

Cybersecurity Regulatory Framework (CRF) for the ICT Sector

Version: 1.0

Date: 29/05/2019

Classification: Public

CONTENT

1. Introduction	3
2. Purpose	3
3. Scope	3
4. Applicability	4
5. Roles and Responsibilities.....	4
6. Glossary.....	5
7. Regulatory Framework.....	8
1. Governance.....	8
2. Asset Management	8
3. Cybersecurity Risk Management.....	9
4. Logical Security.....	9
5. Physical Security	10
6. Third Party Security	10
Annex	10
1. Compliance Level.....	10
2. Structure of the controls	11
3. Documentation of Requirements	14
4. Control Domains	15
1. Governance.....	15
2. Asset Management	22
3. Cybersecurity Risk Management.....	26
4. Logical Security.....	29
5. Physical Security	45
6. Third Party Security	49
REFERENCES	52

1. Introduction

Pursuant to the provisions in the Telecommunications Act (Act) and the Telecommunications Bylaw (Bylaw) related to safeguarding the public interest and user interest as well as maintaining the security of telecommunications information, and following the vision of the Kingdom of Saudi Arabia 2030, CITC decided to establish a comprehensive Cybersecurity Regulatory Framework (CRF) with the objective to increase the cybersecurity maturity of the Information and Telecommunications sector (ICT).

One of the main pillars of economic growth is the ICT sector providing the fundamental competitiveness of the national economy through high-speed broadband, online services, and information assets. With rising expectations towards continuous availability of services, immaculate user experience and effective protection of sensitive data, the strengthening of Saudi Arabia's cybersecurity becomes crucial to increase the digital nation's trust in safe and resilient ICT infrastructure and services.

2. Purpose

The CRF provides requirements for better management of cybersecurity risks through a consistent approach and in line with international best practices and local cybersecurity regulations. The purpose of the CRF is:

- To regulate and empower the cybersecurity practices of the ICT sector.
- To increase the overall cybersecurity maturity level of the ICT sector.
- To define a comprehensive set of cybersecurity requirements that shall be implemented based on a risk-oriented approach.
- To encourage the ICT sector to apply good practices for establishing the appropriate cybersecurity measures.
- To ensure confidentiality, integrity, and availability of the services provided to the customers.

3. Scope

This CRF provides a comprehensive set of cybersecurity requirements that must be implemented by the LSPs to fulfill the minimum security requirements.

Without prejudice to the provisions of CITC regulations and other related regulations, the provisions of this Framework shall apply to licensed service providers. It is important to understand that this framework is not intended to overwrite, and should not be perceived as a replacement of any of the issued regulatory frameworks.

4. Applicability

This framework is applicable to all the LSPs and their subsidiaries, staff, third parties and customers. Each LSP is required to comply with all applicable requirements through developing their own way of achieving the cybersecurity objectives.

Because the requirements were chosen to be comprehensive, some requirements might not be applicable for every LSP. For example if an LSP does not develop software, then compliance with the secure software development (Category ID: 4.14) requirements will not be required in this case. The control will remain applicable in case software is developed via a third party.

5. Roles and Responsibilities

Responsibilities of CITC include:

1. Monitor and steer the LSPs compliance with the defined requirements through various ways, for example inspections of LSPs facilities, compliance workshops, active and reactive audits.
2. Periodically review and update the CRF.
3. Define compliance requirements and setting target dates to ensure LSPs compliance with the CRF.

Responsibilities of the LSPs include:

1. Adopt and implement CRF in accordance with the defined compliance requirements.
2. Provide compliance reporting through for example self-assessments or other different means upon request from CITC.
3. Provide information and documentation to CITC when requested in addition to the defined reporting in the CRF.

6. Glossary

The words and expressions defined in CITC Statutes shall have the same meaning when used in this document. The following words and expressions shall have the meaning assigned to them below, unless the context says otherwise:

Access Control	The process of granting or denying specific requests for obtaining and using information and related information processing services and to enter specific physical facilities.
Advanced Persistent Threats	Advanced Persistent Threats is a stealthy computer network attack in which a person or group gains unauthorized access to a network and remains undetected for an extended period.
Baseline Configuration	A documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.
BYOD	Bring your own device (BYOD) refers to personally owned devices (laptops, tablets, and smart phones) that employees and contractors are permitted to use to carry out business functions.
Cloud Computing	Usage of scalable and elastic pool of shareable physical or virtual resources (such as servers, operating systems, networks, software, applications, and storage equipment) with self-service provisioning and administration on-demand.
Critical Systems	Any systems in which breakdown, unauthorized changes of their operations, and unauthorized access to their information lead to highly affect the availability of the services, organization's operations, economic or financial or social effects at the national level.
Cryptography	Cryptography is the bases that contains principles, means, and methods of storing and transmitting data or information in certain forms to hide its semantic contents and to prevent unauthorized use or not-detected modification so that only the persons concerned can read and process such information and data.
Cyber Threats	Intentional exploitation of computer systems, networks and the entities whose work depend on information technology and digital communication with the aim of causing harm.
Cybersecurity	Protection of networks, systems, operations, and their components of hardware and software, provided services, and contained data from any unauthorized access or disruption or misuse. The Cybersecurity concept includes information security and digital security.
Cybersecurity Incidents	A breach of a system's security policy in order to affect its integrity or availability and/or the unauthorized access or attempted access to a system or systems.
Cybersecurity Risk	An unwanted event or exposure with potentially negative

	consequences.
Disaster recovery (DR)	Disaster Recovery planning means putting in place procedures to be undertaken to restore normalcy of operations in the aftermath of disasters. This includes identifying the recovery strategies for all critical business functions, establishing recovery management organization and process, and creating recovery plans for various levels of business functions.
Environmental Threats	Human behavior that impacts the environment or the secondary impact of a natural disaster, which could cause an interruption in business functions for some predetermined period of time or the compromise of security controls.
ICT-specific	Information and communication technology (ICT) is an extended term for information technology (IT) which stresses the role of unified communications and the integration of telecommunications infrastructure (telephone lines, cable networks, wireless signals), computers and software.
Information Assets	The collection of systems, tools, data and information that enables the organization to perform its business functions thereby satisfying a recognized organization requirement.
ITU	International Telecommunications Union.
LSP	The Licensed Service Providers are all service providers that have requested and own license from CITC to provide the services, as specified in the respective licenses.
Malicious Activities	Activities that inflicts systems in a hidden manner to compromise the confidentiality, safety, accuracy or availability of data, applications or operation systems.
Outsourcing Services	Obtaining commodities and services through contracting with supplier or service provider.
Personally identifiable information (PII)	Information which can be used to distinguish or trace the identity of an individual (e.g., name, biometric records) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g. date and place of birth).
Physical Damage	Harm or injury to a person, property, or system resulting in impairment or loss of function, usefulness, or value.
Resilience	The entity's overall resilience capacity against cyber incidents, harm causers and recovery therefrom.
SMishing	The fraudulent practice of sending text messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords or credit card numbers.
Physical security	Security measures designed to prevent unauthorized access to the facilities, equipment, and resources of the organization and to protect individuals and properties from damage (such as espionage, theft, or terrorist attacks).
Logical security	Security measures designed to protect the systems and networks of the organization from all cyber threats and harmful activities.

Third party	Any organization acting as a party in a contractual relationship to provide goods or services.
--------------------	--

7. Regulatory Framework

The CRF defines the following regulatory statements LSPs shall comply to. Detailed requirements pertaining to each regulatory statement can be found in the Annex.

1. Governance

The LSPs shall:

- 1.1. Define a cybersecurity strategy and develop an implementation roadmap to achieve the defined objectives of the strategy.
- 1.2. Define and implement the relevant cybersecurity organization that will be responsible for the cybersecurity activities within the organization.
- 1.3. Ensure their compliance with internal and relevant external (national, international) regulatory requirements.
- 1.4. Periodically conduct independent cybersecurity audits covering the internal and external compliance requirements to measure the compliance level of the organization.
- 1.5. Conduct periodically cybersecurity awareness & trainings to ensure their personnel has the necessary qualifications and skills to carry out their responsibilities.
- 1.6. Provide their customers with relevant cybersecurity information related to the provided service to improve the cybersecurity awareness.
- 1.7. Ensure organizational-defined requirements for cybersecurity are included in the applied project management methodology.
- 1.8. Ensure cybersecurity requirements related to human resources are addressed in case of any changes of their working relationship.

2. Asset Management

The LSPs shall:

- 2.1. Maintain an up-to-date asset inventory of all the information assets that includes all relevant details to facilitate efficient protection of the information assets.
- 2.2. Classify the information assets to ensure a risk-based protection of the information assets.
- 2.3. Manage the use of personnel devices for business purposes to protect the organization from the risks imposed by such devices.
- 2.4. Define and enforce the acceptable use policy to protect the organization from the risks imposed by the inappropriate use of information assets.
- 2.5. Maintain information assets and recover them in case of a cybersecurity incident to ensure their continued availability and integrity.
- 2.6. Ensure secure disposal of information assets in order to prevent

unauthorized disclosure or modification of information stored on the disposed assets.

3. Cybersecurity Risk Management

The LSPs shall:

- 3.1.** Establish and implement an appropriate cybersecurity risk assessment approach to identify, analyze, and evaluate the risks to protect the information assets.
- 3.2.** Establish and implement an appropriate cybersecurity risk treatment and monitoring approach to manage the identified risks and monitor the treatment plans.

4. Logical Security

The LSPs shall:

- 4.1.** Ensure effective and adequate use of cryptography to provide confidentiality, integrity, authentication and non-repudiation of information in transit, at rest and in use.
- 4.2.** Manage the changes to the information assets to prevent unauthorized and accidental modifications.
- 4.3.** Identify the vulnerabilities of the information assets to prioritize and recommend the remediation action.
- 4.4.** Ensure security patches are applied to the information assets in an appropriate timeframe to fix known issues and enhance their resilience.
- 4.5.** Protect the networks operated by the organization from malicious activities and ensure the networks resilience against cyber threats.
- 4.6.** Monitor and protect the event logs of the information assets and report any suspicious activities that need further investigation.
- 4.7.** Manage the access rights and implement appropriate authentication mechanisms to prevent unauthorized access to information assets.
- 4.8.** Create and enforce a list of software applications that are authorized to be installed and used within the organization.
- 4.9.** Detect and respond to cybersecurity incidents to contain and minimize the impact of the incidents.
- 4.10.** Detect malware and prevent its spread in the organization.
- 4.11.** Classify the organization's information to ensure their adequate protection.
- 4.12.** Take the necessary measures including backup to ensure information recovery after an incident.
- 4.13.** Implement baseline configuration settings to increase the resilience of the information assets.
- 4.14.** Implement a secure software development lifecycle.
- 4.15.** Protect email and web browsers against cybersecurity threats.

4.16. Conduct penetration tests to evaluate the organization's defense capabilities and detect vulnerabilities.

5. Physical Security

The LSPs shall:

- 5.1.** Protect information assets against physical damage and threats.
- 5.2.** Manage physical access to the facilities that host the information assets to prevent unauthorized access.
- 5.3.** Protect information assets from environmental threats.
- 5.4.** Protect information assets residing outside the organization's premises against physical and environmental threats.

6. Third Party Security

The LSPs shall:

- 6.1.** Ensure cybersecurity requirements are contracted and applied by their cloud service provider.
- 6.2.** Ensure cybersecurity requirements are contracted and applied by third parties providing outsourcing services to the organization.

Annex

1. Compliance Level

CITC will set a security target by defining three compliance levels following a risk based approach. Each level comprises of a set of cybersecurity controls. The three levels vary in the complexity of the controls.

Level 1 includes the basic security controls.

Level 2 includes advanced requirements in addition the existing requirements within Level 1.

Level 3 includes requirements that are focusing on efficiency monitoring and continuous improvement to the controls in Levels 1 and 2.

In order to achieve compliance with a higher level, compliance with all preceding levels is required.

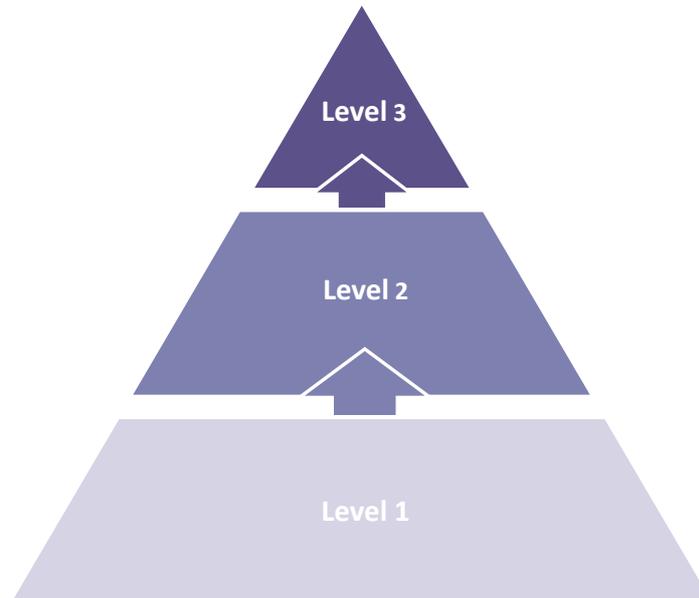


Figure 1 - Compliance Levels

The criticality of the LSP defines the target compliance level and date, which will be officially communicated by CITC (via e.g. memos, website).

2. Structure of the controls

The CRF controls are grouped into six domains:



Figure 2 - CRF Domains

Each domain is broken down into more specific categories that group cybersecurity controls relevant to the specific topic and share the same objective.

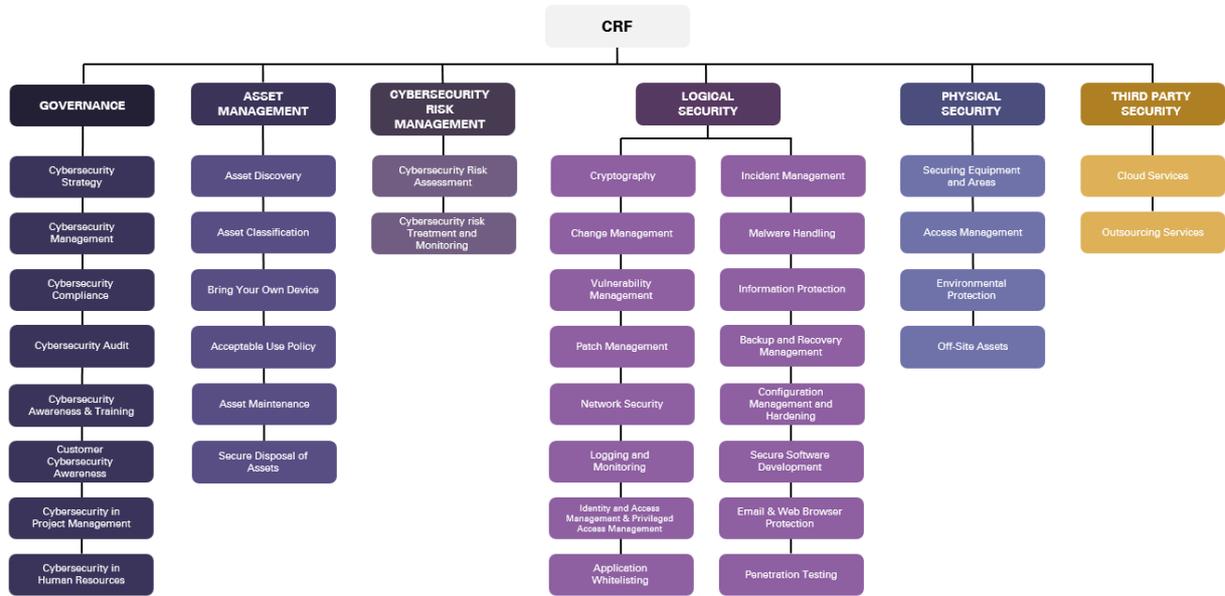


Figure 3 - CRF Domains and Categories

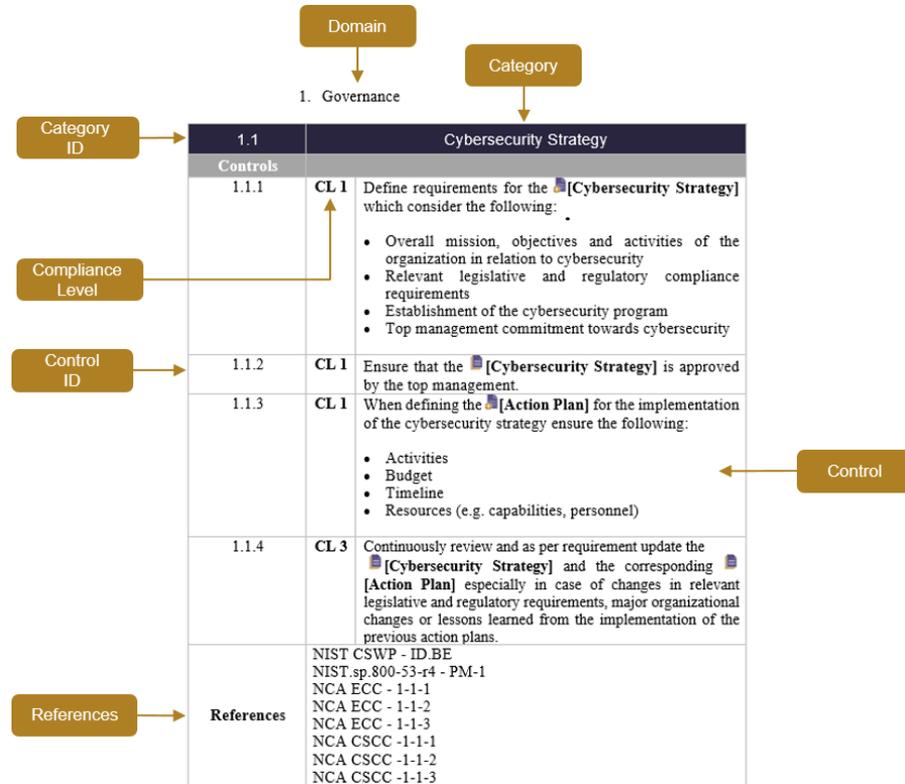


Figure 4 - CRF Structure

Important notes

Particular control information such as [processes], [outcomes], and [references] (e.g. to other controls, categories, processes, CITC documents) are individually highlighted throughout the framework. Where applicable, [ICT-specific] control considerations are highlighted as well.

The controls within the CRF are interconnected, for example an outcome from a control in one category could be an input to another control within a different category (e.g. the [Vulnerabilities Report] generated in the Vulnerability Management category acts as an input to the Patch Management category).

The highlighted processes and outcomes cover most but not necessarily all cybersecurity measures. They just emphasize expected implementations of processes and outcomes to improve the usability and clarity of the CRF controls.

The symbols used in the CRF are listed below:

CRF Symbol Legend

	New Outcome
	Outcome
	New Process
	Process
	Reference
	ICT-specific

3. Documentation of Requirements

In almost all CRF categories, documenting the requirements will be the first step of the implementation by the LSP. The CRF does not prescribe a standard format for the documentation of the requirements mentioned in each of the categories. These requirements can be defined in form of directives, rules, standards or policy documents. However, the requirements document – regardless of its name – must at least include the following:

- Unique document title
- Document version number and date
- Document change tracker
- Document owner responsible for changes
- The requirements document must be officially approved by the authorized personnel/committee within the organization
- The requirements documents must be appropriately disseminated and communicated to all relevant stakeholders within the organization
- Roles and responsibilities for the definition and the approval of the requirements of the category.

Documents that do not fulfil the above requirements will not be qualified to be compliant with the control requirements.

4. Control Domains

1. Governance

1.1	Cybersecurity Strategy	
Controls		
1.1.1	CL 1	<p>Define requirements for the [Cybersecurity Strategy] which consider the following:</p> <ul style="list-style-type: none"> • Overall mission, objectives and activities of the organization in relation to cybersecurity • Relevant legislative and regulatory compliance requirements • Establishment of the cybersecurity program • Top management commitment towards cybersecurity
1.1.2	CL 1	<p>Ensure that the [Cybersecurity Strategy] is approved by the top management.</p>
1.1.3	CL 1	<p>When defining the [Action Plan] for the implementation of the cybersecurity strategy ensure the following:</p> <ul style="list-style-type: none"> • Activities • Budget • Timeline • Resources (e.g. capabilities, personnel)
1.1.4	CL 3	<p>Continuously review and as per requirement update the [Cybersecurity Strategy] and the corresponding [Action Plan] especially in case of changes in relevant legislative and regulatory requirements, major organizational changes or lessons learned from the implementation of the previous action plans.</p>
References	<p>NIST CSWP - ID.BE NIST.sp.800-53-r4 - PM-1 NCA ECC - 1-1-1 NCA ECC - 1-1-2 NCA ECC - 1-1-3 NCA CSCC -1-1-1 NCA CSCC -1-1-2 NCA CSCC -1-1-3</p>	
1.2	Cybersecurity Management	
Controls		

1.2.1	CL 1	Define requirements for the [Cybersecurity Organization] which consider the following: <ul style="list-style-type: none"> • A cybersecurity committee and allocating members who represent different areas within the organization • The needed cybersecurity functions/departments required to implement the [Action Plan] • Allocating roles and responsibilities ensuring that the conflicting duties and areas of responsibilities are clearly segregated
1.2.2	CL 1	Implement the defined [Cybersecurity Organization].
1.2.3	CL 1	Implement the [Action Plan] through the defined [Cybersecurity Organization].
1.2.4	CL 1	Oversee the implementation of the [Action Plan] by the cybersecurity committee by monitoring, dealing with conflicts, and enforcing necessary measures for improvement.
References		ISO 27001 - 5 ISO 27002 - 6.1.1 ISO 27002 - 6.1.2 NCA ECC - 1-2-1 NCA ECC - 1-2-2 NCA ECC - 1-2-3
1.3	Cybersecurity Compliance	
Controls		
1.3.1	CL 1	Define [Requirements for Cybersecurity Compliance] which consider the following: <ul style="list-style-type: none"> • National legislative and regulatory requirements related to cybersecurity • Locally accredited international/cross-border requirements (e.g. included in internationally agreements or commitments) • Organization's internal requirements
1.3.2	CL 1	Define the {Compliance Process} to ensure compliance requirements are identified periodically, documented and communicated (e.g. when new regulatory requirements become effective, necessity to update the organization's cybersecurity requirements).
1.3.3	CL 1	Ensure the compliance requirements are incorporated within the organization.
1.3.4	CL 2	Automate the compliance activities through the use of dedicated tools (e.g. GRC tool).
1.3.5	CL 3	Continuously review and optimize the [Requirements for

		Cybersecurity Compliance] as well as the effectiveness of the process to ensure compliance.
References		ISO 27002 - 18.1 NCA ECC - 1-7-1 NCA ECC - 1-7-2
1.4	Cybersecurity Audit	
Controls		
1.4.1	CL 2	Define 📄[Requirements for Cybersecurity Audit] which consider the following: <ul style="list-style-type: none"> • Conducting periodical audits (e.g. conduct audits at least once a year for critical systems) • Protection and retention of 📄[Audit Records] • Reporting to top management
1.4.2	CL 2	Define and conduct ⚙️{ Internal Audit } process to verify the compliance with the identified 📄[Requirements for Cybersecurity Compliance].
1.4.3	CL 2	Document the findings and recommendations and present them to the top management.
1.4.4	CL 2	Protect the 📄[Audit Records] from unauthorized access, modification, and destruction.
1.4.5	CL 2	Ensure that the audit records are retained as proof for e.g. compliance to legislative and regulatory requirements.
1.4.6	CL 3	Continuously review and optimize the 📄[Requirements for Cybersecurity Audit] as well as the effectiveness of the process to conduct audit and review activities.
References		ISO 27002 - 18.2 ISO 27002 - 18.1.3 NIST.sp.800-53r4 - AU-6 NIST.sp.800-53r4 - AU-9 NIST.sp.800-53r4 - AU-11 NCA ECC - 1-8 NCA CSCC - 1-4
1.5	Cybersecurity Awareness & Training	
Controls		
1.5.1	CL 1	Define 📄[Requirements for Cybersecurity Awareness & Training] which consider the following: <ul style="list-style-type: none"> • Goals and scope • Number and frequency of trainings/year • Allocated resources
1.5.2	CL 1	Define and conduct a 📄[Cybersecurity Awareness &

		<p>Training Program] (e.g. defining goals, scope, targeted audience, validation criteria) that includes various cybersecurity topics considering the following:</p> <ul style="list-style-type: none"> • Cybersecurity roles and responsibilities of the targeted audience • Trending cybersecurity events and threats (e.g. social engineering attacks such as phone scams and impersonation calls) • Advice to personnel not to attempt unauthorized activities (e.g. introduce or use unauthorized equipment or software on a system, relocate equipment without proper authorization). • Secure handling of portable devices and storage media, email services (especially spam and phishing emails), internet surfing services and social media
1.5.3	CL 2	Enhance and implement the  [Requirements for Cybersecurity Awareness & Training] to carry out periodic validation tests to evaluate the effectiveness of the conducted awareness and training program and record the results of evaluation (e.g. check whether the personnel will click on a suspicious link in an email).
1.5.4	CL 2	Enhance and implement the  [Requirements for Cybersecurity Awareness & Training] to define the circumstances under which the  [Cybersecurity Awareness & Training Program] have to be provided (e.g. initial cybersecurity training to new users, training upon changes to information systems or job roles).
1.5.5	CL 2	Tailor the  [Cybersecurity Awareness & Training Program] to provide specialized or security-related skills and training to targeted group of people considering the following personnel: <ul style="list-style-type: none"> • Cybersecurity department personnel • Personnel working in the software development • Personnel involved in cybersecurity risk management department • Personnel with privileged access to critical information assets • Executive personnel
1.5.6	CL 3	Continuously review and optimize the  [Requirements for Cybersecurity Awareness & Training] as well as the  [Cybersecurity Awareness & Training Program] .

References	ISO 27002 - 7.2.2 SANS v6.1 - 17.4 NIST.sp.800-53r4 - AT-2 NCA ECC - 1-9-4 NCA ECC - 1-10-1 NCA ECC - 1-10-2 NCA ECC - 1-10-3 NCA ECC - 1-10-4 NCA ECC - 1-10-5
1.6	Customer Cybersecurity Awareness
Controls	
1.6.1	<p>CL 1 Define [Requirements for Customer Cybersecurity Awareness] which consider the following:</p> <ul style="list-style-type: none"> • Goals and scope • Number and frequency of trainings/year • Allocated resources
1.6.2	<p>CL 1 Define and conduct a [Customer Cybersecurity Awareness Program] by e.g. defining goals, scope, targeted customer group, delivery channel which should consider the following:</p> <ul style="list-style-type: none"> • Information on relevant emerging cybersecurity events and threats (e.g. social engineering attacks such as phone scams and impersonation calls) • Specific recommendations related to the provisioned service (e.g. how to be secure online, SMishing, and secure your mobile device)
1.6.3	<p>CL 2 Enhance and implement the [Requirements for Customer Cybersecurity Awareness] to periodically conduct the [Customer Cybersecurity Awareness Program] for the organization's customers.</p>
1.6.4	<p>CL 3 Continuously review and optimize the [Requirements for Customer Cybersecurity Awareness] as well as the [Customer Cybersecurity Awareness Program].</p>
References	ISO 27002 - 7.2.2 NCA ECC - 1-10-3
1.7	Cybersecurity in Project Management
Controls	
1.7.1	<p>CL 1 Define [Requirements for Cybersecurity in Project Management] which consider the following:</p>

		<ul style="list-style-type: none"> Defining integration of cybersecurity in project management (e.g. cybersecurity personnel as part of the project team) Defining project objectives to ensure that the cybersecurity is included in all phases of the project
1.7.2	CL 1	Perform a risk assessment at the beginning and during the course of each project in accordance with the  [Requirements for Risk Assessment] to identify the cybersecurity risks if any and define the mitigation plans.
1.7.3	CL 2	Track the identified cybersecurity risks and monitor the implementation of the mitigation plans during the course of the project.  [Cybersecurity Risk Treatment and Monitoring] .
1.7.4	CL 3	Continuously review and optimize the  [Requirements for Cybersecurity in Project Management] .
References		ISO 27002 - 6-1-5 NCA ECC - 1-6-1 NCA ECC - 1-6-2 NCA ECC - 1-6-3 NCA ECC - 1-6-4
1.8	Cybersecurity in Human Resources	
Controls		
1.8.1	CL 1	<p>Define  [Requirements for Cybersecurity in Human Resources] which consider the following:</p> <ul style="list-style-type: none"> Defining cybersecurity requirements related to personnel in the organization including contractors before they are employed, during their work, and upon completion/termination of their work Conduct background verification checks on all candidates for employment Hiring highly professional personnel on the jobs related to critical systems Ensuring that the terms and agreements related to the employment also cover the code of conduct (e.g. non-disclosure agreements, cybersecurity responsibilities) and has been included during and after termination of employment with the organization Ensuring that the code of conduct is signed by all the personnel Enforcing the   [Acceptable Use of Information Assets]
1.8.2	CL 1	Ensure that necessary actions (e.g. modify access

		authorizations in accordance with the new operational role) are performed when individuals are reassigned or transferred to other positions within the organization.
1.8.3	CL 1	Enforce disciplinary actions against personnel that do not comply with the organization's cybersecurity requirements.
1.8.4	CL 1	Ensure necessary actions (e.g. revoking employee access rights and privileges, retrieving assigned information assets, retaining access to information assets formerly controlled by terminated individual) have been carried out upon completion/termination of an employees' professional service in the organization.
1.8.5	CL 3	Continuously review and optimize the  [Requirements for Cybersecurity in Human Resources] as well as the effectiveness of the involved processes.
References		<p>ISO 27002 - 7.1.1 ISO 27002 - 7.1.2 ISO 27002 - 7.2.3 ISO 27002 - 7.3.1 ISO 27002 - 8.1.4 NIST.sp.800-53r4 - PS-4 NIST.sp.800-53r4 - PS-5 NCA ECC - 1-9-1 NCA ECC - 1-9-2 NCA ECC - 1-9-3 NCA ECC 1-9-4 NCA ECC - 1-9-5 NCA ECC - 1-9-6 NCA CSCC -1-9-3 NCA CSCC - 1-5-1</p>

2. Asset Management

2.1		Asset Discovery
Controls		
2.1.1	CL 1	<p>Define [Requirements for Asset Discovery] which consider the following:</p> <ul style="list-style-type: none"> Defining an inventory of information assets [Asset Inventory] (e.g. software, hardware, information, critical information assets, equipment, databases) Defining the frequency for the update of the [Asset Inventory] Ownership of the information assets
2.1.2	CL 1	<p>Define and implement an {Asset Discovery} process to identify (e.g. asset discovery tool) all information assets which belong to the organization and update the [Asset Inventory]. Assign an asset owner to each information asset.</p>
2.1.3	CL 1	<p>Review and update the [Asset Inventory] based on the frequency defined in the requirements or whenever there are modifications to the information assets (i.e. addition and removal of assets).</p>
2.1.4	CL 2	<p>Use dedicated and automated tools to discover the information assets. Integrate the information assets and track them from a central system.</p>
2.1.5	CL 3	<p>Continuously review and optimize [Requirements for Asset Discovery] and the {Asset Discovery} process.</p>
References		<p>ISO 27002 - 8.1 ISO 27002 - 8.2 ISO 27002 - 8.3.2 SANS v7.0 - 1.1 SANS v7.0 - 1.2 SANS v7.0 - 2.3 SANS v7.0 - 2.5 ETSI TR 103 305 - 2.11 NCA ECC - 2-1-1 NCA ECC - 2-1-2 NCA ECC - 2-1-6 NCA CSCC -2-1-1 NCA CSCC -2-1-2 NCA CSCC -2-1-6 NCA CSCC - 2-1-1</p>
2.2		Asset classification
Controls		

2.2.1	CL 1	Define 📄[Requirements for Asset Classification] which consider the following: <ul style="list-style-type: none"> • Classification and labelling of information assets as well as the respective protective measures for identification, handling, transfer, storage, return, deletion and disposal
2.2.2	CL 1	Define and implement an ⚙️{Asset Classification} process to classify and label information assets within your 📄[Asset Inventory] according to specific criteria (e.g. criticality, business value, legal requirements, confidentiality, integrity and availability) and the 🏹[Requirements for Information Protection].
2.2.3	CL 1	Implement the handling of assets in accordance with the ⚙️{Asset Classification} process.
2.2.4	CL 3	Continuously review and optimize the 📄[Requirements for Asset Classification] ⚙️{Asset Classification} process.
References		ISO 27002 - 8.1.2 ISO 27002 - 8.2.1 ISO 27002 - 8.2.3 NIST CSWP - ID.AM - 5 NCA ECC - 2-1-5
2.3	Bring your own device (BYOD)	
Controls		
2.3.1	CL 1	Define 📄[Cybersecurity Requirements for BYOD] within the organization which consider the following: <ul style="list-style-type: none"> • Isolation of personal information from the business information • Restrictions on the use of devices depending on the organization's business interest • Access to critical systems
2.3.2	CL 1	Enforce the defined 📄[Cybersecurity Requirements for BYOD] within the organization.
2.3.3	CL2	Ensure that the organization's information stored on the devices are encrypted.
2.3.4	CL 3	Continuously review and optimize the 📄[Cybersecurity Requirements for BYOD] within the organization.
References		SANS v6.1 - 15.9 NCA ECC - 2-6-1 NCA ECC - 2-6-2 NCA ECC - 2-6-3 NCA CSCC -2-6-3 NCA CSCC - 2-5-1

2.4		Acceptable Use Policy
Controls		
2.4.1	CL 1	Define requirements for the 📄[Acceptable Use of Information Assets] which consider the following: <ul style="list-style-type: none"> The acceptable use of information assets (e.g. install software or hardware only after obtaining a formalized approval from the defined roles such as relevant IT departments)
2.4.2	CL 1	Ensure that the 📄[Acceptable Use of Information Assets] has been implemented by the personnel in the organization (e.g. prohibiting installation of unwanted software and application, control access to web pages and prohibit access to malicious sites or dangerous websites).
2.4.3	CL 3	Continuously review and optimize the requirements for the 📄[Acceptable Use of Information Assets].
References	ISO 27002 - 8.1.3 NCA ECC - 2-1-3 NCA ECC - 2-1-4	
2.5		Asset Maintenance
Controls		
2.5.1	CL 2	Define 📄[Requirements for Asset Maintenance] which consider the following: <ul style="list-style-type: none"> Asset maintenance Tracking and monitoring Recovery plan
2.5.2	CL 2	Define and implement an ⚙️{ Asset Maintenance } process to maintain and repair the organization's information assets (including offsite assets) and keeping a log of these activities.
2.5.3	CL 2	As per the organization defined recovery plan, execute the asset recovery during or after a security incident.
2.5.4	CL 2	Perform remote monitoring and tracking (e.g. using location tracking technologies) of the information assets and ensure that they are kept within the organization controlled areas.
2.5.5	CL 3	Continuously review and optimize the 📄[Requirements for Asset Maintenance] and the ⚙️{ Asset Maintenance } process.
References	NIST CSWP - PR.MA-1 NIST CSWP - PR.MA-2 NIST CSWP - RC.RP-1 NIST.sp.800-53r4 – PE - 20 ISO 27002 - 11.2.4	

2.6		Secure disposal of assets
Controls		
2.6.1	CL 1	<p>Define  [Requirements for Disposal of Assets] which consider the following:</p> <ul style="list-style-type: none"> Setting rules for information asset disposal based on the classification and labelling of the information asset defined in the   [Asset Inventory]
2.6.2	CL 1	<p>Define and implement an  {Asset Disposal} process to handle the disposal of the information assets based on the  [Requirements for Disposal of Assets]. Use appropriate techniques (e.g. secure erase, drilling, shredding) when they are no longer required (or when they are reused) in order to prevent unauthorized disclosure or modification of information stored on the assets.</p>
2.6.3	CL 3	<p>Continuously review and optimize the  [Requirements for Disposal of Assets] and the  {Asset Disposal} process.</p>
References		<p>ISO 27002 - 8.3.2 SANS v7.0 - 1.6 SANS v7.0 - 2.6 NCA ECC 2-14-3-4</p>

3. Cybersecurity Risk Management

3.1		Cybersecurity Risk Assessment
Controls		
3.1.1	CL 1	<p>Define  [Requirements for Cybersecurity Risk Assessment] which consider the following:</p> <ul style="list-style-type: none"> • Purpose and scope of the risk assessment in the organization • The frequency and circumstance when risk assessment should be conducted in the organization • Ensuring that the  [Requirements for Cybersecurity Risk Assessment] cover the risks to the information assets and services of the organization, individuals, other organizations, and the countries associated with the organization's information systems
3.1.2	CL 1	<p>Define and implement a  {Risk Assessment} process consisting of:</p> <ul style="list-style-type: none"> • Risk identification: Identify and document internal and external risks based on the information assets of the organization  [Asset Discovery]. Maintain the identified risks in a  [Risk Register] • Risk analysis: Analyze and document the identified risks in terms of probability and impact • Risk evaluation: Identify, prioritize, and document which risk should be treated or accepted based on the organization's risk appetite. Risk evaluation outcomes must be officially approved by the top management • Upon request, report the top cybersecurity risks within the  [Risk Register] along with the remediation plans to the CITC
3.1.3	CL 2	<p>Integrate the  {Risk Assessment} process into the LSP risk management and apply it at least for the following events:</p> <ul style="list-style-type: none"> • In the early stages of major technical projects or major changes to the organization or technical architecture • Before launching new products and services to the market
3.1.4	CL 2	<p>Automate the risk assessment activities through the use of dedicated tools (e.g. GRC tool).</p>
3.1.5	CL 3	<p>Continuously review and optimize the  [Requirements for Cybersecurity Risk Assessment].</p>

References	<p>ISO 27005 - 7.2 NIST.sp.800-53r4 - RA-1 NIST.sp.800-53r4 - RA-3 NIST.sp.800-53r4 - PM-9 NIST.sp.800-53r4 - PM-10 NIST CSWP - ID.RA NIST CSWP - ID.SC NCA ECC - 1.5.1 NCA ECC - 1.5.2 NCA ECC - 1.5.3 NCA ECC - 1.5.4 NCA CSCC -1-5-1 NCA CSCC -1-5-2 NCA CSCC -1-5-3 NCA CSCC -1-5-4</p>	
3.2	Cybersecurity Risk Treatment & Monitoring	
Controls		
3.2.1	CL 1	<p>Define  [Requirements for Cybersecurity Risk Treatment and Monitoring] which consider the following:</p> <ul style="list-style-type: none"> • The risk treatment plan • The risk monitoring plan
3.2.2	CL 1	<p>Define and implement a  {Risk Treatment} process describing how assessed risks are treated resulting in a  [Risk Treatment Plan].</p>
3.2.3	CL 1	<p>Define and implement a  {Risk Monitoring} process consisting of the defined risk monitoring plan, the monitoring of the implementation of the risk treatment plan periodically, the residual risks after, and the status of the accepted risks.</p>
3.2.4	CL 2	<p>Automate the risk treatment and monitoring activities through the use of dedicated tools (e.g. GRC tool).</p>
3.2.5	CL 3	<p>Continuously review and optimize the  [Requirements for Cybersecurity Risk Treatment and Monitoring].</p>
References	<p>ISO 27005 - 9.3 NIST.sp.800-53r4 - PM-9 NIST CSWP - ID.RA NIST CSWP - ID.SC NCA ECC - 1.5.1 NCA ECC - 1.5.2 NCA ECC - 1.5.4 NCA CSCC -1-5-1 NCA CSCC -1-5-2 NCA CSCC -1-5-4</p>	

4. Logical Security

4.1		Cryptography
Controls		
4.1.1	CL 1	<p>Define  [Requirements for Cryptography] which consider the following:</p> <ul style="list-style-type: none"> Defining basic cryptographic protocols and techniques (e.g. AES 256, RSA 2048, and PKI) together with relevant restrictions (e.g. self-signed certificates, MD-5) Conditions under which approved cryptographic protocols should be applied (data in transit, at rest, in use) together with the required level of protection
4.1.2	CL 1	<p>Create a list of  [Cryptographic Solutions] (e.g. products, algorithms and protocols) in accordance to relevant restrictions (e.g. legal, technical, national) and make sure it is approved by the responsible roles.</p>
4.1.3	CL 1	<p>Use the  [Cryptographic Solutions] based on the identified circumstances, in order to protect information throughout its complete life cycle (in transit, at rest, in use) according to its classification  [Requirements for Information Protection].</p>
4.1.4	CL 2	<p>Define and implement a  {Life Cycle Management of Cryptographic Keys} process for handling the generation, protection, archiving, recovery, and destruction of cryptographic keys.</p>
4.1.5	CL 3	<p>Continuously review and optimize the  [Requirements for Cryptography] and the list of approved cryptographic solutions as well as the effectiveness of the implemented cryptographic solutions.</p>
References		<p>ISO 27002 - 10.1.1 ISO 27002 - 10.1.2 SANS v7.0 - 16.4 SANS v7.0 - 18.5 NIST.sp.800-53r4 - SC-12 NIST.sp.800-53r4 - SC-13 NCA ECC - 2-8-1 NCA ECC - 2-8-2 NCA ECC - 2-8-3 NCA ECC - 2-8-4 NCA CSCC -2-8-3</p>
4.2		Change Management
Controls		

4.2.1	CL 1	Define  [Requirements for Change Management] which consider the following: <ul style="list-style-type: none"> Identifying, classifying, and prioritizing changes to the information assets that effect cybersecurity
4.2.2	CL 1	Define and implement the  {Change Management} process to authorize cybersecurity relevant changes (e.g. applied patches, configuration changes as part of remediation, upgrading or introduction of new equipment).
4.2.3	CL 1	Plan and test the identified changes. Assess the potential impact  [Cybersecurity Risk Assessment] of the changes on cybersecurity, communicate the changes, and obtain approval from the defined authorized roles (personnel/committee).
4.2.4	CL 2	Enhance and implement the  [Requirements for Change Management] to consider the procedure for emergency changes.
4.2.5	CL 3	Continuously review and optimize the  [Requirements for Change Management] as well as the controls used in the  {Change Management} process.
References		ISO 27002 - 12.1.2 NCA ECC - 1-6-2 NCA CSCC -1-6-2
4.3	Vulnerability management	
Controls		
4.3.1	CL 1	Define  [Requirements for Vulnerability Management] which consider the following: <ul style="list-style-type: none"> Scope, tools and technology, reporting The frequency of scans Timeframes for remediating the vulnerabilities (based on the criticality)
4.3.2	CL 1	Define and implement a  {Vulnerability Management} process consisting of: <ul style="list-style-type: none"> Scanning: Conduct vulnerability scans on information assets   [Asset Inventory] using relevant tools according to the frequency defined in the requirements for vulnerability management (e.g. monthly for critical systems) Analyzing: Analyze the impact that the vulnerability has on the critical information assets and assign a criticality to it. Define and assign timeframes (depending on the criticality) within which the vulnerabilities have to be remediated Reporting: Report vulnerabilities  [Vulnerabilities Report] along with criticality of the assets to the respective

		departments and define the recommended action. 🏹 [Patch Management]
4.3.3	CL 2	Perform vulnerability scans triggered by distinct events (e.g. product release, major technical change, new equipment added to networks).
4.3.4	CL 2	Use specialized and automated vulnerability scanning tools (e.g. dedicated tools for webservers, mobile apps).
4.3.5	CL 3	Enhance vulnerability classification and reporting based on inputs from other sources (e.g. penetration testing, threat intelligence).
4.3.6	CL 3	Continuously review and optimize the 📄 [Requirements for Vulnerability Management] as well as the ⚙️ {Vulnerability Management} process.
References		<p>ISO 27002 - 12.6 SANS v7 - 3 SANS v6.1 - 4.1 SANS v6.1 - 4.8 NIST.sp.800-53r4 - RA-5 NIST.sp.800-53r4 - CA-8 NCA ECC - 2-10-1 NCA ECC - 2-10-2 NCA ECC - 2-10-3 NCA ECC - 2-10-4 NCA CSCC - 2-9-2 NCA CSCC - 2-10-1 NCA CSCC - 2-10-2 NCA CSCC - 2-10-3</p>
4.4	Patch management	
Controls		
4.4.1	CL 1	<p>Define 📄 [Requirements for Patch Management] which consider the following:</p> <ul style="list-style-type: none"> • Scope of the patch management • Tools and techniques and patch management triggers • Patch testing environment • The frequency (incorporating regular patching)
4.4.2	CL 1	<p>Define and implement a ⚙️ {Patch Management} process that develops a 📄 [Remediation Plan] considering the following aspects:</p> <ul style="list-style-type: none"> • 🏹 📄 [Vulnerabilities Report] • 🏹 [Cybersecurity Risk Assessment] • Testing the patches before deploying in production and creating necessary backups based on the risk assessment results

		<ul style="list-style-type: none"> ➔ [Change Management] Regular patch releases
4.4.3	CL 2	Ensure that the installed patches are successful and that the detected vulnerabilities have been remediated.
4.4.4	CL 2	Enhance and implement the 📄 [Requirements for Patch Management] to include emergency patch activities for highly critical vulnerabilities.
4.4.5	CL 2	Apply patch packages (or software updates) on a regular basis for all the information assets.
4.4.6	CL 2	Automate and enforce patch management wherever possible (e.g. end user devices).
4.4.7	CL 2	Enhance the 📄 [Remediation Plan] and execute it based on threat intelligence, ➔ [Penetration Testing] , and other sources.
4.4.8	CL 3	Continuously review and optimize the 📄 [Requirements for Patch Management] as well as the ⚙️ {Patch Management} process.
References		<p>SANS v6.1 - 4.4 SANS v6.1 - 4.5 SANS v6.1 - 4.7 SANS v7.0 - 3.7 NCA ECC - 2-3-3-3 NCA ECC - 2-10-3-4 NCA CSCC - 2-3-1 NCA CSCC - 2-9-1</p>
4.5	Network Security	
Controls		
4.5.1	CL 1	<p>Define ⚙️ [Requirements for Network Security] which consider the following:</p> <ul style="list-style-type: none"> Managing and controlling the security of the networks operated by the organization and the information assets connected to it Segregation of networks Security requirements to protect the network services and the information transferred through it
4.5.2	CL 1	🚫 Document the ⚙️ [Network Plan] which clearly reflects the actual state of the network (e.g. all connections into the networks, network devices, critical servers).
4.5.3	CL 1	Ensure that the incoming and outgoing traffic is controlled (e.g. preventing malicious traffic, monitoring the traffic loads of switching facilities, controlling unwanted communication such as email, SMS) based on the 📄 [Requirements for Network Security] .

4.5.4	CL 1	Ensure that only trusted and authorized protocols and IP address ranges are allowed to cross the boundary (e.g. firewall). Disable unused protocols (e.g. IPv6) on the equipment to reduce the attack surface on the network.
4.5.5	CL 1	Protect the information transferred (e.g. from interception, copying, modification) through the organization's network and ensure that the confidentiality and integrity of the information are maintained (e.g. encryption).
4.5.6	CL 1	Segregate the network into zones (e.g. domains, subnets) depending on the criticality of the information assets or services present in those zones (e.g. isolating production network from development and testing networks, separating network containing user workstations from authentication servers).
4.5.7	CL 1	Restrict the access to the organization's network (both wired and wireless networks) based on the access control list ➔ [Identity and Access Management & Privileged Access Management] .
4.5.8	CL 1	🚫 Secure the end user data, voice and signaling information transferred through the organization's telecommunications network (e.g. VoIP/SIP traffic, SS7).
4.5.9	CL 1	🚫 Segregate the hosted customer network from the organization's telecommunication operational network.
4.5.10	CL 2	🚫 Ensure that the telecommunication organization's networks that are interconnected, work in co-operation (e.g. to block email spams, DDOS, abnormal traffic patterns).
4.5.11	CL 2	🚫 Enhance and implement the 📖 [Requirements for Network Security] to handle internal and external attacks (e.g. DoS/DDoS) against the organization's network.
4.5.12	CL 2	🚫 Ensure that mechanisms are in place at the ICT facilities to detect and avoid network congestion which results in disruptions of services (e.g. implementation of additional facilities to balance the traffic load).
4.5.13	CL 2	Use specific tools to analyze and filter all traffic (e.g. port filtering, host-based filtering) to detect any unauthorized traffic in the network.
4.5.14	CL 3	Continuously review and optimize the 📖 [Requirements for Network Security] as well as the controls necessary to secure the organization's telecommunication network.
References		<p>ISO 27002 - 13.1.1 ISO 27002 - 13.1.3 ISO 27002 - 13.2.1 ISO 27011 - 13.1.3 ISO 27011 - 13.1.4 ISO 27011 - 13.1.5 ISO 27011 - 13.1.6 SANS v7.0 - 9.4</p>

	SANS v7.0 - 12.3 SANS v7.0 - 12.4 SANS v7.0 - 12.6 SANS v7.0 - 12.7 NCA ECC - 2-5-1 NCA ECC - 2-5-2 NCA ECC - 2-5-3 NCA ECC - 2-5-4 NCA ECC - 2-5-3-6 NCA CSCC - 2-5-3 NCA CSCC - 2-4-1
4.6	Logging & Monitoring
Controls	
4.6.1	<p>CL 1 Define 📄[Requirements for Logging and Monitoring] which consider the following:</p> <ul style="list-style-type: none"> • Logging the events (which are necessary to be monitored) related to the information assets which belong to the organization • Monitoring of the event logs and analysis of the detected events • Required retention period and protection of the event logs
4.6.2	CL 1 Activate event logging and record the event logs (e.g. user activities, exceptions, information security events, privileged operations) related to the information assets.
4.6.3	CL 1 Protect log information and logging facilities from unauthorized access and tampering.
4.6.4	CL 1 Periodically review the event logs and report suspicious events and detected anomalies to the responsible personnel ➡[Incident Management].
4.6.5	CL 1 Retain the logs for a defined time duration as specified in the requirements (e.g. 12 months).
4.6.6	CL 2 Collect, monitor and, analyze events using a log management tool (e.g. SIEM) that includes advanced detection and integration capabilities.
4.6.7	CL 2 Real-time monitoring and review of the event logs of critical information assets.
4.6.8	CL 2 Improve the event detection methods by the use of dedicated tools (e.g. security intelligence tools). Update the rules of the log management tools.
4.6.9	CL 3 Continuously review and optimize the 📄 [Requirements for Logging and Monitoring] as well as the effectiveness of the logging and monitoring.
References	ISO 27002 - 12.4.1

	ISO 27002 - 12.4.2 SANS v7.0 - 6.6 NIST CSWP - DE.AE-4 NIST CSWP - DE.DP-5 NCA ECC - 2-12-1 NCA ECC - 2-12-2 NCA ECC - 2-12-3 NCA ECC - 2-12-4 NCA CSCC - 2-12-3 NCA CSCC - 2-11-1 NCA CSCC - 2-11-2 NCA CSCC - 2-12-1
4.7	Identity and Access Management & Privileged Access Management (IAM & PAM)
Controls	
4.7.1	<p>CL 1 Define  [Requirements for Identity and Access Management] which consider the following:</p> <ul style="list-style-type: none"> • User accounts, privilege accounts, granting, and revoking access rights • Authentication and authorization requirements (e.g. in case of remote access, two-factor authentication) • Defining password management
4.7.2	<p>CL 1 Define and implement a process to  {Allocate/Revoke User Rights} considering:</p> <ul style="list-style-type: none"> • Assign access rights to the users based on what they are authorized to use (e.g. Role Based Access Control) • Reallocate the user access rights upon change of job functions (e.g. changing departments) • Manage user authentication and authorization based on the access control principle (e.g. need-to-know, need-to-use, principle of least privilege, and segregation of duties) and maintain an up-to-date  [Access Control List] • Revoke access rights to the information systems upon change of contractual agreements (e.g. termination of employment, change of departments)
4.7.3	CL 1 Control and restrict the allocation and use of privilege access rights.
4.7.4	CL 1 Provide multi-factor authentication for access to sensitive and critical information systems as well as for remote access.
4.7.5	CL 1 Enforce the defined password management (e.g. use of strong passwords for authentication, regular password changes) and that the user authentication information is secured against disclosure

		(e.g. using encryption mechanisms during the transfer of authentication information).
4.7.6	CL 1	Lockout accounts after a particular number of failed logon attempts (e.g. 5 logon attempts) and investigate repeated account lockouts before reauthorizing access 🏹 [Logging and Monitoring] .
4.7.7	CL 2	Regularly review user identity and access rights (review frequency taking into consideration for e.g. different account types, criticality of the information assets) and ensure conformance to the access control principles (e.g. asset owner should regularly review user access rights).
4.7.8	CL 2	Enhance and implement the 📖 [Requirements for Identity and Access Management] to use tools to automate and centralize the identity and access management.
4.7.9	CL 2	Use dedicated systems for tasks that require administrative access.
4.7.10	CL 3	Continuously review and optimize the 📖 [Requirements for Identity and Access Management] .
References		<p>ISO 27002 - 9.1.2 ISO 27002 - 9.2.1 ISO 27002 - 9.2.2 ISO 27002 - 9.2.3 ISO 27002 – 9.2.5 ISO 27002 - 9.2.6 ISO 27002 - 9.4.3 SANS v7.0 - 4.6 NCA ECC - 2-2-1 NCA ECC - 2-2-2 NCA ECC - 2-2-3 NCA ECC - 2-2-4 NCA CSCC - 2-2-1 NCA CSCC - 2-2-2 NCA CSCC - 2-2-3</p>
4.8	Application Whitelisting	
Controls		
4.8.1	CL 1	<p>Define 📖 [Requirements for Application Whitelisting] which consider the following:</p> <ul style="list-style-type: none"> • A list of authorized software • Approved application whitelisting tools
4.8.2	CL 1	Establish and disseminate an 📖 [Index of Authorized Software] including software applications, software libraries (e.g. *.dll, *.ocx, *.so) and digitally signed scripts (e.g. *.ps1, *.py, macros).
4.8.3	CL 1	Review and update the 📖 [Index of Authorized Software] on a

		regular basis.
4.8.4	CL 2	Use application whitelisting tools to ensure that only authorized software executes on all information assets and ensure that the application whitelisting technology cannot be disabled or bypassed.
4.8.5	CL 3	Continuously review and optimize the  [Requirements for Application Whitelisting] as well as the effectiveness of the application whitelisting.
References		SANS v6.1 - 2.2 SANS v7.0 - 2.6 SANS v7.0 - 2.7 SANS v7.0 - 2.8 SANS v7.0 - 2.9 NCA CSCC - 2-3-1-1
4.9	Incident Management	
Controls		
4.9.1	CL 1	Define  [Requirements for Incident Management] which consider the following: <ul style="list-style-type: none"> • Incident definition, identification and classification, prioritization, and response • Incident reporting structure • Testing the incident response process • Evidence collection • Learning from information security incidents
4.9.2	CL 1	Define and implement  {Incident Response} process considering: <ul style="list-style-type: none"> • Incident detection by analyzing reported events  [Logging and Monitoring] • Incident classification based on predefined criteria as specified in the requirements • Respond to the information security incidents (contain, eradicate, and recover) within the organization defined timeframes  [Change Management] • Prepare the  [Incident Report] and lessons learned • Report major incidents with appropriate details to CITC
4.9.3	CL 1	Conduct regular trainings to test the  {Incident Response} process for its effectiveness (e.g. testing communication channels, response times).
4.9.4	CL 2	Enhance and implement the  [Requirements for Incident Management] to use incident management tools to automate the process and integrate with other relevant systems for increasing

		efficiency.
4.9.5	CL 2	Gather threat intelligence and use it during the analysis of the information security events.
4.9.6	CL 2	Establish a forensic team to investigate the information security incident.
4.9.7	CL 2	Identify, collect, and preserve the evidences of the information security incident. Use the knowledge gained from the information security incident to reduce the probability and impact of future incidents.
4.9.8	CL 3	Continuously review and optimize the  [Requirements for Incident Management] and the associated  {Incident Response} process.
References		<p>ISO 27002 - 16.1 ISO 27002 - 16.1.2 ISO 27002 - 16.1.3 ISO 27002 - 16.1.4 ISO 27002 - 16.1.6 ISO 27002 - 16.1.7 NIST.sp.800-53r4 - IR-1 NIST.sp.800-53r4 - IR-2 NIST.sp.800-53r4 - IR-3 NIST.sp.800-53r4 - IR-4 NIST.sp.800-53r4 - IR-6 NIST CSWP RS.AN-3 NCA ECC - 2-13-1 NCA ECC - 2-13-2 NCA ECC - 2-13-3 NCA ECC - 2-13-4</p>
4.10	Malware Handling	
Controls		
4.10.1	CL 1	<p>Define  [Requirements for Malware Handling] which consider the following:</p> <ul style="list-style-type: none"> • Detection and prevention controls to protect against malware • Implementation of technical controls to safeguard the organization's information assets
4.10.2	CL 1	Use end-point protection software and ensure that this software regularly updates its signature database. Implement measures to prevent this software from being deactivated or altered by users.
4.10.3	CL 1	Implement appropriate security measures to block different sources of malicious traffic (e.g. using internet filters, emails filters to block phishing emails, restricting download of dangerous content)  [Email & Web-Based Protection].
4.10.4	CL 1	Implement protective measures to safeguard removable media

		against malware (e.g. conduct an anti-malware scan of removable media when inserted or connected).
4.10.5	CL 2	Implement advanced malware detection techniques (e.g. enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains).
4.10.6	CL 2	Use advanced logging and monitoring tools for analyzing and alerting of detected malware events ➡ [Logging and Monitoring] .
4.10.7	CL 3	Continuously review and optimize the 📖 [Requirements for Malware Handling] as well as the technical controls used to protect the information assets against the spread of malware.
References		SANS v7.0 - 7.9 SANS v7.0 - 8.1 SANS v7.0 - 8.2 SANS v7.0 - 8.4 SANS v7.0 - 8.6 SANS v7.0 - 8.7 NCA ECC - 2-4-3 NCA ECC - 2-5-3 NCA CSCC - 2-5-3
4.11	Information Protection	
Controls		
4.11.1	CL 1	Define 📖 [Requirements for Information Protection] which consider the following: <ul style="list-style-type: none"> • Classification level and criteria (e.g. restricted, confidential, public) ➡ ⚙️ {Asset Classification} • Privacy, ownership, protection, transmission, and retention of information • Ensuring the privacy of personally identifiable information or other sensitive information in the organization ➡ [Cybersecurity Compliance]
4.11.2	CL 1	Define and implement an ⚙️ {Information Classification} process considering: <ul style="list-style-type: none"> • Categorize information based on the classification criteria specified in the requirements • Handle critical information according to the defined criteria (e.g. business value, legal, technical, national and cross-border requirements)
4.11.3	CL 1	Implement security mechanisms to protect information (in transit, at rest, in use) taking into account the 📖 [Requirements for Cryptography] and data loss prevention techniques.

4.11.4	CL 1	Prevent the transmission of information from production environment to another environment and the usage of critical systems data in test and development environments.
4.11.5	CL 2	Determine a retention period for information in accordance with organizational requirements and relevant legislations. Restrict the retention to information needed in the production environment of critical systems.
4.11.6	CL 3	Continuously review and optimize the  [Requirements for Information Protection] and associated processes.
References		ISO 27002 - 8.2.1 SANS v6.1 - 13.3 NCA ECC - 2-7-1 NCA ECC - 2-7-2 NCA ECC - 2-7-3 NCA ECC - 2-7-4 NCA CSCC - 2-6-1 NCA CSCC - 2-7-3
4.12	Backup and Recovery Management	
Controls		
4.12.1	CL 1	Define  [Requirements for Backup and Recovery Management] which consider the following: <ul style="list-style-type: none"> • Scope of online and offline backups including the retention period • Rapid recovery of information after cybersecurity incidents • Periodically backup of information assets • Protection of backups • Availability of backups
4.12.2	CL 1	Define and implement a  {Backup} process consisting of the scope of online and offline backups and their coverage of information assets (e.g. backup of complete system, through processes such as imaging).
4.12.3	CL 1	Define and implement a  {Recovery} process to ensure that information assets are recovered within an acceptable timeframe based on their criticality  {Asset Classification} .
4.12.4	CL 1	Implement the  {Backup} process by periodically conducting backups to information assets based on the business requirements (e.g. Recovery Time Objective).
4.12.5	CL 1	Ensure a proper protection of backups via physical security  [Securing Equipment and Areas] .
4.12.6	CL 2	Establish an alternate storage/backup site that provides security measures equivalent to the primary site.
4.12.7	CL 2	Ensure the confidentiality, integrity, and availability of backups in adverse situations (e.g. using encryption).

4.12.8	CL 2	Continuously test and review the  {Backup} and the  {recovery} processes to check their effectiveness.
4.12.9	CL 2	Enhance and implement the  [Requirements for Backup and Recovery Management] to use tools to automate the  {Backup} and the  {Recovery} processes.
4.12.10	CL 3	Continuously review and optimize the  [Requirements for Backup and Recovery Management] and the associated processes.
References		ISO 27002 - 12.3.1 NIST.sp.800-53r4 - CP-6 NIST.sp.800-53r4 - CP-9 NCA ECC - 2-9-1 NCA ECC - 2-9-2 NCA ECC - 2-9-3 NCA CSCC - 2-8-1 NCA CSCC - 2-9-3
4.13	Configuration Management and Hardening	
Controls		
4.13.1	CL 1	Define  [Requirements for Configuration Management and Hardening] which consider the following: <ul style="list-style-type: none"> Secure images and baseline configurations for the information assets and used software/hardware
4.13.2	CL 1	Implement the defined baseline configuration settings for the information assets.
4.13.3	CL 1	 Employ system and device hardening according to industry-recognized best practices (e.g. disable the default configurations which have been installed on the network devices).
4.13.4	CL 1	Restrict the use of unnecessary functions (e.g. use of unauthorized ports, services) and configure the information assets to provide only essential capabilities.
4.13.5	CL 1	Monitor and verify configuration settings against the baseline settings.
4.13.6	CL 2	Utilize a dedicated tool to monitor and verify configuration settings and alert upon unauthorized deviation from baseline configuration settings.
4.13.7	CL 2	Use dedicated tools that can automatically configure/reconfigure configuration settings  [Change Management] on all the information assets.
4.13.8	CL 3	Continuously review and optimize the  [Requirements for Configuration Management and Hardening].
References		NIST.sp.800-53r4 - CM-6 NIST.sp.800-53r4 - CM-7

	<p>SANS v6.1 - 3.1 SANS v7.0 - 5.4 SANS v7.0 - 5.5 SANS v7.0 - 11.3 NCA ECC 1-6-2-2 NCA ECC 1-6-3-5 NCA ECC 2-5-3-5</p>	
4.14	Secure Software Development	
Controls		
4.14.1	CL 1	<p>Define  [Requirements for Secure Software Development] which consider the following:</p> <ul style="list-style-type: none"> Utilization of secure coding standards and practices (e.g. approved libraries, APIs) Segregation of and allocation of access rights to different environments Conducting tests to verify the compliance of the developed software with the organization's cybersecurity requirements
4.14.2	CL 1	Ensure that only authorized personnel has access to the appropriate environment  [Identity and Access Management & Privileged Access Management] .
4.14.3	CL 1	Utilize secure coding standards and practices (e.g. security-by-design principles supported via static or dynamic analysis tools) and ensure the security integration between the applications.
4.14.4	CL 1	Ensure a secure and reliable transmission of the software between the environments.
4.14.5	CL 1	Use only trusted and up-to-date third-party components for internally developed software.
4.14.6	CL 2	Conduct and document a security review for developed software and source code (e.g. performing error checking for all input). Conduct security tests to verify the extent to which the developed software meets the organization's cybersecurity requirements.
4.14.7	CL 3	Continuously review and optimize the  [Requirements for Secure Software Development] .
References	<p>ISO 27002 - 14.2.1 SANS v7.0 - 18.1 SANS v7.0 - 18.9 SANS v7.0 - 18.3 SANS v7.0 - 18.2 NIST.sp.800-53-r4 SA-15-b NCA ECC - 1-6-3 NCA CSCC - 1-3-2 NCA CSCC -1-6-3</p>	
4.15	Email & Web Browser Protection	

Controls		
4.15.1	CL 1	Define  [Requirements for Emails and Web Browser Protection] which consider the following: <ul style="list-style-type: none"> Utilization of standardized security mechanisms for email and web browser protection
4.15.2	CL 1	Implement the  [Requirements for Emails and Web Browser Protection] (e.g. email filtering for spam and phishing protection, multi-factor authentication, backup and archive for emails, protection against Advanced Persistent Threats, untrusted websites).
4.15.3	CL 1	Restrict the access to unauthorized web-based email services (e.g. firewall rules, network based URL filters).
4.15.4	CL 3	Continuously review and optimize the  [Requirements for Emails and Web Browser Protection].
References		SANS v7.0 – 7 NCA ECC - 2-5-3-3 NCA ECC - 2-4-1 NCA ECC - 2-4-2 NCA ECC - 2-4-3 NCA ECC - 2-4-4
4.16	Penetration Testing	
Controls		
4.16.1	CL 2	Define  [Requirements for Penetration Testing] which consider the following: <ul style="list-style-type: none"> Purpose of the penetration tests and overall objectives Defining the frequency of the penetration tests
4.16.2	CL 2	Define a  {Penetration Testing} process consisting of the scope and frequency (e.g. at least once quarterly on the critical information assets) of the penetration tests using standard methodologies to identify unknown vulnerabilities (e.g. grey box testing, white box testing).
4.16.3	CL 2	Depending on the penetration test methodology used, use the   [Vulnerabilities Report] as an input to guide the penetration tests.
4.16.4	CL 2	Report the  [Penetration Test Report] to the respective departments to trigger remediation actions when applicable  [Patch Management].
4.16.5	CL 3	Continuously review and optimize the  [Requirements for Penetration Testing] as well as the methods used in conducting penetration tests and the associated processes.

References	SANS v6.1 – 20.1 SANS v6.1 – 20.6 NCA ECC – 2-11 NCA CSCC – 2-10
-------------------	---

5. Physical Security

5.1	Securing Equipment and Areas	
Controls		
5.1.1	CL 1	<p>Define  [Requirements for Securing Equipment and Areas] which consider the following:</p> <ul style="list-style-type: none"> • Protecting equipment and physical facilities • Delivery and loading areas • Transportation of equipment
5.1.2	CL 1	<p>Define security perimeters (considering the  [Requirements for Asset Management]) in order to protect physical facilities (e.g. offices, rooms, data centers, ground stations, and telecommunication processing equipment) that contain sensitive or critical information assets.</p>
5.1.3	CL 1	<p> Ensure that the equipment reside within appropriate security zones and is stored in secure physical facilities during non-operational hours.</p>
5.1.4	CL 1	<p>Secure the delivery/loading areas that could be used by unauthorized personnel to enter the organization's premises (e.g. segregate physically where possible, incoming and outgoing shipments).</p>
5.1.5	CL 1	<p>Protect the equipment against damage from environmental threats, hazards, and unauthorized access. In addition, take into consideration the following factors for the protection of equipment:</p> <ul style="list-style-type: none"> • Power failures and disruptions (caused by the failure of supporting utilities) • Securing cables against interception, interference or damage as well as a proper cable management (e.g. cable labelling, color code) •  Operating the equipment according to the manufacturer specified requirements and controlling the working atmosphere (e.g. temperature, humidity, air quality, water, and light) •  Protection against unauthorized access (e.g. surveillance through CCTV) • Clear desk and clear screen policy (e.g. lock sensitive information stored on papers in a safe place, lock screens of computers and/or terminals when not in use or unattended)
5.1.6	CL 1	<p> Protect the equipment during their transportation taking into consideration e.g. the assessed risks, security during movement</p>

5.1.7	CL 3	Continuously review and optimize the [Requirements for Securing Equipment and Areas].
References		<p>ISO 27002 - 11.1.1 ISO 27002 - 11.1.6 ISO 27002 - 11.2.1 ISO 27002 - 11.2.2 ISO 27002 - 11.2.3 ISO 27002 - 11.2.8 ISO 27002 - 11.2.9 ISO 27011 - X.1051 - TEL.11.1.7 ISO 27011 - X.1051 - TEL.11.1.8 NCA ECC - 2-14-1 NCA ECC - 2-14-2 NCA ECC - 2-14-3 NCA ECC - 2-14-4</p>
5.2	Physical Access Management	
Controls		
5.2.1	CL 1	<p>Define [Requirements for Physical Access Management] which consider the following:</p> <ul style="list-style-type: none"> Physical access authorizations and control Monitoring physical access
5.2.2	CL 1	Create and approve a [Physical Access Control List] of individuals with authorized access to the organization's facilities and issue appropriate authorization credentials.
5.2.3	CL 1	Define and implement {Physical Access Management} process to grant and manage access (e.g. secure keys) to the physical facilities.
5.2.4	CL 1	Establish physical entry controls for visitors (e.g. provide security badges to the visitors and monitor unusual activity).
5.2.5	CL 2	Continuously review the [Physical Access Control List] of individuals with authorized access to facilities and remove them from the list when access is no longer required.
5.2.6	CL 2	Regularly review physical access logs for suspicious activity [Logging and Monitoring].
5.2.7	CL 3	Continuously review and optimize the [Requirements for Physical Access Management] as well as the effectiveness of the controls used for handling the physical access management.
References		<p>ISO 27002 - 11.1.2 NIST.sp.800-53r4 PE-2 NIST.sp.800-53r4 PE-3 NIST.sp.800-53r4 PE-6 NIST.sp.800-53r4 PE-8 NCA ECC - 2-14</p>

5.3		Environmental Protection
Controls		
5.3.1	CL 1	Define 📖 [Requirements for Environmental Protection] which consider the following: <ul style="list-style-type: none"> Defining physical protection measures against internal and external environmental threats
5.3.2	CL 1	Implement physical protection measures (e.g. deploy and maintain fire detection and suppression devices/systems) against internal (e.g. accidents, power failures, other disruptions caused by failures in supporting utilities) and external environmental threats and hazards (e.g. natural disasters).
5.3.3	CL 3	Continuously review and optimize the 📖 [Requirements for Environmental Protection] as well as the effectiveness of the controls established for emergency situations.
References		ISO 27002 - 11.1.4 ISO 27002 - 11.2.2 NIST.sp.800-53r4 - PE -11 NIST.sp.800-53r4 - PE -12 NIST.sp.800-53r4 - PE -13 NIST.sp.800-53r4 - PE -14 NIST.sp.800-53r4 - PE -15 NCA ECC - 3-1
5.4		Off-Site Assets
Controls		
5.4.1	CL 1	Define 📖 [Requirements for Off-Site Assets] which consider the following: <ul style="list-style-type: none"> Protection of equipment and physical facilities installed on offsite premises Interconnected telecommunication services
5.4.2	CL 1	Implement appropriate security measures to protect the organization's equipment installed on off-site premises (e.g. alternate work sites, co-locations) and ensure that the off-site premises are effectively secured (e.g. against physical and environmental threats).
5.4.3	CL 1	🚫 Specify well defined boundary and interfaces with other telecommunications organizations when telecommunication services are interconnected.
5.4.4	CL 3	Continuously review and optimize the 📖 [Requirements for Off-Site Assets] as well as the effectiveness of cybersecurity controls to protect the off-site assets.

References	ISO 27011 - X.1051 - 11.1.9 ISO 27011 - X.1051 - 11.3.1 ISO 27011 - X.1051 - 11.3.3 NIST.sp.800-53r4 PE-17
-------------------	---

6. Third Party Security

6.1		Cloud Services
Controls		
6.1.1	CL 1	Define  [Requirements for Cloud Services] which consider the following: <ul style="list-style-type: none"> • Cloud risk assessment • Identifying cybersecurity requirements expected from the cloud provider • Service level agreements
6.1.2	CL 1	Conduct a risk assessment in accordance with the  [Requirements for Cybersecurity Risk Assessment] prior to adopting cloud services (or in the event of changes in relevant legislative and regulatory requirements) to ensure that risks related to the use of cloud services are appropriately addressed.
6.1.3	CL 1	Identify the cybersecurity requirements (e.g. classification of data before hosting in the cloud, protecting the confidentiality, integrity and availability of the organization's data, segregation of the organization's data in cloud from other data residing in the cloud) which the cloud service provider should comply with  {Information Classification} .
6.1.4	CL 1	Establish service level agreements (SLAs) with the cloud service provider which consider at least the following: <ul style="list-style-type: none"> • Pre-defined cybersecurity requirements • Communication procedure in case of a cybersecurity incident • Right to terminate the cloud service (returning organization data in a usable format, irreversibly delete the organization's data)
6.1.5	CL 1	Ensure the hosting and storage site of the organization's data is in the Kingdom of Saudi Arabia.
6.1.6	CL 2	Audit, review, and monitor the cloud service provider for compliance with contractual obligations.
6.1.7	CL 3	Continuously review and optimize the  [Requirements for Cloud] as well as the procedures involved in selecting the cloud services and the expected cybersecurity requirements.
References	ISO 27002 - 15.1 ISO 27002 - 15.2.1	

	NCA ECC - 4-2-1 NCA ECC - 4-2-2 NCA ECC - 4-2-3 NCA ECC - 4-2-4 NCA CSCC - 4-2-1 NCA CSCC -4-2.3 NCA CSCC -4-2-3	
6.2	Outsourcing Services	
Controls		
6.2.1	CL 1	Define  [Requirements for Outsourcing Services] which consider the following: <ul style="list-style-type: none"> • Risk assessment for outsourcing services to a third party • Addressing cybersecurity requirements expected from the third party provider • Service level agreements
6.2.2	CL 1	Conduct a risk assessment in accordance with the  [Requirements for Cybersecurity Risk Assessment] prior to outsourcing any service to a third party provider (or in the event of changes in relevant legislative and regulatory requirements) to ensure that risks related to the use of outsourcing are appropriately addressed.
6.2.3	CL 1	Identify the cybersecurity requirements which the third party provider should comply with (e.g. non-disclosure clauses).
6.2.4	CL 1	Establish service level agreements with the third party service provider which consider at least the following: <ul style="list-style-type: none"> • Pre-defined cybersecurity requirements • Communication procedure in case of a cybersecurity incident • Right to terminate the contractual obligation with the third-party provider
6.2.5	CL 2	Audit, review, and monitor the third party provider for compliance with contractual obligations.
6.2.6	CL 2	Ensure that third party personnel are screened when they are contracted to work on critical systems.
6.2.7	CL 3	Continuously review and optimize the  [Requirements for Outsourcing Services] as well as the procedures involved in selecting the third party service provider and the expected cybersecurity requirements.
References	ISO 27002 - 15.1 ISO 27002 - 15.2.1 NIST CSWP - ID.SC-4 NIST CSWP - ID.SC-5	

NCA ECC - 4-1-1
NCA ECC - 4-1-2
NCA ECC - 4-1-3
NCA ECC - 4-1-4
NCA CSCC - 4-1-1
NCA CSCC - 4-1-2
NCA CSCC - 4-1-3
NCA CSCC - 4-1-4
NCA CSCC - 4-1-1

REFERENCES

For the development of this Framework CITC has considered inputs from a number of related cybersecurity standards, frameworks, regulations and similar work done by other regulatory authorities. The following references were considered during the development of the CRF:

- ISO/IEC 27001 (2013)
- ISO/IEC 27002 (2013)
- ISO 27011/ITU-T X.1051 (2016)
- ISO/IEC 27004 (2016)
- ITU-T X series
- SANS CIS Critical Security Controls Version 6.1 (2016) and 7 (2018)
- ETSI TR 103 305 - 2.11 (2018)
- National Institute of Standards & Technologies: Framework for Improving Critical Infrastructure Cybersecurity (NIST CSWP, 2018)
- National Institute of Standards & Technologies: Security and Privacy Controls for Federal Information Systems and Organizations (NIST Special Publication 800-53, Revision 4, 2013)
- National and sectorial frameworks (NCA Essential Cybersecurity Controls, 2018 and NCA Critical Systems Cybersecurity Controls, 2018)