الهيئـــة الوطنيـــة
للأمـــن السيبـــراني

National Cybersecurity Authority

Guide to Cloud Cybersecurity Controls – Cloud Service Tenants Implementation

(GCCC-CST – 1: 2023)

TLP: white
Document Classification: Public

Disclaimer: This Guide has been developed by the National Cybersecurity Authority to enable organizations to implement the Cloud Cybersecurity Controls (CCC–1:2022) for Cloud Service Tenants (CSTs). 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 Cloud Cybersecurity Controls implementation. The assessor or auditor has the right to request other evidences as deemed necessary to ensure that all Cloud Cybersecurity Controls are implemented.

In the Name of Allah,

The Most Gracious,

The Most Merciful

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

List of Figures

Introduction

This guideline defines the implementation guidance for implementing the cybersecurity controls stated in Cloud Cybersecurity Controls (CCC–1:2022) for Cloud Service Tenants (CSTs) developed by the National Cybersecurity Authority. This cybersecurity guideline follows international best practices to facilitate implementation of cybersecurity controls in the organization.

Objectives

The main objective of this implementation guideline is to facilitate implementation of the cybersecurity requirements in Cloud Cybersecurity Controls (CCC–1:2022) for Cloud Service Tenants (CSTs) for information and technology assets in organizations. This implementation guideline is based on industry leading practices which will help organizations ensure compliance with regulatory standards and therefore minimize the cybersecurity risks that originate from internal and external threats.

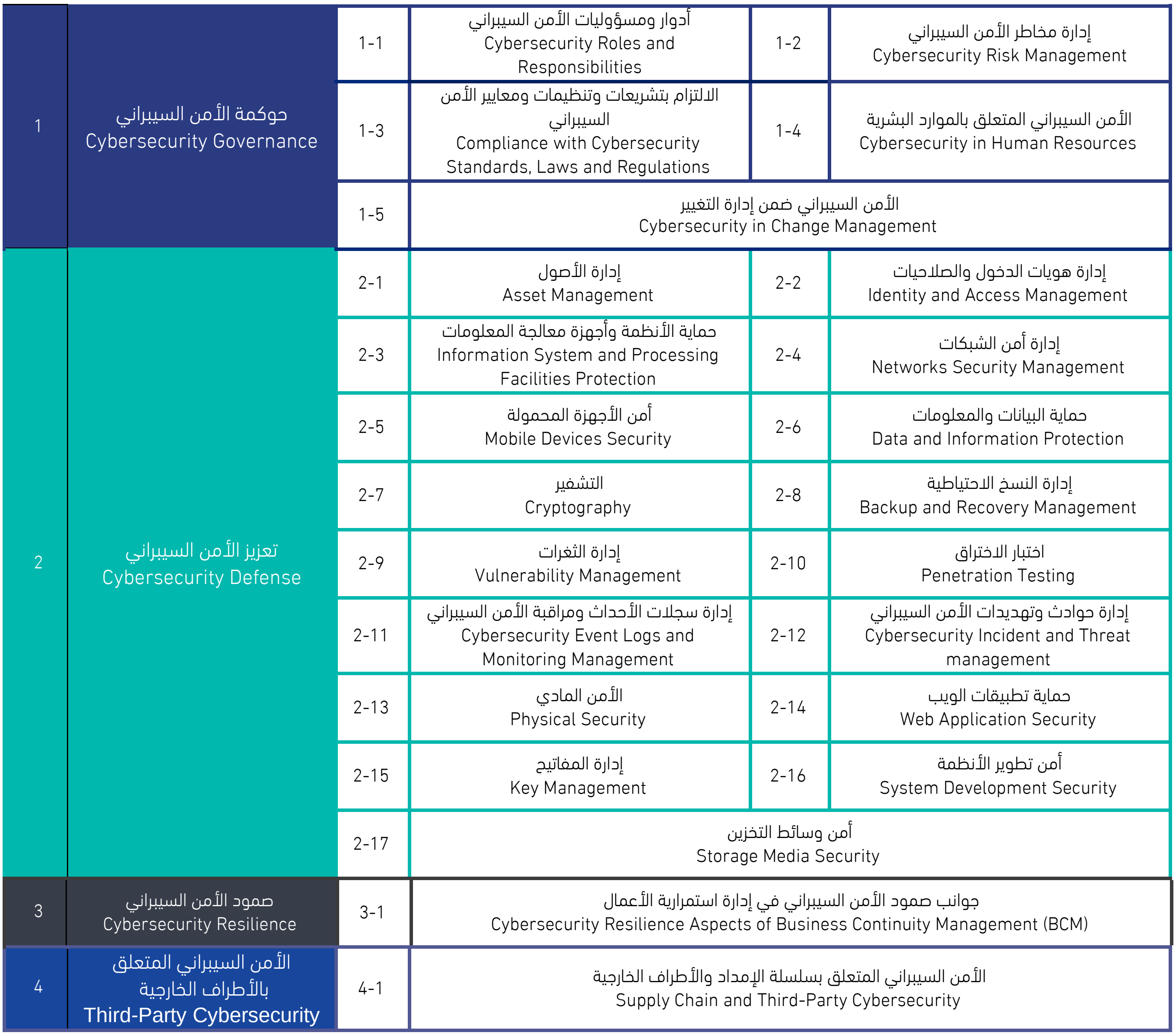
Scope of Work and Applicability

This guideline's scope of work is aligned with the scope of work of the Cloud Cybersecurity Controls (CCC–1:2022), which is:

- The CCC is applicable to both CPSs and CSTs, and these controls illustrates the minimum requirements of cybersecurity for cloud computing.
- CSPs within the scope of CCC are any CSP which provide cloud computing services to the CSTs within the scope of work.
- This implementation guideline is applicable to the CSTs within the scope of CCC and CSTs refers to any governmental organization within or outside the Kingdom of Saudi Arabia (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, which are all referred to herein as “The Organization”.
- The NCA strongly encourages all other organizations in the Kingdom to leverage this guideline to facilitate implementing controls and improve and enhance their cloud cybersecurity.

Cloud Cybersecurity Controls Domains and Structure

Figure 1 below shows the CCC domains and subdomains.

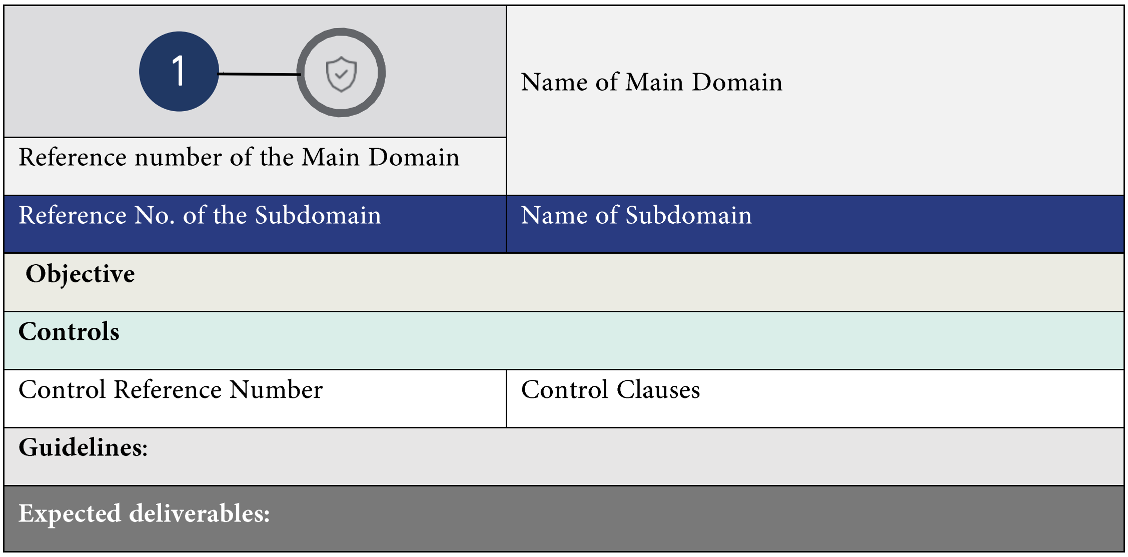


1	حوكمة الأمن السيبراني Cybersecurity Governance	1-1	أدوار ومسؤوليات الأمن السيبراني Cybersecurity Roles and Responsibilities	1-2	إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management
		1-3	الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني Compliance with Cybersecurity Standards, Laws and Regulations	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

Structure of the Guideline

Figure 2 below shows the methodological structure of the implementation guideline



1	Name of Main Domain
Reference number of the Main Domain	
Reference No. of the Subdomain	Name of Subdomain
Objective	
Controls	
Control Reference Number	Control Clauses
Guidelines:	
Expected deliverables:	

Figure 2: CCC Implementation Guideline Structure

CCC Implementation Guidance for Cloud Service Providers

General guidelines
● Identify the cloud computing services utilized 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 that are related to cloud services, 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 CSTs. ● Develop a plan to implement CCC for CSTs, and monitoring it continuously.

CCC Implementation Guideline for Cloud Service Tenants

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-T-1	In addition to the ECC control 1-4-1, the Authorizing Official shall also identify, document and approve:	
	1-1-T-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 **Guidelines:** ● Identify cloud services in use and related cybersecurity stakeholders both internal and external (e.g. CSPs and their Cybersecurity units, corporate Cloud Cybersecurity Architecture, Engineering, Operations teams, Cloud Security Managed Services representatives, Cloud Security SaaS representatives, Authorizing Office).
		Expected deliverables: ● Cloud Cybersecurity Roles and Responsibilities and RACI matrix defined and approved and documented 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-T-1	Cybersecurity risk management methodology mentioned in the ECC Subdomain 1-5 shall also include for the CST, as a minimum:	
	1-2-T-1-1	Defining acceptable risk levels for the cloud services.
		Related cybersecurity tools: ● Template for Cybersecurity Risk Management Policy **Guidelines:** In addition to the ECC control 1-5 implementation guidelines: ● Identify cloud services in use and analyse their business impact in a defined process (e.g.: Business Impact Analysis) to understand and assess (at least) service disruptions, data leaks and exposures, unauthenticated access risks and blast radius of damage one cloud issue may cause. ● Define risk levels for cloud services (e.g.: critical, high, medium, low) based on the organization's cybersecurity risk management methodology, and implementing necessary measures according to the risk level.
		Expected deliverables: ● Catalogue of cloud services with assigned acceptable risk level.
	1-2-T-1-2	Considering data and information classification accredited by CST in cybersecurity risk management methodology.
		Related cybersecurity tools: ● Template for Cybersecurity Risk Management Policy ● Templates for Cybersecurity Risk Management Processes **Guidelines:** ● Identify data processed/stored in the organization and classify it into agreed upon categories (e.g. public, restricted, secret, top secret) based on value to the organization, and include them in the cybersecurity risk management methodology.
		Expected deliverables: ● Cybersecurity Risk Management Methodology with unique approach to data classes.
	1-2-T-1-3	Developing cybersecurity risk register for cloud services, and monitoring it periodically according to the risks.

		Related cybersecurity tools: ● Template for Cybersecurity Risk Management Policy ● Template for Cybersecurity Risk Register **Guidelines:** ● Identify risks related to cloud services and CSPs – use Threat Intelligence feeds and Incident Response registries to analyse risk applicable to cloud services (e.g. data leakage due to misconfigured public cloud storage service or due to weak authentication) and periodically monitoring them according to nature and classification of the risk, ensuring they are addressed with appropriate priority.
		Expected deliverables: ● Cybersecurity Cloud Services Risk Register. ● Cybersecurity Cloud Services Risk Register review plan.
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-T-1	In addition to the ECC control 1-7-1, the CST legislative and regulatory compliance should include as a minimum with the following requirements:	
	1-3-T-1-1	Continuous or real-time compliance monitoring of the CSP with relevant cybersecurity legislation and contract clauses.
		Related cybersecurity tools: ● Template for Compliance with Laws and Regulations Policy ● Template for Reviewing and Auditing Policy ● Template for Audit Plan Record **Guidelines:** ● Identify national legislation and regulations related to cybersecurity of cloud services and Cloud Service Providers ● Review the contract with CSP regarding cybersecurity obligations. Define the way how to monitor/verify it regularly (e.g.: CSP's obligation to report to CSTs vulnerabilities can be verified with if these reports are delivered or justified) ● Request CSP's compliance reports (e.g.: by making it a contractual requirement)

		• Monitor CSP's compliance in a continuous manner (like daily or weekly verification) or in real-time (e.g. automated checks)
		Expected deliverables: • CSP's compliance reports verified periodically. • Reports or evidence demonstrating the monitoring of compliance within contracts.
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-T-1	In addition to sub controls in the ECC control 1-9-3, the following requirements should be covered prior the professional relationship of staff with the CST shall cover, at a minimum:	
	1-4-T-1-1	Screening or vetting candidates of personnel with access to Cloud Service sensitive functions (Key Management, Service Administration, Access Control).
		Related cybersecurity tools: • Template for Cybersecurity Human Resources Policy **Guidelines:** • Review job titles and descriptions for duties in areas of Key Management (including encryption), technical Cloud Service Management, Identity and Access Management) and make sure candidates for these jobs are under screening/vetting (e.g.: Cloud Access Provisioning Engineer, Cloud Service Administrator, Key Vault Security Engineer)
		Expected deliverables: • Catalogue of privileged user roles (including Key Management, Service Administration, Access control) • Screening/Vetting process defined for candidates that use these user roles.

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-T-1	In addition to controls in the ECC control 2-1, the CST shall cover the following additional controls for cybersecurity requirements for cybersecurity event logs and monitoring management, as a minimum:	
	2-1-T-1-1	Inventory of all cloud services and information and technology assets related to the cloud services.
		Related cybersecurity tools: ● Template for Asset Management Policy **Guidelines:** ● Identify cloud services in use (e.g.: via contract review, solution architecture review, active network connections monitoring) ● Identify data stored or processed in cloud (e.g. review cloud services for data flows and data storages) ● Identify cloud technology assets or group of assets (e.g. review cloud services for technical components in use). Consider fluent nature of IaaS components and auto scalability functions. ● Maintain Inventories of cloud services, data and technical assets (e.g. build a database of cloud services and data stored and/or processed and technical assets involved in these operations);
		Expected deliverables: ● Inventory of cloud services and related data and 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-T-1	In addition to sub controls in the ECC control 2-2-3, the CST shall cover the following additional sub controls for cybersecurity requirements for identity and access management requirements, as a minimum:	
	2-2-T-1-1	Identity and access management for all cloud credentials along their full lifecycle.
		Related Cybersecurity Tools: ● Template for Identity and Access Management Standards, encompassing password management ● Template for Identity and Access Management Policy **Guidelines:** In addition to sub controls in the ECC control 2-2-3 implementation guideline: ● Analyse and adapt the Identity and Access model relevant to cloud services (e.g.: RBAC, roles, service principals, policies, resources, resource groups, accounts, accounts groups) ● Manage accesses granularly ● Make use of Federated Authentication ● Enable strong/multifactor authentication
		Expected deliverables: ● Cloud Identity Lifecycle process defined
	2-2-T-1-2	Confidentiality of cloud user identification, cloud credential and cloud access rights information, including the requirement on users to keep them private (for employed, third party and CST personnel).
		Related Cybersecurity Tools: ● Template for Identity and Access Management Standards, encompassing password management ● Template for Identity and Access Management Policy **Guidelines:** ● Restrict Access to Identity Management and Access Management systems to the dedicated staff (e.g.: IAM Operations personnel) ● Make authentication technical methods encrypted (e.g.: TLS in place)
		Expected deliverables: ● Login screens only via encrypted channels (e.g. TLS)

	2-2-T-1-3	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 Configuration and Hardening Policy ● Template for Secure Configuration and Hardening Standard **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 5 minutes and timeout after 10 minutes of inactivity)
		Expected deliverables: ● Session management system with session lockouts and session timeouts configured.
	2-2-T-1-4	Multi-factor authentication for privileged cloud users.
		Related Cybersecurity Tools: ● Template for Identity and Access Management Standards, encompassing password management ● Template for Identity and Access Management Policy **Guidelines:** ● Define privileged cloud entitlements (e.g.: modifications in functions: Key Management, Identity and Access Management, Service Management/Administration) ● Define privileged roles and identities that use these privileged entitlements (e.g. Role of IAM Engineer for Artificial Intelligence Cloud Solutions) ● Build a mandatory multi-factor authentication (e.g. using software/mobile authenticator) policy and assign it to privileged users or groups of users.

		Expected deliverables: ● Multi-factor authentication policy assigned to privileged users or groups of users. ● List of privileged cloud users.
	2-2-T-1-5	Formal process to detect and prevent unauthorized access to cloud (such as a threshold of unsuccessful login attempts).
		Related Cybersecurity Tools: ● Template for Identity and Access Management Standards, encompassing password management ● Template for Identity and Access Management Policy **Guidelines:** In addition to sub controls in the ECC control 2-2-3 implementation guideline: ● 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 ● Prevent using the same account from various locations (e.g. impossible travel). ● Setting up alerts and notifications for unsuccessful login attempts and monitoring them as part of event monitoring activities. ● Restricting user access after exceeding the maximum number of unsuccessful login attempts.
		Expected deliverables: ● Impossible travel scenarios detected and prevented
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-T-1	In addition to sub controls in the ECC control 2-3-3, the CST shall cover the following additional sub controls for cybersecurity requirements for information system and processing facilities protection requirements, as a minimum:	

	2-3-T-1-1	Verifying that the CSP isolates the community cloud services provided to CSTs (government organizations and CNI organizations) from any other cloud computing provided to organizations outside the scope of work.
		Related Cybersecurity Tools: ● Template for Reviewing and Auditing Policy ● Template for Audit Plan Log ● Template for Server Security Standard **Guidelines:** ● Review CSP's independent audits and assurance for proves of effective isolation of community clouds from public and other community clouds (e.g.: review physical isolation controls, logical isolation controls, multi-tenancy).
		Expected deliverables: ● CSP's community cloud isolation verified by agreed upon means between the CST and CSP.
2-4	**Networks Security Management**	
Objective	To ensure the protection of CSP's and CST's network from cyber risks.	
Controls		
2-4-T-1	In addition to sub controls in the ECC control 2-5-3, the CST shall cover the following additional sub controls for cybersecurity requirements for networks security management requirements, as a minimum:	
	2-4-T-1-1	Protecting the connection channel with CSP.
		Related Cybersecurity Tools: ● Template for Network Security Policy ● Template for Network Security Standard **Guidelines:** ● Define security requirements for connectivity with CSPs in terms of confidentiality, integrity and availability of data transferred through these connections (e.g. encryption in transit, connection redundancy, fail-over connectivity, volumetric DDoS protection, channel/VPN authentication) ● Design and implement the network connection accordingly (e.g.: use two separate ISPs to two regions where CSP operates, use VPNs) ● Define Disaster Recovery Plan for cloud connectivity.

		Expected deliverables: ● Disaster Recovery Plan for CST to CSPs connections. ● A network diagram document illustrating the implementation of cybersecurity practices to protect network communication between CSTs and CSPs.
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-T-1	In addition to sub controls in the ECC control 2-6-3, the CST shall cover the following additional sub controls for cybersecurity requirements for mobile device security, as a minimum:	
	2-5-T-1-1	Data sanitation and secure disposal for end-user devices with access to the cloud services.
		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 with access to the cloud services (e.g.: mobile, desktop, laptop) ● Select effective data sanitation and disposal methods relevant to these technologies (e.g. device to wipe out using Mobile Device Management systems) ● Build processes and capabilities to securely sanitize these devices (e.g.: use MDM with desired device sanitation features).
		Expected deliverables: ● Approved and implemented data sanitation and device disposal tools and methods.
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-T-1	In addition to sub controls in the ECC control 2-7-3, the CST shall cover the following additional sub controls for cybersecurity requirements for protecting CST's data and information in cloud computing, as a minimum:	
	2-6-T-1-1	Exit Strategy to ensure means for secure disposal of data on termination or expiry of the contract with the CSP.
		Related Cybersecurity Tools: ● Template for Data Cybersecurity Policy ● Template for Data Cybersecurity Standard **Guidelines:** ● Analyse cloud technical capabilities to securely dispose data stored in cloud storage (e.g.: data encryption using CST managed key including that key disposal) ● Define Cloud Exit strategy including cryptographic key disposal to make CST's data encrypted in CSP's infrastructure after leaving.
		Expected deliverables: ● Cloud Exit Strategy documented. ● Evidence confirming the existence of a service provided by the CSP that allow the CST to securely dispose of data or, at the very least, within the contract between the CST and the CSP, grants the CST the ability to dispose of the data.
	2-6-T-1-2	Using secure means to export and transfer data and virtual infrastructure.
		Guidelines: ● Analyse portability of solutions deployed to CSPs (e.g.: dependency on CSP's native services, features, technologies) ● Ensure the formatting of data and export technical capabilities of data in cloud services (e.g.: usage of standardized data formats, protocols) ● Ensure the virtual assets and data can be transferred out securely (e.g.: through encrypted channels) on demand.

		Expected deliverables: ● Defined requirements and applied security measures relevant to export and transfer of data and virtual infrastructure.
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		
2-7-T-1	In addition to sub controls in the ECC control 2-8-3, the CST shall cover the following additional sub controls for cryptography, as a minimum:	
	2-7-T-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:** ● Develop a Cryptographic Standard aligned with National Cryptographic Standards (NCS-1:2020).
		Expected deliverables: ● Cryptographic standard document.
	2-7-T-1-2	Encryption of data and information transferred to or transferred out of the cloud according to the relevant law and regulatory requirements.
		Related Cybersecurity Tools: ● Template for Encryption Standard ● Template for Encryption Policy ● Template for Encryption Key Management Standard **Guidelines:** ● Identify law and regulations related to cloud data flows (e.g.: National Cryptographic Standards) and verify compliance with these regulations.

		Expected deliverables: ● Hybrid cloud connectivity encryption.
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-T-1	In addition to sub controls in the ECC control 2-10-3, the CST shall cover the following additional sub controls for cybersecurity requirements for vulnerability management requirements, as a minimum:	
	2-9-T-1-1	Assessing and remediating vulnerabilities cloud services and at least once every three months.
		Related Cybersecurity Tools: ● Template for Security Vulnerability Assessment Procedure ● Template for Vulnerability Management Policy ● Template for Vulnerability Management Standard ● Template for Vulnerability Log **Guidelines:** ● Define and implement the Threat and Vulnerability Management control policy that includes the intent, purpose, and governance of how a CST 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 (e.g. quarterly assessments), ○ Acceptable periods of remediation of threats and vulnerabilities - three months. ○ The vulnerability detection methods are in use (e.g. end-point threat detection agent) ○ 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: ● Document outlining the establishment and assurance of the implementation of a Vulnerability Management Policy encompassing cloud computing. ● Report assessing and addressing vulnerabilities related to cloud services at least once every three months.
	2-9-T-1-2	Management of CSP-notified vulnerabilities safeguards in place.

		Related Cybersecurity Tools: ● Template for Security Vulnerability Assessment Procedure ● Template for Vulnerability Management Policy ● Template for Vulnerability Management Standard ● Template for Vulnerability Log **Guidelines:** ● Define and implement a Threat and Vulnerability Management policy that includes the intent, purpose, and governance of how a CST must address threats and vulnerabilities for their respective scope under the Security Shared Responsibility Model. At a minimum, the policy should specify: ○ how a CST is notified about vulnerabilities detected by CSP ○ Assessment methods for these vulnerabilities ○ How remediating actions are tracked for timely and effective closure
		Expected deliverables: ● Document outlining the establishment and assurance of the implementation of a Vulnerability Management Policy encompassing cloud computing. ● Report on managing vulnerabilities notified to the CST by the CSP, including the remediation process.
2-11	**Cybersecurity Event Logs and Monitoring Management**	
Objective	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.	
Controls		
2-11-T-1	In addition to sub controls in the ECC control 2-12-3, the CST shall cover the following additional sub controls for cybersecurity requirements for cybersecurity event logs and monitoring management, as a minimum:	
	2-11-T-1-1	Activating and collecting of login event logs, and cybersecurity event logs on assets related to cloud services.

		Related Cybersecurity Tools: ● Template for Event Log Management and Cybersecurity Monitoring Policy ● Template for Event Log Management and Cybersecurity Monitoring Standard **Guidelines:** ● Enable logging of account authentication and other cybersecurity events in cloud services (e.g.: use cloud native logging service and related agents)
		Expected deliverables: ● Cloud Services cybersecurity event log
	2-9-T-1-2	Monitoring shall include all activated cybersecurity logs on the cloud services of the CST.
		Related Cybersecurity Tools: ● Template for Event Log Management and Cybersecurity Monitoring Policy ● Template for Event Log Management and Cybersecurity Monitoring Standard **Guidelines:** ● Define monitoring use-cases relevant to cloud services (e.g.: monitoring of modifications of user accesses) ● Collect cybersecurity logs relevant to defined monitoring use-cases across cloud services (e.g.: API calls relevant to user accesses modifications are captured) ● Monitor cloud service cybersecurity logs (e.g. use cloud native or on-prem SIEM class technologies to analyse logs do detect security incidents)
		Expected deliverables: ● Cybersecurity event logs monitored
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-T-1	Cybersecurity requirements for key management within the CST shall be identified, documented and approved.	
	Related Cybersecurity Tools: - Template for Cybersecurity Cloud Computing and Hosting - Template for Cybersecurity Documentation Development Procedure **Guidelines:** - Identify cybersecurity requirements for Key Management aspects (e.g.: key exchange, storage, usage, ownership) - use questionnaires and conduct workshops with relevant stakeholders. - Define, approve and regularly review (e.g. annually) the Key Management standard to define cybersecurity requirements.	
	Expected deliverables: - Key Management Cybersecurity requirements documented and formally approved. - Results of the periodic review.	
2-15-T-2	Cybersecurity requirements for key management within the CST shall 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 Encryption Key Management documented and formally approved. - Document outlining procedures for reporting standard violations.	
2-15-T-3	In addition to the ECC sub control 2-8-3-2, cybersecurity requirements for key management within the CST shall cover, at minimum, the following:	
	2-15-T-3-1	Ensure well-defined ownership for cryptographic keys.

		Related Cybersecurity Tools: ● Template for Encryption Key Management Standard **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 CST employees. ● Review regularly 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 ● Results of the periodic review
	2-15-T-3-2	A secure data retrieval mechanism in case of cryptographic encryption key lost (such as backup of keys and enforcement of trusted key storage, strictly external to cloud).
		Related Cybersecurity Tools: ● Template for Encryption Key Management Standard **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)
		Expected deliverables: ● Cryptographic key retrieval plan
2-15-T-4	Cybersecurity requirements for key management within the CST shall be applied and reviewed periodically.	
	Related Cybersecurity Tools: ● 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 regularly.

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-T-1	In addition to sub controls in the ECC control 3-1-3, the CST shall cover the following additional sub controls for cybersecurity requirements for cybersecurity resilience aspects of business continuity management, as a minimum:	
	3-1-T-1-1	Developing and implementing disaster recovery and business continuity procedures related to cloud computing, 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 (e.g. data leakage or unintentional exposure) ● Develop, approve and implement disaster recovery and business continuity procedures/plans for cloud computing based on requirements. ● Test the procedures regularly and upon significant changes to ensure its applicability.
		Expected deliverables: ● Disaster Recovery Procedure/Plan for cloud computing. ● Business Continuity Procedure/Plan for cloud computing.

الهيئـــة الوطنيـــة
للأمـــن السيبـــراني

National Cybersecurity Authority