • Sample of SIEM reports/alerts/use cases.
2-15-P-4	Cybersecurity requirements for key management within the CSP shall be reviewed periodically.	
	Related Cybersecurity tools: • Template for Cybersecurity Reviewing and Auditing Policy • Template for the Lifecycle Management of Cybersecurity Policies, Procedures, and Standards, covering Development, Implementation, Assessment and Periodic Reviews **Guidelines:** • Review periodically cybersecurity requirements for key management, at least annually. • Maintain records of periodical reviews (e.g.: who and when reviewed and a change log).	
	Expected deliverables: • Cybersecurity requirements for Key Management reviewed Periodically. • Periodic review logs.	
2-16	**System Development Security**	
Objective	Ensure CSPs' systems are developed, integrated and deployed in a secure manner.	
Controls		
2-16-P-1	Cybersecurity requirements for system development within the CSP shall be identified, documented and approved.	

	Related Cybersecurity tools: • Template for Secure Software Development Lifecycle Policy **Guidelines:** • Identify cybersecurity requirements for system development using questionnaires and workshops with relevant stakeholders. • Document these requirements (Cybersecurity standard for System Development).	
	Expected deliverables: • Cybersecurity requirements for system development are formally approved and periodically reviewed.	
2-16-P-2	Cybersecurity requirements for system development within the CSP shall be applied.	
	Guidelines: • Enforce Cybersecurity standard for System Development. • Measure compliance with that standard. • Manage exceptions for this standard. • Escalate violations regarding this standard.	
	Expected deliverables: • Enforced cybersecurity requirements for system development. • Document outlining the implementation of the compliance measurement tool for standard implementation. • Documents for violation escalation procedures.	
2-16-P-3	Cybersecurity requirements for system development within the CSP shall include as a minimum the following controls along the development lifecycle:	
	2-16-P-3-1	Considering cybersecurity requirements of the Cloud Technology Stack and relevant systems in the design and implementation of the cloud computing services.
		Related Cybersecurity tools: • Template for Secure Software Development Lifecycle Policy **Guidelines:** • Identify cybersecurity requirements of the Cloud Technology Stack and relevant systems for cloud computing services. • Apply identified requirements both during design and implementation of the cloud computing services. • Periodically review the compliance with the requirements and monitor whether new applicable requirements occurred.

TLP: White

Document Classification: Public

		Expected deliverables: • Sample of compliance review. • Applied cybersecurity requirements.
	2-16-P-3-2	Protecting system development environments, testing environments (including data used in testing environment), and integration platforms.
		Related Cybersecurity tools: • Template for Secure Software Development Lifecycle Policy **Guidelines:** • Identify risks related to development environments, testing environments and integration platforms. • Develop and implement protection measures to provide secure development and testing environment, as well as secure integration platforms, taking account of identified risk • Ensure that protection of data used in testing environment is included in the implemented protection measures.
		Expected deliverables: • List of identified risks. • Evidence confirming the identification of preventive measures and ensuring the protection of data used in the testing environment.
2-16-P-4	Cybersecurity requirements for system development within the CSP shall be applied and reviewed periodically.	
	Related Cybersecurity tools: • Template for Cybersecurity Reviewing and Auditing Policy • Template for Developing Cybersecurity Documentation Procedures **Guidelines:** • Review requirements Periodically based on defined timeframes, at least annually. • Define Roles and Responsibilities in the review process. • Update requirements, if applicable. • Maintain records of periodical reviews (e.g.: who and when reviewed and a change log).	
	Expected deliverables: • Current cybersecurity requirements for system development. • Sample of periodical reviews.	
2-17	**Storage Media Security**	

Objective	Ensure CSPs' secure handling of information and data on physical media.	
Controls		
2-17-P-1	Cybersecurity requirements for usage of information and data media within the CSP shall be identified, documented and approved.	
	Guidelines: • Identify cybersecurity requirements for usage of information and media (e.g.: labelling, encryption, secure storage, secure disposal) - use questionnaires and conduct workshops with relevant stakeholders. • Define Information and Data Media Usage standard to document these requirements. • Formally approve the standard. • Periodically review the standard (e.g.: annually)	
	Expected deliverables: • Information and data media usage standard	
2-17-P-2	Cybersecurity requirements for usage of information and data media within the CSP shall be applied.	
	Guidelines: • Enforce Cybersecurity standard for Information and Data Media Usage (e.g.: access control, encryption)	
	Expected deliverables: • Information and data media labelled, securely stored and disposed.	
2-17-P-3	Cybersecurity requirements for usage of information and data media within the CSP shall cover, at minimum, the following:	
	2-17-P-3-1	Enforcement of sanitization of media, prior to disposal or reuse.
		Guidelines: • Define requirements for media sanitization to ensure that storage media is erased in a secure manner (e.g.: the process is irreversible). • Define media sanitization methods (e.g. overwrite storage media with random input data several times, destroy or overwrite encryption keys, degaussing) • Select sanitization tools that implement defined methods. • Enforce sanitization of media by making it a mandatory step in media reuse or disposal process (e.g.: build a proper process flow)

TLP: White

Document Classification: Public

		Expected deliverables: • Media sanitization tools in use.
	2-17-P-3-2	Using secure means when disposing of media.
		Guidelines: • Define requirements for secure disposal of media. • Identify methods for disposal that meet these requirements. • Apply accepted methods for the secure disposal of data from storage media. • Ensure that data is not recoverable using any means.
		Expected deliverables: • Defined requirements and acceptable methods for disposal of media.
	2-17-P-3-3	Provision to maintain confidentiality and integrity of data on removable media.
		Guidelines: • Identify risks related to confidentiality and integrity of data on removable media (e.g. media theft). • Define applicable controls and requirements for data confidentiality and integrity on removable media (e.g.: encryption, physical security). • Apply applicable security measures to ensure data confidentiality and integrity on removable media. • Periodically review and update the controls and requirements to ensure its applicability.
		Expected deliverables: • List of identified risks. • Defined controls and requirements for data on removable media. • Regular review reports.
	2-17-P-3-4	Human readable labelling of media, to explain its classification and the sensitivity of the information it contains.
		Guidelines: • Establish clear labelling rules of the media including its classification and the sensitivity of information (e.g. Top secret, Secret, Restricted) • Ensure that used classification and sensitivity levels are well-defined and communicated.

		• Ensure that each media in use is labelled according to the established rules. • Ensure that each new media to be used is labelled according to the established rules.
		Expected deliverables: • Established labelling rules. • Each media is labelled according to established rules.
	2-17-P-3-5	Controlled and physically secure storage of removable media.
		Guidelines: • Identify risks related to storage of removable media (e.g. media theft) • Define applicable controls (including physical controls) and requirements for secure storage of removable media, taking account of identified risks. • Apply these controls (e.g. access control, HVAC)
		Expected deliverables • List of identified risks for storing removable media. • Controls and requirements for secure storage of removable media.
	2-17-P-3-6	Restriction and control of usage of portable media inside the Cloud Technology Stack.
		Guidelines: • Identify risks related to usage of portable media inside the Cloud Technology Stack (e.g. media theft) • Define and approve adequate restrictions and controls of portable media inside the Cloud Technology Stack taking account of identified risks. • Implement the restrictions and controls (e.g. encryption, ownership, RFID tags).
		Expected deliverables: • List of identified risks for using external storage media on the Cloud Technology Stack. • Approved restrictions and controls for using external storage media on the Cloud Technology Stack.

TLP: White

Document Classification: Public

2-17-P-4	Cybersecurity requirements for usage of information and data media within the CSP shall be applied and reviewed periodically.
	Related Cybersecurity tools: • Template for Cybersecurity Reviewing and Auditing Policy • Template for Developing Cybersecurity Documentation Procedures **Guidelines:** • Review requirements Periodically based on defined timeframes, at least annually. • Define Roles and Responsibilities in the review process. • Update requirements, if applicable. • Maintain records of periodical reviews (e.g.: who and when reviewed and a change log).
	Expected deliverables: • Current cybersecurity requirements for usage of information and data media • Periodical review logs.

3 (Cybersecurity Resilience)

3-1	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	
Objective	To ensure the inclusion of the cybersecurity resiliency requirements within the CSPs' and CSTs' business continuity management and to remediate and minimize the impacts on systems, information processing facilities and critical e-services from disasters caused by cybersecurity incidents.	
Controls		
3-1-P-1	In addition to sub controls in the ECC control 3-1-3, the CSP shall cover the following additional sub controls for cybersecurity requirements for cybersecurity resilience aspects of business continuity management, as a minimum:	
	3-1-P-1-1	Developing and implementing disaster recovery and business continuity procedures in a secure manner.
		Related Cybersecurity tools: • Template for Cybersecurity Policy within Business Continuity **Guidelines:** • Define requirements for disaster recovery and business continuity procedures, taking account of identified risks related to cloud computing. • Develop, approve and implement disaster recovery and business continuity procedures/plans including security measures, taking account of defined requirements. • Clearly communicate and make the documents available for the relevant authorized personnel. • Test the procedures Periodically and upon significant changes to ensure its applicability.
		Expected deliverables: • Disaster Recovery Procedure/Plan for cloud computing. • Business Continuity Procedure/Plan for cloud computing.
	3-1-P-1-2	Developing and implementing procedures to ensure resilience and continuity of cybersecurity systems dedicated to the protection of Cloud Technology Stack.

TLP: White

Document Classification: Public

		Related Cybersecurity tools: • Template for Cybersecurity Policy within Business Continuity **Guidelines:** • Develop procedures to ensure resilience and continuity that are specific to cybersecurity of Cloud Technology Stack. • Review Periodically these procedures. • Make resilience and continuity mechanisms an Architectural Principle for cybersecurity. • Develop catalogue of resilience and continuity assurance techniques and methods.
		Expected deliverables: • Document outlining enhanced measures to ensure resilience and continuity of cybersecurity systems dedicated to protecting the Cloud Technology Stack. • Periodical review reports and documents. • Evidence illustrating techniques and methods ensuring resilience and continuity.

4 (Third-Party Cybersecurity)

4-1	Supply Chain and Third-Party Cybersecurity	
Objective	To ensure the protection of assets against the cybersecurity risks related to third-parties including outsourcing and managed services as per policies and procedures, and related laws and regulations.	
Controls		
4-1-P-1	In addition to implementing the ECC controls 4-1-2 and 4-1-3, the CSP shall cover the following additional sub controls for third-party cybersecurity requirements, as a minimum:	
	4-1-P-1-1	Ensure that the CSP fulfills NCA's requests to remove software or services, provided by third-party providers that may be considered a cybersecurity threat to national organizations, from the marketplace provided to CSTs.
		Related Cybersecurity tools: • Template for Cybersecurity Policy Regarding Third-Party **Guidelines:** • Maintain a catalogue of third-party providers and their software available to CSTs. • Establish a robust process to remove specific software from the marketplace based on NCA's requests. • Introduce appropriate legal statements allowing CSP to remove from the marketplace any software considered as cybersecurity threat.
		Expected deliverables: • Review the catalogue of third-party software providers and their software. • A document outlining procedures for removing specific programs from the market based on legislative requests.
	4-1-P-1-2	Requirement to provide security documentation for any equipment or services from suppliers and third-party providers.
		Related Cybersecurity tools: • Template for Cybersecurity Policy Regarding Third-Party **Guidelines:** • Introduce contractual obligations on suppliers and third-party providers to provide security documentation of their equipment, product or service.

TLP: White

Document Classification: Public

		• Define security aspects to be documented (e.g. security architecture, security controls in place, security technologies in use) • Intake and review Periodically provided documentation.
		Expected deliverables: • Security documentation for equipment or services from suppliers and third-party providers. • Periodical review reports and documents.
	4-1-P-1-3	Third party providers compliant with law and regulatory requirements relevant to their scope.
		Related Cybersecurity tools: • Template for Cybersecurity Policy Regarding Third-Party **Guidelines:** • Identify and document Periodically (e.g. annually) laws and regulatory requirements relevant to third party providers. • Audit third party providers or request independent audits to verify their compliance.
		Expected deliverables: • Relevant laws and regulatory requirements identified for each of third-party providers. • Proof of compliance with laws and regulatory requirements provided for each third-party provider.
	4-1-P-1-4	Risk management and security governance on third-party providers as part of general cybersecurity risk management and governance.
		Related Cybersecurity tools: • Template for Cybersecurity Policy Regarding Third-Party **Guidelines:** • Include third-party providers related risks (e.g. supply chain risk) into the cybersecurity risk management and governance processes.
		Expected deliverables: • Third party risks embedded into Risk Management processes. • Sample of risk register that includes third party identified risks.

الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority