Cybersecurity Regulatory Framework (CRF) for Service Providers in the Information and Communications Technology Sector

Version: 1.0

Date: June 2020
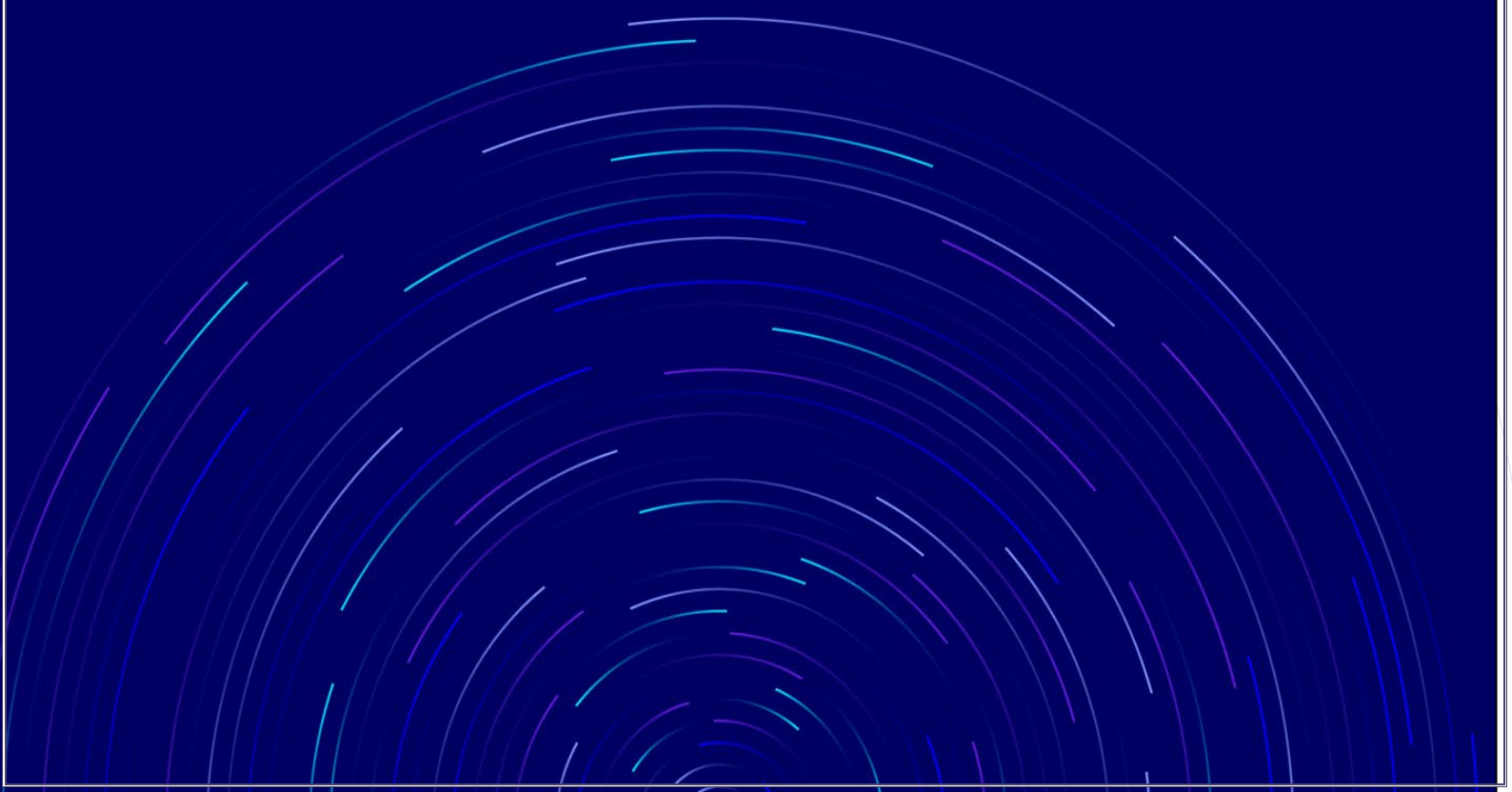
Classification: Public

CONTENT

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, CST decided to establish a comprehensive Cybersecurity Regulatory Framework (CRF) with the objective to increase the cybersecurity maturity of the Information and Communications Technology (ICT) sector and it mainly concerns organizations who are licensed or registered by CST and those subject to it as the regulator of the ICT sector in the Kingdom of Saudi Arabia.

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, strengthening 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 Service Providers in the ICT sector.
- To increase the overall cybersecurity maturity level of the ICT sector.
- To adopt a risk management methodology to achieve cybersecurity requirements.
- To encourage ICT sector Service Providers 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 ICT sector Service Providers (SPs) to fulfill the minimum security requirements.

Without prejudice to the provisions of CITC regulations which are the Act and Bylaw and the CITC regulations and regulatory frameworks, policies, guidelines and other relevant provisions and regulations including the decisions issued by CST and related directives and regulations. The provisions of this Framework shall apply to SPs subject to CST in its capacity as regulator of the sector, and specifically to licensed and registered 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. CST may determine, in its sole discretion, the scope of application of this framework to all SPs and this may be in the form of a mandatory application to all, mandatory and heuristic or partially mandatory.

4. SPs Classified as Critical National Infrastructure

All SPs classified as Critical National Infrastructure (CNI) in accordance with CST and the NCA, must comply with the following:
Essential Cybersecurity Controls (ECC) issued by the NCA (published on the NCA website).

Roles and Responsibilities

1. SP classified as CNI has full responsibility for its cybersecurity.

2. The NCA shall monitor the compliance of SPs classified as CNI with the ECC document issued by the NCA (published on the NCA website).

3. SPs classified as CNI shall apply and implement controls in this section in accordance with specified compliance requirements.

4. SPs classified as CNI shall provide CST with a copy of the compliance reports submitted to the NCA.

5. SPs classified as CNI shall share the critical cybersecurity risks with CST.

6. When a cybersecurity incident occurs, the SP classified as CNI is obliged to immediately report to the NCA and notify CST.

7. SPs Classified as CNI shall share security alerts, threat intelligence information, Indicators of Compromise, and cybersecurity incident reports with CST.

8. CST has the right to add additional controls whenever the need arises, CST will define the compliance targets and monitor compliance with those controls through various ways – including but not limited to – self assessment, field inspections, compliance workshops, proactive and incident triggered audits.

5. SPs not Classified as Critical National Infrastructure

All SPs not classified as CNI (non-CNI SPs) must comply with the following requirements and controls:

Requirements

1. Governance

   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 structure that will be responsible for the cybersecurity activities within the organization.

   1.3. Ensure compliance with internal and relevant external (national, international) regulatory requirements.

   1.4. Conduct periodic independent cybersecurity audits covering the internal and external compliance requirements to measure the compliance level of the organization.

   1.5. Conduct periodic 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 services to improve the cybersecurity awareness.

   1.7. Ensure organizational-defined cybersecurity requirements 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 employment status.

2. Asset Management

   2.1. Maintain an accurate and 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 cybersecurity risks imposed.

   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 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

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

4.1. Ensure effective and adequate use of cryptography to provide confidentiality, integrity, authenticity and non-repudiation of information in transit, at rest and in use.

4.2. Manage the changes to the information assets to control the consequences of the changes.

4.3. Identify the vulnerabilities of the information assets, to prioritize and recommend the remediation actions.

4.4. Ensure cybersecurity 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 suspicious events to the responsible personnel.

4.7. Mange 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 recovery of information assets 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

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.

6. Third Party Security

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 information assets to the organization.

Controls

1. Governance

1.1		Cybersecurity Strategy
Controls		
1.1.1	CL 1	Define and document requirements for the [Cybersecurity Strategy] which consider the following: • 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	Ensure that the [Cybersecurity Strategy] is approved by the top management.
1.1.3	CL 1	Ensure that the [Action Plan] for the implementation of the cybersecurity strategy considers the following: • Activities • Budget • Timeline • Resources (e.g. capabilities, personnel)
1.1.4	CL 3	Continuously measure, review and as per requirements 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.
References		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	
1.2	**Cybersecurity Management**	
Controls		
1.2.1	CL 1	Define and document requirements for the 🔩[Cybersecurity Organization] which consider the following: • A cybersecurity committee and allocating members who represent different areas within the organization • The needed cybersecurity functions/departments required to implement the ➔📄[Action Plan] • Direct reporting to top management to avoid conflict of interest • 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.
1.2.5	CL 3	Continuously measure, review and optimize requirements for the 📄[Cybersecurity Organization] to ensure an efficient Cybersecurity Organization.
Reference	ISO 27001 – 5	

s	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 and document [Requirements for Cybersecurity Compliance] which consider the following: • Relevant 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 and implement 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 3	Continuously measure, 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 and document [Requirements for Cybersecurity Audit] which consider the following: • Conducting independent and 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 implement {Internal Audit} process to verify the compliance with the identified [Requirements for Cybersecurity Compliance].
1.4.3	CL 2	Conduct independent audits at planned intervals (or when significant changes occur) to review the implementation of the [Requirements for Cybersecurity Compliance] in the organization.
1.4.4	CL 2	Document the findings and recommendations and present them to the top management.
1.4.5	CL 2	Protect the [Audit Records] from unauthorized access, modification, and destruction.
1.4.6	CL 2	Ensure that the audit records are retained as proof for e.g. compliance to legislative and regulatory requirements.
1.4.7	CL 3	Continuously measure, review and optimize the [Requirements for Cybersecurity Audit] as well as the effectiveness of the process 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 and document [Requirements for Cybersecurity Awareness & Training] which consider the following: • Goals and scope • Number and frequency of trainings/year • Allocated resources
1.5.2	CL 1	Define and implement a [Cybersecurity Awareness & Training Program] (e.g. defining goals, scope, targeted audience, validation criteria) that includes various cybersecurity topics considering the following: • 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 • 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)
1.5.3	CL 2	Enhance and implement the [Requirements for Cybersecurity Awareness & Training] to include periodic validation tests to evaluate the

		effectiveness of the conducted 📄[Cybersecurity 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 trainings 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 trainings to targeted group of people considering the following personnel: • Cybersecurity department • IT personnel • Personnel working in the software development • Personnel involved in cybersecurity risk management • Personnel with privileged access to critical information assets • Executive personnel
1.5.6	CL 3	Continuously measure, review and optimize the 📄[Requirements for Cybersecurity Awareness & Training].
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	CL 1	Define and document 🔐[Requirements for Customer Cybersecurity Awareness] which consider the following: • Goals and scope • Number and frequency of trainings/year • Allocated resources
1.6.2	CL 1	Define and implement a 🔐[Customer Cybersecurity Awareness Program] by e.g. defining goals, scope, targeted customer group, delivery channel which should consider the following: • 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	CL 2	Enhance and implement the 📄[Requirements for Customer Cybersecurity Awareness] to periodically conduct the 📄[Customer Cybersecurity Awareness Program] for the organization's customers.
1.6.4	CL 3	Continuously measure, review and optimize the 📄[Requirements for Customer Cybersecurity Awareness].
References	ISO 27002 – 7.2.2	
1.7	**Cybersecurity in Project Management**	
Controls		

1.7.1	CL 1	Define and document [Requirements for Cybersecurity in Project Management] which consider the following: • 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 [Cybersecurity 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 measure, 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	Define and document [Requirements for Cybersecurity in Human Resources] which consider the following: • 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	Ensure that all suspected breaches of relevant cybersecurity requirements by personnel are subject to a proper investigation and appropriate disciplinary action is taken
1.8.4	CL 1	Ensure necessary actions (e.g. revoking personnel access rights and privileges, retrieving assigned information assets, retaining access to information assets formerly controlled by terminated individual) have been carried out upon completion of professional services or termination of personnel.
1.8.5	CL 3	Continuously measure, review and optimize the [Requirements for Cybersecurity in Human Resources].
References	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

2. Asset Management

2.1		Asset Discovery
Controls		
2.1.1	CL 1	Define and document [Requirements for Asset Discovery] which consider the following: • 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	Define and implement an {Asset Discovery} process to identify (e.g. using an asset discovery tool) all information assets which belong to the organization and update the [Asset Inventory]. Assign an asset owner to each information asset.
2.1.3	CL 1	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).
2.1.4	CL 2	Use dedicated and automated tools to discover the information assets. Integrate the information assets and track them from a central system.
2.1.5	CL 3	Continuously measure, review and optimize the [Requirements for Asset Discovery] as well as the effectiveness of the process.
References		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 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	
2.2	**Asset Classification**	
Controls		
2.2.1	CL 1	Define and document [Requirements for Asset Classification] which consider the following: • 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 3	Continuously measure, review and optimize the [Requirements for Asset Classification] as well as the effectiveness of the 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 and document [Cybersecurity Requirements for BYOD] within the organization

		which consider the following: • Isolation of personal information from the business information • Restrictions on the use of devices depending on the organization's business interest • Restrictions on the access of critical systems • Secure deletion of the organization's information
2.3.2	CL 1	Enforce the defined [Cybersecurity Requirements for BYOD] within the organization.
2.3.3	CL 1	Securely delete the organization's information after the completion of the associated job function and when the information is no longer necessary.
2.3.4	CL2	Ensure that the organization's information stored on the devices are encrypted.
2.3.5	CL 3	Continuously measure, 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 of Information Assets	
Controls		
2.4.1	CL 1	Define and document the [Requirements for Acceptable Use of Information Assets] which consider the following: • The acceptable use of information assets
2.4.2	CL 1	Ensure the implementation of the [Requirements for Acceptable Use of Information Assets] (e.g. prohibiting installation of unwanted software, control access to web pages, allow the use of removable media based on business-needs only).
2.4.3	CL 3	Continuously measure, review and optimize the

		requirements for the 📄[Requirements for 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 and document 📄[Requirements for Asset Maintenance] which consider the following: • 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	Monitor information assets appropriately, based on the 📄[Asset Classification].
2.5.5	CL 3	Continuously measure, review and optimize the 📄[Requirements for Asset Maintenance] as well as the effectiveness of the 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	Define and document 📄[Requirements for Secure Disposal of Assets] which consider the following:

		• 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	Define and implement a 🔑{Secure Asset Disposal} process to handle the disposal of the information assets based on the 🗎[Requirements for Secure Disposal of Assets] that uses appropriate techniques (e.g. secure erase, drilling, shredding) in order to prevent unauthorized disclosure or modification of information stored on the assets.
2.6.3	CL 3	Continuously measure, review and optimize the 🗎 [Requirements for Secure Disposal of Assets] as well as the effectiveness of the process.
References		ISO 27002 – 8.3.2 SANS v7.0 – 1.6 SANS v7.0 – 2.6 NCA ECC 2-14-3-4

3. Cybersecurity Risk Management

3.1	Cybersecurity Risk Assessment	
Controls		
3.1.1	CL 1	Define and document 🔐[Requirements for Cybersecurity Risk Assessment] which consider the following: • 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 of the organization, individuals, and other organizations

3.1.2	CL 1	Define and implement a 🔎{Risk Assessment} process consisting of: • Risk identification: Identify and document internal and external risks based on the information assets of the organization ➦[Asset Discovery]and 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 • Report the top cybersecurity risks within the 📄[Risk Register] along with the remediation plans to the CST
3.1.3	CL 2	Integrate the ⚙️{Risk Assessment} process into the organization's risk management framework and apply it at least for the following events: • In the early stages of major technical projects or major changes to the organization or technical architecture • Before launching new products and services
3.1.4	CL 3	Continuously measure, review and optimize the 📄[Requirements for Cybersecurity Risk Assessment] as well as the effectiveness of the process.

References	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
3.2	**Cybersecurity Risk Treatment & Monitoring**
Controls	
3.2.1	CL 1	Define and document [Requirements for Cybersecurity Risk Treatment and Monitoring] which consider the following: • The risk treatment plan • The risk monitoring plan
3.2.2	CL 1	Define and implement a {Risk Treatment} process describing how assessed risks are treated resulting in a [Risk Treatment Plan].
3.2.3	CL 1	Define and implement a {Risk Monitoring} process that monitors and reviews the identified risks, the implementation of the risk treatment plan, the residual risk, and the status of the accepted risks.
3.2.4	CL 3	Continuously measure, review and optimize the [Requirements for Cybersecurity Risk Treatment and Monitoring] as well as the effectiveness of the processes.

Reference s	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

4. Logical Security

4.1		Cryptography
Controls		
4.1.1	CL 1	Define and document 📰[Requirements for Cryptography] which consider the following: • Defining basic cryptographic protocols and techniques (e.g. AES 256, RSA 2048, and PKI) together with relevant restrictions (e.g. self-signed certificates, MD5) • Conditions under which approved cryptographic protocols should be applied (data in transit, at rest, in use) taking into account the ➚📄 [Requirements for Information Protection]
4.1.2	CL 1	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.
4.1.3	CL 1	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].
4.1.4	CL 2	Define and implement a 🔍{Life Cycle Management of Cryptographic Keys} process for handling the generation, protection, archiving, recovery, and destruction of cryptographic keys.
4.1.5	CL 3	Continuously measure, review and optimize the 📄 [Requirements for Cryptography].
References	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
4.2		**Change Management**
Controls		
4.2.1	CL 1	Define and document [Requirements for Change Management] which consider the following: • 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 measure, review and optimize the [Requirements for Change Management] as well as the effectiveness of the 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 and document 🗎[Requirements for Vulnerability Management] which consider the following: • 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: • Scanning: Conduct vulnerability scans on information assets ➚🗎[Asset Inventory] using relevant tools according to the frequency defined in the requirements (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 and 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 measure, review and optimize the 📄 [Requirements for Vulnerability Management] as well as the effectiveness of the process.
References	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	

4.4	Patch Management
Controls	

4.4.1	CL 1	Define and document 📑[Requirements for Patch Management] which consider the following: • 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	Define and implement a 🔎{Patch Management} process that develops a 📑[Remediation Plan] considering the following aspects: • ↗📄[Vulnerabilities Report] • ↗[Cybersecurity Risk Assessment] • Testing the patches before deploying in production and creating necessary backups based

		on the risk assessment results • ↗[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 measure, review and optimize the 📄[Requirements for Patch Management] as well as the effectiveness of the process.
References	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	
4.5	Network Security	
Controls		
4.5.1	CL 1	Define and document 🛡[Requirements for Network Security] which consider the following: • 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. using firewalls). Disable unused protocols, (e.g. disabling IPv6 if not used) 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].
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	Cooperate with other organizations that own or operate interconnected networks with the organization's network to detect and protect the connected users and the networks from malicious acts (e.g. to block email spams, DDoS, abnormal traffic patterns, implement Caller ID authentication to block illegal caller ID spoofing).
4.5.11	CL 2	Ensure that the interfaces (e.g. Internet Exchange Points) to other networks are appropriately secured (e.g. securing BGP infrastructure, implementing high availability through redundancy, using strong cryptography).
4.5.12	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.
4.5.13	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).
4.5.14	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.
4.5.15	CL 3	Continuously measure, review and optimize the [Requirements for Network Security].
References	ISO 27002 – 13.1.1 ISO 27002 – 13.1.3 ISO 27002 – 13.2.1 ISO 27011 – X.1051 – TEL.11.3.3 ISO 27011 – X.1051 – TEL.13.1.3	

	ISO 27011 – X.1051 – TEL.13.1.4	
	ISO 27011 – X.1051 – TEL.13.1.5	
	ISO 27011 – X.1051 – TEL.13.1.6	
	SANS v7.0 – 9.4	
	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 and Monitoring**	
Controls		
4.6.1	CL 1	Define and document 📄[Requirements for Logging and Monitoring] which consider the following: • Logging the events (e.g. login attempts, configuration changes, firewall logs) 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. Threat Intelligence Platforms) to update the rules of the log management tools.
4.6.9	CL 3	Continuously measure, review and optimize the 📄 [Requirements for 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 (IAM)	
Controls		
4.7.1	CL 1	Define and document 📇[Requirements for Identity and Access Management] which consider the following: • User accounts, privilege accounts, granting, and revoking access rights • Authentication and authorization requirements (e.g. in case of remote access, two-factor

		authentication) • Password management requirements
4.7.2	CL 1	Define and implement a process to {Allocate/Revoke User Rights} considering: • 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)
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 password management requirements (e.g. use of strong passwords for authentication, regular password changes, account suspension and lockouts after multiple failed login attempts) 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 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).

4.7.7	CL 2	Enhance and implement the 📄[Requirements for Identity and Access Management] to use tools to automate and centralize the identity and access management.
4.7.8	CL 2	Use dedicated systems for tasks that require administrative access (e.g. configuration of critical systems).
4.7.9	CL 3	Continuously measure, review and optimize the 📄[Requirements for Identity and Access Management] as well as the effectiveness of the process.
References	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	
4.8	Application Whitelisting	
Controls		
4.8.1	CL 1	Define and document 🧩[Requirements for Application Whitelisting] which consider the following: • 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 measure, review and optimize the 📄 [Requirements for 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 and document 📄[Requirements for Incident Management] which consider the following: • 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: • Incident detection by analyzing reported events ↪[Logging and Monitoring] • Incident classification based on predefined criteria as specified in the requirements • Respond to the cybersecurity incidents (contain, eradicate, and recover) within the organization

		defined timeframes ➦[Change Management] • Prepare the 🗐[Incident Report] and lessons learned • Report cybersecurity incidents with appropriate details to CST
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 incidents.
4.9.7	CL 2	Identify, collect, and preserve the evidences of the information security incidents. Use the knowledge gained from the information security incidents to reduce the probability and impact of future incidents.
4.9.8	CL 3	Continuously measure, review and optimize the 📄[Requirements for Incident Management] as well as the effectiveness of the process.
References	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	
4.10	**Malware Handling**	
Controls		
4.10.1	CL 1	Define and document 📄[Requirements for Malware Handling] which consider the following: • 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, ensure that this software regularly updates its signature database, and 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 Browser 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 measure, review and optimize the 📄[Requirements for Malware Handling].
References	NIST.sp.800-53r4 – SI-3 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 and document 📑[Requirements for Information Protection] which consider the following: • Classification level and criteria (e.g. restricted, confidential, public) �ý⚙{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: • 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 of critical information to the necessary requirements. ↱ [Cybersecurity Compliance]
4.11.6	CL 3	Continuously measure, review and optimize the 🖹 [Requirements for Information Protection] as well as the effectiveness of the process.
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 and document 🖻[Requirements for Backup and Recovery Management] which consider the following: • 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 considering the following: • Business requirements (e.g. Recovery Point

		Objective)
		• 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	Ensure the confidentiality, integrity, and availability of backups in adverse situations (e.g. using encryption, protection of backups via physical security ➦ [Protection of Physical Information Assets]).
4.12.5	CL 2	Establish an alternate storage/backup site that provides security measures equivalent to the primary site.
4.12.6	CL 2	Continuously test and review the ⚙{Backup} and the ⚙{Recovery} processes to check their effectiveness.
4.12.7	CL 2	Enhance and implement the 📄[Requirements for Backup and Recovery Management] to use tools to automate the ⚙{Backup} and the ⚙{Recovery} processes.
4.12.8	CL 3	Continuously measure, review and optimize the 📄 [Requirements for Backup and Recovery Management] as well as the effectiveness of the 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 and document [Requirements for Configuration Management and Hardening] which consider the following: • 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 measure, review and optimize the [Requirements for Configuration Management and Hardening].
References	NIST.sp.800-53r4 – CM-6 NIST.sp.800-53r4 – CM-7 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	
4.14	**Secure Software Development**	
Controls		
4.14.1	CL 1	Define and document 🪟[Requirements for Secure Software Development] which consider the following: • Utilization of secure coding standards and practices (e.g. approved libraries, APIs) • Segregation 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 have access to the appropriate environment ➦[Identity and 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 of 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).
4.14.7	CL 2	Conduct security tests to verify the extent to which the developed software meets the organization's cybersecurity requirements.
4.14.8	CL 3	Continuously measure, review and optimize the 📄 [Requirements for Secure Software Development].
References	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	
4.15	**Email & Web Browser Protection**	
Controls		
4.15.1	CL 1	Define and document 📑[Requirements for Emails and Web Browser Protection] which consider the following: • 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 measure, 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 and document 🗂[Requirements for Penetration Testing] which consider the following: • 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 measure, review and optimize the 📄[Requirements for Penetration Testing] as well as the effectiveness of the process.
References	SANS v6.1 – 20.1 SANS v6.1 – 20.6 NCA ECC – 2-11 NCA CSCC – 2-10	

5. Physical Security

5.1		Protection of Physical Information Assets
Controls		
5.1.1	CL 1	Define and document 📄[Requirements for the Protection of Physical Information Assets] which consider the following: • Protecting physical facilities that host information assets • Protecting physical information assets and physical facilities installed on offsite premises • Delivery and loading areas • Transportation of physical information assets • Defining physical protection measures against environmental threats
5.1.2	CL 1	Define security perimeters in order to protect physical facilities (e.g. offices, rooms, data centers, ground stations, and telecommunication processing equipment) that contain information assets.
5.1.3	CL 1	Ensure that the physical information assets reside within appropriate security zones and are stored in secure physical facilities during non-operational hours.
5.1.4	CL 1	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).
5.1.5	CL 1	Protect physical information assets against damage from environmental threats, hazards, and unauthorized physical access by taking into consideration the following factors: • Protection measures against physical threats (e.g. fires, accidents, power failures, failures in

		supporting utilities, natural disasters) • Securing cables against interception, interference or damage as well as a proper cable management (e.g. cable labelling, color code) • ⊕Operating physical information assets 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, alarm systems, motion sensors)
5.1.6	CL 1	⊕Protect physical information assets during their transportation taking into consideration e.g. the assessed risks, security during movement.
5.1.7	CL 3	Continuously measure, review and optimize the 📄[Requirements for the Protection of Physical Information Assets].
References	ISO 27002 – 11.1.1 ISO 27002 – 11.1.4 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 ISO 27011 – X.1051 – TEL.11.1.9 ISO 27011 – X.1051 – TEL.11.3.1 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 NIST.sp.800-53r4 – PE –17	

	NCA ECC – 3-1 NCA ECC – 2-14-1 NCA ECC – 2-14-2 NCA ECC – 2-14-3 NCA ECC – 2-14-4	
5.2		**Physical Access Management**
Controls		
5.2.1	CL 1	Define and document [Requirements for Physical Access Management] which consider the following: • Physical access authorizations and control • Monitoring physical access
5.2.2	CL 1	Create 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 measure, review and optimize the [Requirements for Physical Access Management] as well as the effectiveness of the process.
References	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	

6. Third Party Security

6.1		Cloud Services
Controls		
6.1.1	CL 1	Define and document 📇[Requirements for Cloud Services] which consider the following: • Cybersecurity requirements expected from the cloud provider • Service level agreements
6.1.2	CL 1	Conduct a risk assessment in accordance with the ➚[Cybersecurity Risk Assessment] and ➚ [Information Protection] prior to adopt 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 identified and addressed.
6.1.3	CL 1	Based on the cloud risk assessment and the ➚ [Requirements for Asset classification] identify the 📇[Cloud Cybersecurity Requirements] needed to protect the confidentiality, integrity and availability of the information assets in the cloud.
6.1.4	CL 1	Establish service level agreements (SLAs) with the cloud service provider which consider at least the following: • 📄[Cloud Cybersecurity Requirements] • Incident notification and recovery obligations • Making sure that the cloud service can be terminated in case of non-compliance with the contractual agreements • Defining the exit procedures covering the secure deletion of data (e.g. irreversibly delete the organization's data, media destruction, returning organization data in a usable format, data retention).
6.1.5	CL 1	Ensure that 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 measure, review and optimize the [Requirements for Cloud Services].
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 and document [Requirements for Outsourcing Services] which consider the following: • Risk assessment for outsourcing information assets 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 [Cybersecurity Risk Assessment] and [Information Protection] prior to outsourcing any information assets 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	Based on the risk assessment identify the [Third-party Cybersecurity Requirements] which the third-party provider must comply with to protect the confidentiality, integrity and

		availability of the outsourced information assets (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: • 📄[Third-party Cybersecurity Requirements] • Communication procedure in case of a cybersecurity incident • Ensuring that the outsourced service can be terminated in case of non-compliance with the contractual agreements • Defining the exit procedures covering the secure deletion of data (e.g. media destruction, encryption).
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 measure, review and optimize the 📄 [Requirements for Outsourcing Services].
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

Roles and Responsibilities

1. Non-CNI SP has full responsibility for its cybersecurity.

2. CST shall monitor the non-CNI SPs compliance with the defined requirements (listed above) through various ways, - including but not limited to - self assessment, field inspections, compliance workshops, proactive and incident triggered audits.

3. CST shall periodically review and update the CRF.

4. CST shall define compliance requirements and set target dates to ensure non-CNI SPs compliance with the CRF.

5. Non-CNI SPs shall apply and implement requirements and controls in accordance with specified compliance targets.

6. Non-CNI SPs shall submit compliance reporting through for example self-assessment or other means upon request from CST.

7. Non-CNI SPs shall provide information and documentations to CST when requested in addition to the defined reporting in the CRF.

6. Glossary

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 Threat (APT) Protection	Protection against advanced threats that use invisible techniques to gain unauthorized access to systems and networks and stay as long as possible through circumventing detection and protection tools. To accomplish that, viruses and zero-day malware are used in these techniques.
Asset / Information Assets	Anything tangible or intangible that has value to the organization. There are many types of assets, and some of which include obvious things, such as: persons, machineries, utilities, patents, software and services. The term could also include less obvious things, such as: information and characteristics (e.g., organization's reputation and public image, as well as skill and knowledge).
Attack	Any kind of malicious activity that attempts to achieve unauthorized access, collection, disabling, prevention, destroy or sabotage of the information system resources or the information itself.
Audit	Independent review and examination of records and activities to assess the effectiveness of cybersecurity controls and to ensure compliance with established policies, operational procedures and relevant standard, legal and regulatory requirements.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system
Authorization	It is the function of defining and verifying access rights/privileges to resources related to organization's

	information and technical assets security in general and to access control in particular.
Availability	Ensuring timely access to and use of information, data, systems and applications
Backup	Files, devices, data and procedures available for use in case of failure or loss, or in case of deletion or suspension of their original copies
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 personal and contractors are permitted to use to carry out business functions.
Change Management	It is a service management system that ensures a systematic and proactive approach using effective standard methods and procedures (e.g., change in infrastructure and networks). Change Management helps all stakeholders, including individuals and teams alike, move from their current state to the next desired state, and also helps reduce the impact of relevant incidents on service.
Closed-Circuit Television CCTV	Closed-Circuit Television (CCTV), also known as video surveillance, is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors. The term is often applied to those used for surveillance in areas that may need monitoring where physical security is needed.
Cloud Computing	A model for enabling on-demand network access to a shared pool of configurable IT capabilities/resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal operation management effort or service provider interaction. It allows users to access technology-based

	services from the cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them. The cloud computing model is composed of five essential characteristics: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity and measured service. There are three types of cloud computing services delivery models: Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), and Cloud Infrastructure as a Service (IaaS); Based on the enterprise access for cloud computing, there are four models: Private Cloud, Community Cloud, Public Cloud, and Hybrid Cloud.
Compromise	Disclosure of or obtaining information by unauthorized persons, which are unauthorized to be leaked or obtained, or violation of the cybersecurity policy of the organization through disclosure, change, sabotage or loss of anything, either intentionally or unintentionally. The expression "compromise" means disclosure of, obtaining, leaking, altering or use of sensitive data without authorization (including cryptographic keys and other critical cybersecurity standards).
Confidentiality	Maintaining authorized restrictions on access to and disclosure of information, including means of protecting privacy/personal information.
Confidential Data/ Information	Organizational information (or data) that is considered highly critical and sensitive as per the organization's data classification, which it has prepared to be used by the organization itself or other specific organizations. One way to determine the classification of such type of information/data is through assessing the impact from unauthorized disclosure, access, loss or damage. Impacts could be financial or reputational on the organization or customers, impact on the lives of people related to the disclosed information, impact and harm on the national security, economy or capabilities. Confidential Data/Information includes all information that if disclosed,

	lost or damaged in an unauthorized manner, there would be legal consequences.
Critical National Infrastructure (CNI)	These are the assets (i.e., facilities, systems, networks, processes, and key operators who operate and process them), whose loss or vulnerability to security breaches may result in: • Significant negative impact on the availability, integration or delivery of basic services, including services that could result in serious loss of property and/or lives and/or injuries, alongside observance of significant economic and/or social impacts. • Significant impact on national security and/or national defense and/or state economy or national capacities
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	These are the rules that include the principles, methods and means of storing and transmitting data or information in a particular form in order to conceal its semantic content, prevent unauthorized use or prevent undetected modification so that only the persons concerned can read and process the same.
Cyber Attack	Intentional exploitation of computer systems, networks, and organizations whose work depends on digital ICT, in order to cause damage.
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 Resilience	The overall ability of organizations to withstand cyber events and, where harm is caused, recover from them.
Cybersecurity Risks	The risks to organizational operations (including vision, mission, functions, image or reputation), organizational assets, individuals, other organizations, or the nation due to the potential of unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.
Cyberspace	The interconnected network of IT infrastructure, including the Internet, communications networks, computer systems and Internet-connected devices, as well as the associated hardware and control devices. The term can also refer to a virtual world or domain such as a simple concept.
Data and Information Classification	Setting the sensitivity level of data and information that results in security controls for each level of classification. Data and information sensitivity levels are set according to predefined categories where data and information is created, modified, improved, stored or transmitted. The classification level is an indication of the value or importance of the data and information of the organization.
Data Archiving	It is the process of moving data that is no longer actively used to a separate storage device for long-term retention. Archive data consists of older data that is still important to the organization and may be needed for future reference, as well as data that must be retained for relevant legal and regulatory compliance.
Disaster Recovery	Programs, activities and plans designed to restore the organization›s critical business functions and services to

	an acceptable situation, following exposure to cyber attacks or disruption of such services.
Domain Name System (DNS)	A technical system that uses a database distributed over the network and/or the Internet which allows the translation of domain names into IP addresses, and vice-versa in order to identify service addresses such as web and email servers.
Effectiveness	Effectiveness refers to the degree to which a planned impact is achieved. Planned activities are considered effective if these activities are already implemented, and the planned results are considered effective if the results are already achieved. KPIs can be used to measure and evaluate the level of effectiveness.
Efficiency	The relationship between the results achieved (outputs) and the resources used (inputs). The efficiency of a process or system can be enhanced by achieving more results using the same resources (inputs) or even less.
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.
Event	Something that happens in a specific place (such as network, systems, applications) at a specific time
Hyper Text Transfer Protocol Secure (HTTPS)	A protocol that uses encryption to secure web pages and data when they are transmitted over the network. It is a secure version of the Hypertext Text Transfer Protocol (HTTP).
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.
Identification	It is the means of verifying the identity of a user, process, or device, typically as a prerequisite for granting access to resources in a system.
Incident	A compromise through violation of cybersecurity policies, acceptable use policies, practices or cybersecurity controls or requirements.
Integrity	Protection against unauthorized modification or destruction of information, including ensuring information non-repudiation and authenticity
Intrusion Prevention System (IPS)	A system with intrusion detection capabilities, as well as the ability to prevent and stop suspicious or potential incidents.
Key Performance Indicator (KPI)	A type of performance measurement that evaluates the success of an organization or of a particular activity in which it engages to achieve particular objectives and goals.
Labelling	Display of information (by specific and standard naming and coding) that is placed on the organization›s assets (such as devices, applications and documents) to be used to refer to some information related to the classification, ownership, type and other asset management information.
Least Privilege	A basic principle in cybersecurity that aims at granting users the access privileges they need to carry out their official responsibilities only.
Logical security	Security measures designed to protect the systems and networks of the organization from all cyber threats and harmful activities.

LSP	The Licensed Service Providers are all service providers that have requested and own license from CST 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.
Malware	A program that infects systems, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system.
Multi-Factor Authentication (MFA)	A security system that verifies user identity, which requires the use of several separate elements of identity verification mechanisms. Verification mechanisms include several elements: • Knowledge (something only the user knows "like password"). • Possession (something only owned by the user "such as a program, device generating random numbers or SMSs" for login records, which are called: One-Time-Password). • Inherent Characteristics (a characteristic of the user only, such as fingerprint).
Multi-tier Architecture	An architecture or structure to which a client-server approach is applied, in which the functional process logic, data access, data storage and user interface are developed and maintained as separate units on separate platforms.
Need-to-know and Need-to-use	The restriction of data, which is considered sensitive unless one has a specific need to know; for official business duties.
(Inter) National Requirements	National requirements are those developed by a regulatory organization or body in Saudi Arabia for regulatory use (e.g., NCA's Essential Cybersecurity Controls ECC-1:2018) International requirements are those

	developed by a global organization for worldwide regulatory or best practices use (e.g., SWIFT, PCI DSS).
Offline/Offsite Backup	A backup of databases, settings, systems, applications and devices in which it is offline and not accessible to update. Typically, backup tapes are utilized for offsite backup.
Online Backup	A method of storage in which the backup is regularly taken on a remote server over a network, (either within the organization's network or hosted by a service provider)
Organization Staff	Individuals who work for the organization (including employees, temporary employees and contractors).
Outsourcing Services	Obtaining commodities and services through contracting with supplier or service provider.
Patch	Supporting data pack used to upgrade, fix or improve computer operating systems, software or applications. This includes fixing security vulnerabilities and other bugs, with such patches usually called fixes or bug fixes and system usability or performance improvement.
Penetration Testing	The practice of testing a computer system, network, web application or mobile application to find vulnerabilities that an attacker could exploit.
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.
Phishing Emails	The attempt to obtain sensitive information such as usernames, passwords, or credit card details, often for malicious reasons and intentions, by disguising as a trustworthy organization in email messages.
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).
Policy	A document whose statements define a general commitment, direction, or intention of an organization as formally expressed by its Authorizing Official. Cybersecurity policy is a document whose statements express management's formal commitment to the implementation and improvement of the organization's cybersecurity program and include the organization's objectives regarding the cybersecurity and its controls and requirements, and the mechanisms for improving and developing it.
Privacy	Freedom from unauthorized interference or disclosure of personal information about an individual.
Procedure	A document with a detailed description of the steps necessary to perform specific operations or activities in compliance with relevant standards and policies. Procedures can be a subset of processes.
Process	A set of interrelated or interactive activities that translated input into output. Such activities are influenced by the policies of the organization.
Recovery	A procedure or process to restore or control something that is suspended, damaged, stolen or lost.
Retention	The length of time that information, data, event logs or backups must be retained, regardless of the form (i.e., paper and electronic).
Security Information and Event Management (SIEM)	A system that manages and analyzes security events logs in real time in order to provide monitoring of threats, analysis of the results of interrelated rules for event logs and reports on logs data, and incident response.
Secure Coding Standards	A practice for the development of computer software and applications in a way that protects against the exposure to cybersecurity vulnerabilities related to software and applications.

Secure Configuration and Hardening	Protecting, hardening and configuring the settings of computers, systems, applications, network devices and security devices for resisting cyber-attacks, such as: stopping or changing factory and default accounts, stopping of unused services and unused network ports.
Security Testing	A process intended to ensure that modified or new systems and applications include appropriate security controls and protection and do not introduce any security holes or vulnerabilities that might compromise other systems or applications or misuses of the system, application or its information, and to maintain functionality as intended.
Security-by Design	A methodology to systems and software development and networks design that seeks to make systems, software and networks free from cybersecurity vulnerabilities/weaknesses and impervious to cyber-attack as much as possible through measures such as: continuous testing, authentication safeguards and adherence to best programming and design practices.
Segregation of Duties	Key principle in cybersecurity that aims at minimizing errors and fraud when processing specific tasks. It is accomplished through having several people with different privileges, required to complete a task.
Third party	Any organization acting as a party in a contractual relationship to provide goods or services.
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.
Threat Intelligence	It provides organized information and analysis of recent, current and potential attacks that could pose a cyber threat to the organization.

Vulnerability	Any type of weakness in a computer system, software, application, set of procedures, or in anything that leaves cybersecurity exposed to a threat.
Zero-Day Malware	Malware that is unknown before, produced/disseminated recently, and normally hard to detect by signature-based protection anti-malware applications.

7. Annex

I. Annex Scope

This annex is concerned with clarifying compliance targets, and structure of requirements and controls related to non-CNI SPs.

II. Compliance Target

CST will set a compliance 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.
- 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.
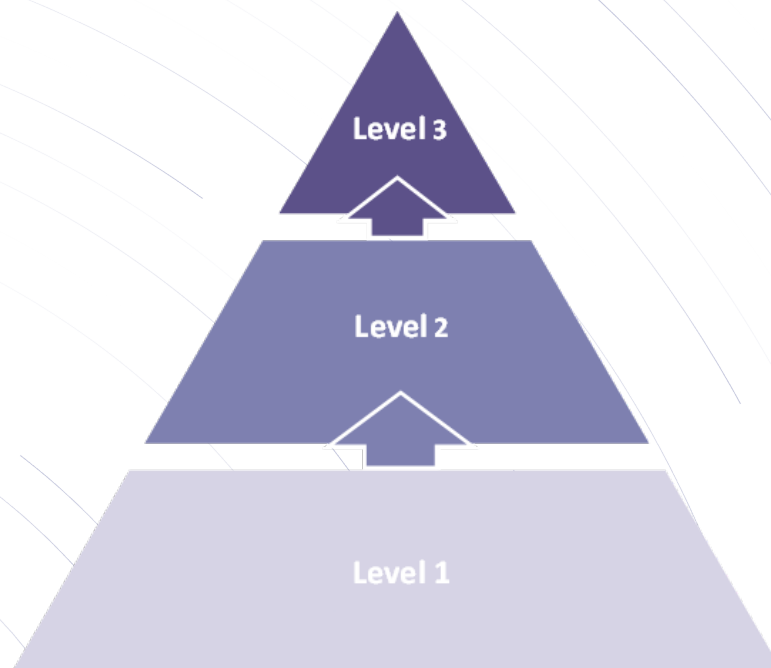
Figure1 – Compliance Levels

The compliance targets for non-CNI SPs include the target compliance level and date, which will be officially communicated by CST.

III. Structure of the controls

The CRF controls for non-CNI SPs are grouped int six domains:

Figure2 – CRF Domains for non-CNI SPs

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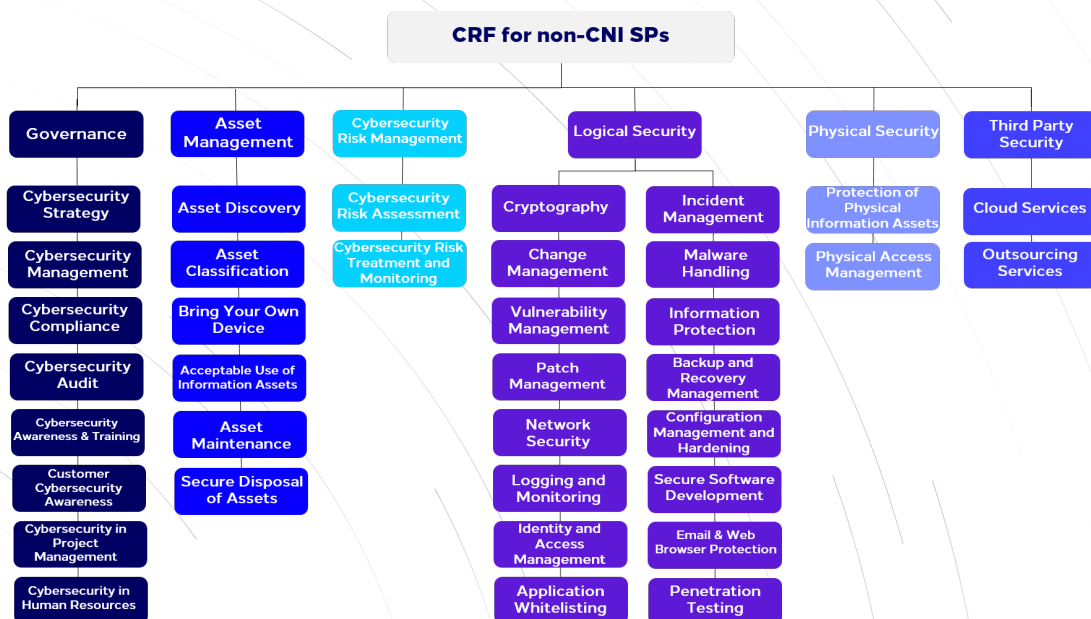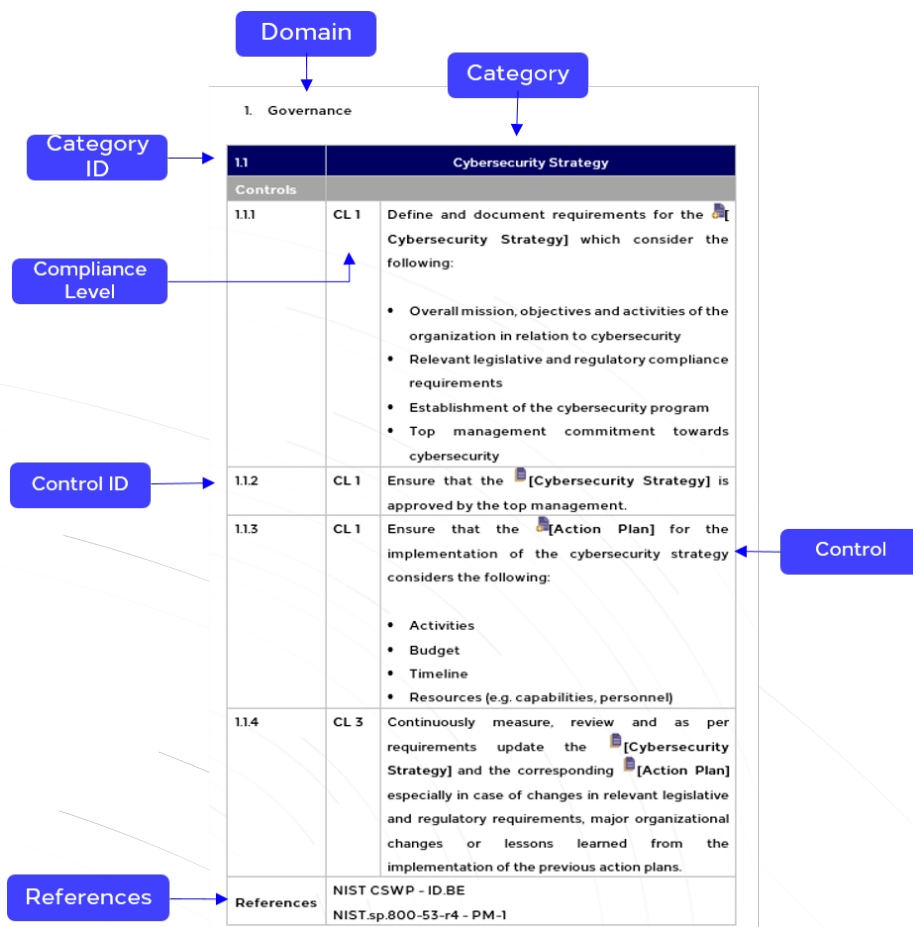

Figure 3 - CRF Domains and Categories for SPs not Classified as CNI

Figure4 - CRF Structure

Important notes

Particular control information such as 🔎[processes], ▦[outcomes], and ➦ [references] (e.g. to other controls, categories, processes, CST 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:

	New Outcome
	Outcome
	New Process
	Process
	Reference
	ICT specific

IV. References

For the development of this Framework CST 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)
- 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)
- NCA Essential Cybersecurity Controls (2018)
- NCA Critical Systems Cybersecurity Controls (2018)