الهيئـــة الوطنية
للأمـــن السيبـــراني
National Cybersecurity Authority

Guide to Essential Cybersecurity Controls (ECC) Implementation

(GECC – 1: 2023)

TLP: White
Document Classification: Public

Disclaimer: This Guide has been developed by the National Cybersecurity Authority (NCA) to enable organization to implement the Essential Cybersecurity Controls (ECC). Organizations must not rely solely on this guide to implement the ECC. They need to take into account the unique requirements of their organization and its environment. The NCA confirms that this document is only a guide that can be used as an illustrative model and does not necessarily mean that this is the only method of implementing the ECC, provided that other methods do not conflict with the requirements of the NCA. This document contains some illustrative deliverables related to the ECC implementation. The assessor/auditor has the right to request other evidence as deemed necessary to ensure that all requirements in the ECC are implemented.

In the Name of Allah,

The Most Gracious,

The Most Merciful

Traffic Light Protocol (TLP):

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

🔴 **Red – Personal, Confidential, and for the Intended Recipient Only**
The recipient has no rights to share information classified in red with any person outside the defined range of recipients, either inside or outside the organization.

🟠 **Amber – Restricted Sharing**
The recipient may share information classified in orange only with intended recipients inside the organization and with recipients who are required to take action related to the shared information.

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

⚪ **White – No Restriction**

Table of Contents

List of the Figures

Introduction

The National Cybersecurity Authority (referred to in this document as "NCA") developed this guide for implementing the Essential Cybersecurity Controls (ECC – 1: 2018), to aid national organizations in implementing the requirements that are necessary to comply with the ECC. This guide was developed based on the information and experiences that NCA collected and analyzed since the publication of the ECC and is aligned with cybersecurity best practices to facilitate the implementation of the controls across national organizations.

Objective

The main objective of this guide is to enable and aid national organizations in implementing the necessary and applicable ECC requirements that are needed for their compliance with the ECC, in addition to strengthening their cybersecurity posture, and reducing cybersecurity risks that may arise from internal and external cyber threats.

Scope of Work

This guide's scope of work is the same as the (ECC-1:2018): These controls are applicable to government organizations in the Kingdom of Saudi Arabia (including ministries, authorities, establishments, and others) and their companies and entities, as well as private sector organizations owning, operating, or hosting Critical National Infrastructures (CNIs), which are all referred to herein as "The Organization".

ECC Domains and Structure

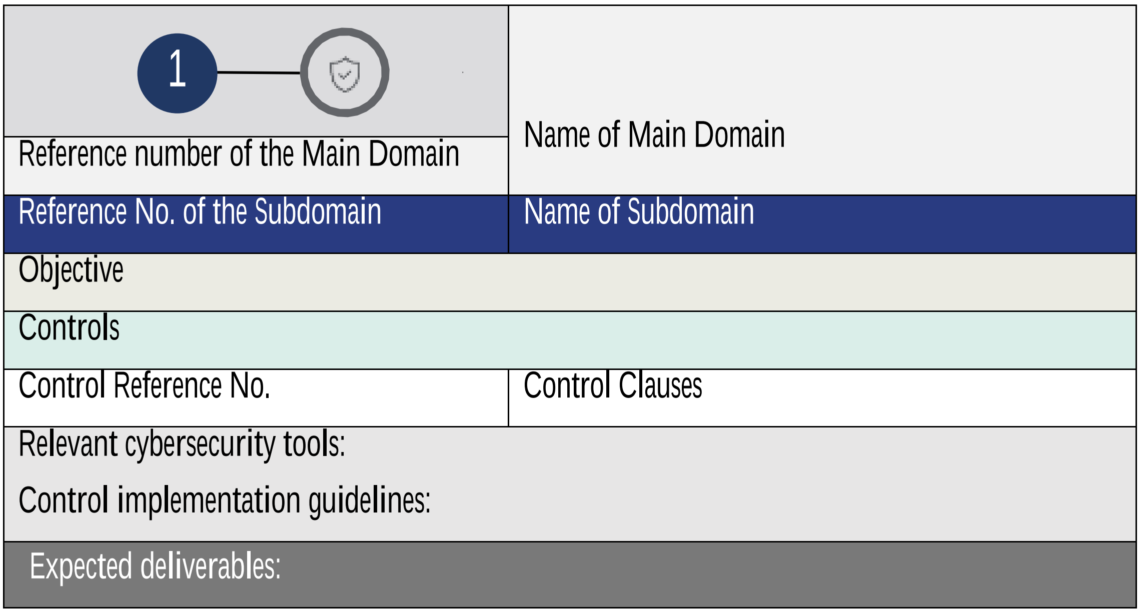
Figure 1 below shows the ECC domains and subdomains

1	حوكمة الأمن السيبراني Cybersecurity Governance	1-1	استراتيجية الأمن السيبراني Cybersecurity Strategy	1-2	إدارة الأمن السيبراني Cybersecurity Management
		1-3	سياسات وإجراءات الأمن السيبراني Cybersecurity Policies and Procedures	1-4	أدوار ومسؤوليات الأمن السيبراني Cybersecurity Roles and Responsibilities
		1-5	إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management	1-6	الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية Cybersecurity in Information Technology Projects
		1-7	الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني Cybersecurity Regulatory Compliance	1-8	المراجعة والتدقيق الدوري للأمن السيبراني Periodical Cybersecurity Review and Audit
		1-9	الأمن السيبراني المتعلق بالموارد البشرية Cybersecurity in Human Resources	1-10	برنامج التوعية والتدريب بالأمن السيبراني Cybersecurity Awareness and Training Program
2	تعزيز الأمن السيبراني Cybersecurity Defense	2-1	إدارة الأصول Asset Management	2-2	إدارة هويات الدخول والصلاحيات Identity and Access Management
		2-3	حماية الأنظمة وأجهزة معالجة المعلومات Information System and Processing Facilities Protection	2-4	حماية البريد الإلكتروني Email Protection
		2-5	إدارة أمن الشبكات Networks Security Management	2-6	أمن الأجهزة المحمولة Mobile Devices Security
		2-7	حماية البيانات والمعلومات Data and Information Protection	2-8	التشفير Cryptography
		2-9	إدارة النسخ الاحتياطية Backup and Recovery Management	2-10	إدارة الثغرات Vulnerability Management
		2-11	اختبار الاختراق Penetration Testing	2-12	إدارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management
		2-13	إدارة حوادث وتهديدات الأمن السيبراني Cybersecurity Incident and Threat management	2-14	الأمن المادي Physical Security
		2-15	حماية تطبيقات الويب Web Application Security		
3	صمود الأمن السيبراني Cybersecurity Resilience	3-1	جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال Cybersecurity Resilience Aspects of Business Continuity Management (BCM)		
4	الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية Third-Party and Cloud Computing Cybersecurity	4-1	الأمن السيبراني المتعلق بالأطراف الخارجية Third-Party Cybersecurity	4-2	الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة Cloud Computing and Hosting Cybersecurity
5	الأمن السيبراني لأنظمة التحكم الصناعي ICS Cybersecurity	5-1	حماية أجهزة وأنظمة التحكم الصناعي Industrial Control Systems (ICS) Protection		

Figure 1: ECC Domains and Subdomains

Guide Structure

Figure 2 below shows the Guide's methodological structure



1 Reference number of the Main Domain	Name of Main Domain
Reference No. of the Subdomain	Name of Subdomain
Objective	
Controls	
Control Reference No.	Control Clauses
Relevant cybersecurity tools: Control implementation guidelines:	
Expected deliverables:	

FIGURE 2: ECC STRUCTURE

ECC Implementation Guidelines

1 Cybersecurity Governance

1-1	Cybersecurity Strategy
Objective	To ensure that cybersecurity plans, goals, initiatives and projects are contributing to compliance with related laws and regulations.
Controls	
1-1-1	A cybersecurity strategy must be defined, documented and approved. It must be supported by the head of the organization or his/her delegate (referred to in this document as Authorizing Official). The strategy goals must be in-line with related laws and regulations.
	Relevant cybersecurity tools: • All cybersecurity strategy models and roadmap. Control implementation guidelines: • Conduct a workshop with stakeholders in the organization to align the objectives of the cybersecurity strategy with the organization's strategic objectives. • Develop and document cybersecurity the strategy of the organization in order to align the organization's cybersecurity strategic objectives with related laws and regulations, including but not limited to (CCC, CSCC). A cybersecurity strategy often includes the following: ○ Vision ○ Mission ○ Strategic Objectives ○ Strategy Implementation Plan ○ Projects ○ Initiatives • In order for the cybersecurity strategy of the organization to be effective, the approval of the representative must be based on the authority matrix approved by the organization.
	Expected deliverables:

	• The cybersecurity strategy document approved by the organization (electronic copy or official hard copy). • Initiatives and projects included in the cybersecurity strategy of the organization.
1-1-2	A roadmap must be executed to implement the cybersecurity strategy.
	Relevant cybersecurity tools: • All cybersecurity strategy models and roadmap. • Cybersecurity performance report and measurement template. Control implementation guidelines • Develop a roadmap for implementing the cybersecurity strategy including the execution of the strategy's initiatives and projects to: ○ Define cybersecurity priorities. ○ Make recommendations related to cybersecurity works in the organization in a manner consistent with the nature of its work. ○ Monitor the implementation of cybersecurity strategy projects and initiatives and take corrective steps if necessary. ○ Ensure the implementation of initiatives and projects according to requirements. ○ Provide a clear and unified vision and communicate it to all internal and external stakeholders. ○ Obtain NCA's approval for any cybersecurity initiatives that are beyond the scope of the organization.
	Expected deliverables : • Strategy implementation roadmap. • List of cybersecurity projects and initiatives and their status.
1-1-3	The cybersecurity strategy must be reviewed periodically according to planned intervals or upon changes to related laws and regulations.
	Control implementation guidelines: • Review and update the cybersecurity strategy periodically according to a documented and approved review plan as follows:

	○ In specific intervals according to best practices (to be determined by the organization and documented with the necessary approval in the strategy document). ○ If there are changes in the relevant laws and regulations (e.g., changes in cybersecurity requirements applicable to the organization). ○ In the event of material changes in the organization. • Document and approve the review procedures and changes to the cybersecurity strategy by the representative.
	Expected deliverables: • An approved document that defines the review schedule for the cybersecurity strategy. • An updated cybersecurity strategy after documenting changes to the cybersecurity requirements and to be approved by the representative. • Project status reports. • Formal approval by the representative on the updated strategy (e.g., via the organization's official e-mail, paper or electronic signature).

1-2	Cybersecurity Management
Objective	To ensure Authorizing Official's support in implementing and managing cybersecurity programs within the organization as per related laws and regulations
Controls	
1-2-1	A dedicated cybersecurity function (e.g., division, department) must be established within the organization. This function must be independent from the Information Technology/Information Communication and Technology (IT/ICT) functions (as per the Royal Decree number 37140 dated 14/8/1438H). It is highly recommended that this cybersecurity function reports directly to the head of the organization or his/her delegate while ensuring that this does not result in a conflict of interest.
	Relevant cybersecurity tools: • Cybersecurity Function Organizational Structure. • Cybersecurity Roles and Responsibilities Template. • Cybersecurity General Policy Template.

	Control implementation guidelines: ● Establish a cybersecurity function within the organization to enable it to carry out its cybersecurity tasks as required, taking into account the following points: ○ Ensure that the cybersecurity function's reporting line is different from that of the IT department or the digital transformation department, as per Royal Decree No. 37140 dated 14/8/1438H. ○ Ensure that the cybersecurity function is reporting to the head of the organization or his/ her deputy/ assistant for the sectors concerned with regulation, including but not limited to, deputy/ assistant head of business sectors or regulatory sectors, or the agents and heads of business sectors in the organization. ○ Ensure the following in order to avoid conflict of interest: ○ The cybersecurity function is responsible for all cybersecurity monitoring activities (including compliance monitoring, operation monitoring, operations, etc.) ○ The cybersecurity function is responsible for all cybersecurity governance activities (including defining cybersecurity requirements, managing cybersecurity risks, etc.)
	Expected deliverables: ● The organization's organizational structure (electronic copy or official hard copy), covering the organizational structure of the cybersecurity function. ● The decision to establish the Cybersecurity functions and its mandate (electronic copy or official hard copy). ● Reports on the cybersecurity policies compliance results.
1-2-2	The position of cybersecurity function head (e.g., CISO), and related supervisory and critical positions within the function, must be filled with full-time and experienced Saudi cybersecurity professionals.
	Control implementation guidelines: ● Appoint full-time and highly qualified Saudi cybersecurity professionals to fill the following job roles and positions: ○ Head of the cybersecurity function, who is responsible for leading the cybersecurity operations within the organization, setting the vision and direction for cybersecurity, strategies, resources and related

activities, and providing insights to the organization's leadership regarding effective cybersecurity risk management methods for the organization.

  - Supervisory positions within the cybersecurity function (e.g., managers of departments and functions within the cybersecurity function as per the organizational structure and/or the cybersecurity function governance and operating model approved by the authorization official), and in case there is a vacancy for any supervisory position, an employee is to be assigned to run the operations of the function or department until the supervisory position is filled as per an approved timeline.
  - Critical roles within the cybersecurity function that include responsibilities requiring confidentiality and integrity where if not performed as required, it would have negative impacts on the cybersecurity of the organization, its operations, and its systems while also considering the national laws and regulations related to nationalizing the cybersecurity positions within the organization, including direct or indirect employees and contractors (including, but not limited to, royal orders and decrees, orders issued by the Council of Ministers, and official circulars and regulatory orders issued by the National Cybersecurity Authority). The Saudi Cybersecurity Workforce Framework (SCyWF) can be utilized as reference regarding the job positions related to cybersecurity.
- Define the required academic qualifications and years of experience to serve as the head of the cybersecurity function and the supervisory and critical job roles and positions. For example, but not limited to:
  - Developing a job description of the head of the cybersecurity function position to include the minimum required number of years of experience and related fields, and the appropriate academic qualifications, and appropriate training and professional certificates in the cybersecurity and technical fields relying on The Saudi Cybersecurity Workforce Framework (SCyWF).

Expected deliverables:

- A detailed list of all personnel (direct or indirect employees and contractors), whose work is related to cybersecurity, that includes names, nationality,

	contractual type, position titles, job roles, years of experience, academic and professional qualifications. ● Job descriptions of the head of the cybersecurity and the supervisory and critical positions related to cybersecurity relying on The Saudi Cybersecurity Workforce Framework (SCyWF).
1-2-3	A cybersecurity steering committee must be established by the Authorizing Official to ensure the support and implementation of the cybersecurity programs and initiatives within the organization. Committee members, roles and responsibilities, and governance framework must be defined, documented and approved. The committee must include the head of the cybersecurity function as one of its members. It is highly recommended that the committee reports directly to the head of the organization or his/her delegate while ensuring that this does not result in a conflict of interest.
	Relevant cybersecurity tools: ● Cybersecurity supervisory committee governance document template. Control implementation guidelines: ● Establish the cybersecurity supervisory committee as a committee specialized in directing and leading cybersecurity affairs, processes, programs, and initiatives in the organization. The committee's must be directly reporting to the organization's head or his/ her deputy, taking into account non-conflict of interests. ● Identify the members of the supervisory committee, where the cybersecurity supervisory committee includes members who influence or are influenced by the cybersecurity of the organization. Such members include but are not limited to, the head of the organization or his/ her deputy, the head of the cybersecurity function, the head of the IT department, the head of the Compliance Department, the Head of the Human Resources Department. In addition, define the duties and responsibilities of the supervisory committee and its business governance framework, and formally document them in the Committee's Charter. The Committee's charter must be approved by the organization's representative (head of organization or his/ her deputy). ● Include the head of cybersecurity function as a permanent member of the committee. ● Conduct periodic meetings (based on the intervals specified in the committee's charter document). The periodic meetings cover ensuring follow-up on the implementation of cybersecurity programs and regulations in the

	organization, managing cybersecurity risks, and submitting meeting minutes to the organization head. ● Review the implementation of all cybersecurity policies and procedures. ● Update cybersecurity strategy initiatives and objectives. ● Ensure that the cybersecurity strategy is aligned with the organization's strategy on a regular basis.
	Expected deliverables : ● Supervisory committee charter in the organization. The charter clarifies the date of establishment of the committee and its reference and its approval by the organization's representative. ● A documented and approved list showing the names of the organization's cybersecurity supervisory committee members. ● Cybersecurity supervisory committee's agenda in the organization. ● Minutes of meetings held for the cybersecurity supervisory committee at the organization.

1-3	Cybersecurity Policies and Procedures
Objective	To ensure that cybersecurity requirements are documented, communicated and complied with by the organization as per related laws and regulations, and organizational requirements.
Controls	
1-3-1	Cybersecurity policies and procedures must be defined and documented by the cybersecurity function, approved by the Authorizing Official, and disseminated to relevant parties inside and outside the organization.
	Relevant cybersecurity tools: ● All policies, procedures, and standard controls templates included within NCA's cybersecurity toolkit. Control implementation guidelines: ● Define and document cybersecurity requirements in cybersecurity policies, procedures, and standard controls, and approve them by the organization's representative based on the authority matrix approved by the organization.

	• Ensure the communication of policies and procedures to the organization's personnel and internal and external stakeholders. Such communication must be done through the approved communication channels as per the scope specified in the policy (e.g., publishing policies and procedures through the organization's internal portal, or publishing policies and procedures by e-mail).
	Expected deliverables : • All cybersecurity policies, procedures, and standard controls documented and approved by the organization's representative or his/ her deputy. • Communicate cybersecurity policies, procedures, and standard controls to personnel and stakeholders .
1-3-2	The cybersecurity function must ensure that the cybersecurity policies and procedures are implemented.
	Relevant cybersecurity tools: • A template of personnel acknowledgment and approval to follow the cybersecurity policies. • A template of personnel acknowledgment and approval to maintain information confidentiality. Control implementation guidelines: • Develop an action plan to implement cybersecurity policies, procedures, and standard controls. Such plan must include all internal and external stakeholders, to whom the organization's policies, procedures, and standard controls apply. Such stakeholders must be followed- up and monitored periodically to ensure the full and effective implementation of all requirements. • The cybersecurity function must ensure the implementation of cybersecurity controls and adherence to the approved and documented cybersecurity policies, procedures, and standard controls. • Ensure the implementation of cybersecurity policies, procedures, and standard controls, including controls and requirements, manually or electronically (automated).
	Expected deliverables : • An action plan to implement the cybersecurity policies and procedures of the organization.

	• A report that outlines the review of the implementation of cybersecurity policies and procedures.
1-3-3	The cybersecurity policies and procedures must be supported by technical security standards (e.g., operating systems, databases and firewall technical security standards).
	Relevant cybersecurity tools: • A template of all standard controls included in cybersecurity tools. Control implementation guidelines: • Define, document, and approve technical standard controls to cover the organization's information and technology assets (e.g., firewall technical security standard controls, network devices, databases, server operating systems, BYOD operating systems, secure development standard, cryptography standard, etc.). • Communicate the technical standard controls to the relevant departments in the organization (e.g., IT department) and ensure that they are applied periodically to information and technology assets.
	Expected deliverables : • The organization's approved technical cybersecurity standard controls documents.
1-3-4	The cybersecurity policies and procedures must be reviewed periodically according to planned intervals or upon changes to related laws and regulations. Changes and reviews must be approved and documented.
	Control implementation guidelines: • Review the cybersecurity policies, procedures, and standard controls in the organization periodically according to a documented and approved plan for review and based on a period specified in the policy (e.g., periodic review must be conducted annually). • Review and update the cybersecurity policies, procedures, and standard controls in the organization in the event of changes in the relevant laws and regulations (for example, when a new cybersecurity law is issued that applies to the organization). • Document the review and changes to the cybersecurity policies, procedures, and standard controls and approve them by the head of the organization or his/her deputy .

	Expected deliverables: • An approved document that defines the review schedule. • An approved document that clarifies the review of cybersecurity policies, procedures and standard controls in the organization on a periodic basis based on the period of time set for review. • Policies, procedures, and standard controls documents indicating that they have been reviewed and updated, and that changes have been documented and approved by the representative . • Official approval and approval by the representative on updated policies, procedures, and standard controls .

1-4	Cybersecurity Roles and Responsibilities
Objective	To ensure that roles and responsibilities are defined for all parties participating in implementing the cybersecurity controls within the organization.
Controls	
1-4-1	Cybersecurity organizational structure and related roles and responsibilities must be defined, documented, approved, supported and assigned by the Authorizing Official while ensuring that this does not result in a conflict of interest.
	Relevant cybersecurity tools: • Cybersecurity Roles and Responsibilities Template. Control implementation guidelines: • Define and document cybersecurity roles and responsibilities and inform and ensure all parties involved in the implementation of cybersecurity controls at the organization of their responsibilities in implementing cybersecurity programs and requirements. • Support the organizational structure, roles, and responsibilities of the organization by the executive management .This must be done through the approval of the representative. • Include the following roles and responsibilities (but not limited to) : ○ Roles and responsibilities related to the cybersecurity supervisory committee.

	○ Roles and responsibilities related to the head of the cybersecurity function. ○ Roles and responsibilities related to the cybersecurity function (e.g., develop and update cybersecurity policies and standard controls, conduct cybersecurity risk assessment, conduct compliance checks on cybersecurity policies and legislation, monitor cybersecurity events, assess vulnerabilities, manage access, develop and implement cybersecurity awareness programs, etc.) ○ Roles and responsibilities related to cybersecurity for other departments in the organization (e.g., IT, personnel, physical security, etc.) ○ Cybersecurity roles and responsibilities for all personnel. ● Assign roles and responsibilities to the organization's personnel, taking into consideration the non-conflict of interests.
	Expected deliverables: ● Cybersecurity Function Organizational Structure Document. ● The organization's approved cybersecurity roles and responsibilities document (electronic copy or official hard copy). ● A document that clarifies the assignment of cybersecurity roles and responsibilities to the organization's personnel.
1-4-2	The cybersecurity roles and responsibilities must be reviewed periodically according to planned intervals or upon changes to related laws and regulations.
	Control implementation guidelines: ● Review the cybersecurity roles and responsibilities in the organization periodically according to a documented and approved plan for review and based on a planned interval (e.g., periodic review must be conducted annually). ● Review and update the cybersecurity roles and responsibilities in the organization in the event of changes in the relevant laws and regulations (for example, when a new cybersecurity law is issued that applies to the organization). ● Document the review and changes to the cybersecurity requirements related to cybersecurity roles and responsibilities and approve them by the representative.

	Expected deliverables: ● An approved document that defines the review schedule for the roles and responsibilities. ● Roles and responsibilities document indicating that they are up to date and the changes to the cybersecurity requirements for roles and responsibilities have been documented and approved by the representative.

1-5	Cybersecurity Risk Management
Objective	To ensure managing cybersecurity risks in a methodological approach in order to protect the organization's information and technology assets as per organizational policies and procedures, and related laws and regulations.
Controls	
1-5-1	Cybersecurity risk management methodology and procedures must be defined, documented and approved as per confidentiality, integrity and availability considerations of information and technology assets.
	Relevant cybersecurity tools: ● Cybersecurity Risk Management Policy Template. ● Cybersecurity Risk Management Procedures Template. Control implementation guidelines: ● Define and document cybersecurity risk management requirements which are based on relevant regulations, best practices, and standard controls of cybersecurity risk management, taking into account the confidentiality, availability, and integrity of information and technology assets to cover the following: ○ The methodology and procedures of cybersecurity risk management in the organization must include: - Identification of assets and their value. - Identification of risks to the business, assets, or personnel of the organization.

	– Risk assessment, so that the likelihood and impact of the identified risks are defined. – Risk response, where cyber risk treatment methods are identified. – Risk monitoring, so that the risk register is updated after each risk assessment and response plan. • Support the cybersecurity risk management methodology and procedures in the organization by the Executive Management through the approval of the representative.
	Expected deliverables : • The approved cybersecurity risk management methodology (electronic copy or official hard copy). • Approved cybersecurity risk management procedures.
1-5-2	The cybersecurity risk management methodology and procedures must be implemented by the cybersecurity function.
	Relevant cybersecurity tools: • Cybersecurity Risk Management Register Template. Control implementation guidelines: • Implement all requirements of the cybersecurity risk management methodology and procedures adopted by the organization. • Establish a cybersecurity risk register to document and monitor risks. • Develop plans to address cybersecurity risks of the organization.
	Expected deliverables: • Cybersecurity Risk Register of the organization. • Cybersecurity Risk Treatment Plan of the organization. • A report that outlines the cybersecurity risk assessment and monitoring.
1-5-3	The cybersecurity risk assessment procedures must be implemented at least in the following cases:
	1-5-3-1 Early stages of technology projects.
	Control implementation guidelines:

- Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.
- Include cybersecurity requirements within the first phase of the information and technology projects lifecycle (Technical Project Lifecycle) within the organization.
- Implement cybersecurity risk assessment procedures at an early stage of technical projects to avoid events or circumstances that could compromise the confidentiality, integrity, and availability of information and technology assets, including, in particular, the identification of information and technology assets in technology projects, potential exposure to threats, and relevant vulnerabilities.
- Remediate all cybersecurity risks in accordance with the approved cybersecurity risk management methodology.

Expected deliverables:

- A report that outlines the identification, assessment, and remediation of cybersecurity risks throughout the technical project lifecycle in the organization.

1-5-3-2	Before making major changes to technology infrastructure.

Control implementation guidelines:

- Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.
- Include cybersecurity requirements within the IT Change Management lifecycle in the organization.
- Implement cybersecurity risk assessment procedures before making a material change in the technology architecture to avoid events or circumstances that could compromise the confidentiality, integrity, and availability of information and technology assets, including, in particular, the identification of information and technology assets in technology projects, potential exposure to threats, and relevant vulnerabilities. These changes include, but are not limited to: a basic and sensitive update to one or several systems in the network, such as database systems, or a radical change in network mapping
- Remediate all cybersecurity risks in accordance with the approved cybersecurity risk management methodology.

Expected deliverables:

	• A report that outlines the identification, assessment, and remediation of the cybersecurity risks of material changes to the production environment of the organization's information and technology assets.	
	1-5-3-3	During the planning phase of obtaining third party services.
	Control implementation guidelines: • Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. • Include cybersecurity requirements within the third-party, contracts, and procurement management procedures in the organization. • Implement cybersecurity risk assessment procedures when planning to acquire services from a third party. to avoid events or circumstances that could compromise the confidentiality, integrity, and availability of information and technology assets, including, in particular, the identification of information and technology assets in technology projects, potential exposure to threats, and relevant vulnerabilities. • Remediate all cybersecurity risks in accordance with the approved cybersecurity risk management methodology.	
	Expected deliverables: • A report that outlines the identification, assessment, and remediation of third-party cybersecurity risks that provide outsourcing services to IT or managed services.	
	1-5-3-4	During the planning phase and before going live for new technology services and products.
	Control implementation guidelines: • Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. • Include cybersecurity requirements within the Release Management procedures in the organization. • Implement cybersecurity risk assessment procedures at the planning stage and before the release of new technology products and services to avoid events or circumstances that could compromise the confidentiality, integrity, and availability of information and technology assets, including, in particular, the	

	identification of information and technology assets in technology projects, potential exposure to threats, and relevant vulnerabilities. • Remediate all cybersecurity risks in accordance with the approved cybersecurity risk management methodology.
	Expected deliverables: • A report that outlines the identification, assessment, and remediation of cybersecurity risks in the planning stage and before releasing new technical products and services in the production environment.
1-5-4	The cybersecurity risk management methodology and procedures must be reviewed periodically according to planned intervals or upon changes to related laws and regulations. Changes and reviews must be approved and documented.
	Control implementation guidelines: • Review and update the cybersecurity risk management methodology and procedures and cybersecurity risk management requirements in the organization periodically according to a documented and approved plan for review and based on a planned interval (e.g., periodic review must be conducted annually). • Review and update the cybersecurity risk management methodology and procedures and cybersecurity risk management requirements in the organization in the event of changes in the relevant laws and regulations (for example, when a new cybersecurity law is issued that applies to the organization). • Document the review and changes to the cybersecurity requirements related to cybersecurity risk management methodology and procedures and approve them by the representative.
	Expected deliverables: • An approved document that defines the review schedule for the cybersecurity risk management methodology and procedures. • Cybersecurity risk methodology and procedures indicating that they have been reviewed and updated, and that changes have been documented and approved by the representative .

1-6	Cybersecurity in Information and Technology Project Management
Objective	To ensure that cybersecurity requirements are included in project management methodology and procedures in order to protect the confidentiality, integrity and availability of information and technology assets as per organization policies and procedures, and related laws and regulations.
Controls	
1-6-1	Cybersecurity requirements must be included in project and asset (information/ technology) change management methodology and procedures to identify and manage cybersecurity risks as part of project management lifecycle. The cybersecurity requirements must be a key part of the overall requirements of technology projects.
	Relevant cybersecurity tools: ● Secure Software Development Cycle Policy Template. ● Secure Software Development Cycle Procedure Template. Control implementation guidelines: ● Include cybersecurity requirements in the project management methodology and procedures and in the change management of the information and technology assets in the organization to ensure that cybersecurity risks are identified and addressed. Such requirements include: ○ Assess and detect vulnerabilities before the deployment of services or systems online, or upon any change to systems within Information and Technology Project Management. ○ Fix identified vulnerabilities before launching projects and changes. ○ Review Secure Configuration and Hardening and Patching and address observations identified before launching projects and changes. ○ Define the requirements for connection with cyber surveillance systems. ● Support cybersecurity requirements of the project management methodology and procedures by the Executive Management through the approval of the head of the organization or his/ her deputy.
	Expected deliverables: ● Project Management Methodology Document in the organization. ● Change management methodology or procedures in the organization's information and technology assets document.

1-6-2	The cybersecurity requirements in project and assets (information/technology) change management must include at least the following:	
	1-6-2-1	Vulnerability assessment and remediation.
	Control implementation guidelines: • Define and document the requirements of this control in the cybersecurity requirements document and approve them by the representative. • Define systems, services, and technology components subject to Vulnerabilities Assessment within the scope of technical projects and change requests. • Develop and adopt procedures for the implementation of Vulnerabilities Assessment and remediation in accordance with related laws and regulations. • Conduct Vulnerabilities Assessment before launching technical projects in the production environment and assess it in a timely manner and address it effectively. • Conduct Vulnerabilities Assessment before the implementation of changes to the production environment and assess it in a timely manner and address it effectively.	
	Expected deliverables: • A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. • A report that outlines the assessment and remediation of cybersecurity vulnerabilities throughout the technical project lifecycle and changes to information and technology assets.	
	1-6-2-2	Conducting a configurations ’ review, secure configuration and hardening and patching before changes or going live for technology projects.
	Relevant cybersecurity tools: • Cybersecurity Requirements Checklist Template for Project Management and Changes to Information and Technology Assets. • Cybersecurity Requirements Checklist Template for Application Development. Control implementation guidelines: • Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.	

		• Define systems, services, and technology components subject to Secure Configuration and Hardening review within the scope of technical projects and change requests. • Provide technical Security Standard controls for systems, services, and technology components subject to Secure Configuration and Hardening review. • Develop and adopt procedures for the implementation of Secure Configuration and Hardening review in accordance with the relevant laws and regulations. • Review secure Configuration and Hardening and Patching before launching technology projects in the production environment. • Review secure Configuration and Hardening and Patching before implementing changes to the production environment.
		Expected deliverables: • A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. • Technical Security Standard controls for systems, services, and technology components subject to Secure Configuration and Hardening review. • A report that outlines the assessment and review of Secure Configuration and Hardening throughout the technical project lifecycle and changes to information and technology assets in the organization before launching projects and implementing changes.
1-6-3		The cybersecurity requirements related to software and application development projects must include at least the following:
	1-6-3-1	Using secure coding standards.
		Relevant cybersecurity tools: • Secure Coding Standard Template. Control implementation guidelines: • Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. • Define and document technical cybersecurity requirements for Secure Coding Standard controls (covering all phases of the secure coding process) based on relevant laws and regulations, best practices and standard controls related to the development and protection of software and applications against internal

		and external threats in the organization to minimize cyber risks and focus on key security objectives namely; confidentiality, integrity, and availability. • Communicate Secure Coding Standard controls to the relevant departments in the organization (e.g., IT department) and their implementation periodically.
		Expected deliverables: • A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. • Secure Coding Standard controls approved by the organization. • Documents that confirm the implementation of Secure Coding Standard controls to information and technology assets.
	1-6-3-2	Using trusted and licensed sources for software development tools and libraries.
		Control implementation guidelines: • Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. • Use only modern, reliable and licensed sources for software development tools and libraries.
		Expected deliverables: • A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. • An updated list of licensed and documented software used for application development tools and libraries.
	1-6-3-3	Conducting compliance test for software against the defined organizational cybersecurity requirements.
		Relevant cybersecurity tools: • Cybersecurity Requirements Checklist Template for Application Development. Control implementation guidelines: • Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. • Conduct testing to verify that applications meet the cybersecurity requirements of the organizations, such as penetration testing, to ensure that

	cybersecurity controls are applied to the development of secure coding standard controls and detect weaknesses, vulnerabilities, and issues in software. • Access Management requirements for users and review the cybersecurity architecture.	
	Expected deliverables: • A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. • List of application development projects and list of security tests performed to verify the comprehensiveness of the tests and the extent to which the applications meet the organization's cybersecurity requirements and implementation reports.	
	1-6-3-4	Secure integration between software components.
	Control implementation guidelines • Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. • Ensure security of integration between applications by, but not limited to, security testing of various integration technologies, including: ○ Perform System Integration Testing (SIT). ○ Perform API testing.	
	Expected deliverables: • A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. • A report that outlines the testing and assessment of secure Integration between applications based on the organization's cybersecurity requirements and implementation reports.	
	1-6-3-5	Conducting a configurations ’ review, secure configuration and hardening and patching before going live for software products.
	Control implementation guidelines: • Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. • Review secure Configuration and Hardening and Patching before launching applications and ensure their implementation in the following cases:	

	○ Secure Configuration and Hardening of information and technology assets and applications must be reviewed periodically and their implementation according to the approved technical security standard controls must be ensured. ○ Secure configuration and hardening must be reviewed before launching projects and changes in information and technology assets. ○ Secure Configuration and Hardening must be reviewed before launching applications. ● Approve the Image for the Secure configuration and hardening of information and technology assets in accordance with the technical security standard controls and kept it in a safe place. ● Provide technology required to centrally manage Secure Configuration and Hardening and ensure the automated implementation or update of Secure Configuration and Hardening for all information and technology assets at pre-determined regular intervals.
	Expected deliverables: ● A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. ● Reports or evidence that Secure Configuration and Hardening and patching are reviewed before launching applications. ● Reports or evidence that Secure Configuration and Hardening and patching are periodically reviewed.
1-6-4	The cybersecurity requirements in project management must be reviewed periodically.
	Control implementation guidelines: ● Review the cybersecurity project management requirements periodically according to a documented and approved plan for review and based on a planned interval (e.g., periodic review must be conducted annually). ● Document the review and changes to the cybersecurity requirements for project management in the organization and approve them by the head of the organization or his/her deputy.
	Expected deliverables:

	• An approved document that defines the review schedule for the cybersecurity requirements for project management. • Evidence that the periodic review of cybersecurity requirements in project management and changes to the information and technology assets of the organization is performed.

1-7	Compliance with Cybersecurity Standard controls, Laws and Regulations
Objective	To ensure that the organization's cybersecurity program is in compliance with related laws and regulations.
Controls	
1-7-1	The organization must comply with related national cybersecurity laws and regulations.
	Relevant cybersecurity tools: • Compliance with Cybersecurity Standard controls, Laws and Regulations Policy Template. Control implementation guidelines: • Work with stakeholders in the organization (i.e., legal function and governance and compliance function) to identify, document, and periodically update a list of national cybersecurity laws and regulations and related requirements that are relevant to the organization's operations and issued by the National Cybersecurity Authority (NCA) (which might include, but not limited to, royal orders and decrees, orders issued by the Council of Ministers, and official circulars and regulatory orders issued by the National Cybersecurity Authority (NCA)). • Ensure compliance with all national cybersecurity laws and regulations requirements referred to in the previous point. • Provide necessary technologies; to verify compliance with national cybersecurity laws and regulations. • Prepare periodic reports for organization's compliance with all national cybersecurity laws and regulations to be submitted to the National Cybersecurity Authority (NCA) whenever requested.
	Expected deliverables :

	• A document (such as a policy, procedure, or/and letter approved by the authorization official) indicating the identification and documentation of the requirements related to this control. • An updated list that clarifies the national cybersecurity laws and regulations that are relevant to the organization's operations and issued by the National Cybersecurity Authority (NCA). • A report that clarifies the extent of organization's compliance with national cybersecurity laws and regulations applicable to the organization.
1-7-2	The organization must comply with any nationally-approved international agreements and commitments related to cybersecurity.
	Control implementation guidelines: • Work with the organization's stakeholders to identify, document, approve and periodically update the list of international cybersecurity agreements or obligations, and periodically document and update them, subject to prior approval by the National Cybersecurity Authority. • Ensure compliance with all cybersecurity national laws and regulations requirements approved by the National Cybersecurity Authority within the organization. • Provide necessary technologies to verify compliance with the laws and regulations related to cybersecurity.
	Expected deliverables : • A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. • An updated list of locally approved international agreements and obligations applicable to cybersecurity function. • A report that outlines the extent of compliance with cybersecurity international agreements and obligations applicable to the organization.

1-8	Periodical Cybersecurity Review and Audit

Objective	To ensure that cybersecurity controls are implemented and in compliance with organizational policies and procedures, as well as related national and international laws, regulations and agreements.
Controls	
1-8-1	Cybersecurity reviews must be conducted periodically by the cybersecurity function in the organization to assess the compliance with the cybersecurity controls in the organization.
	Relevant cybersecurity tools: • Cybersecurity Review and Audit Template. • Cybersecurity Review and Audit Log Template. Control implementation guidelines: • Review the implementation of cybersecurity requirements at the organization by the cybersecurity function periodically according to a documented and approved plan for review and based on a period specified in the policy (e.g., quarterly review), to ensure that the cybersecurity controls of the organization are effectively implemented and operate in accordance with the regulatory policies and procedures of the organization, the national laws and regulations, and the international requirements approved by the organization.
	Expected deliverables : • A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. • Approved plan to review the implementation of cybersecurity controls. • Documents that confirm the implementation of Cybersecurity Standard controls to information, technology, and physical assets. • Periodic review reports of cybersecurity controls implementation in the organization.
1-8-2	Cybersecurity audits and reviews must be conducted by independent parties outside the cybersecurity function (e.g., Internal Audit function) to assess the compliance with the cybersecurity controls in the organization. Audits and reviews must be conducted independently, while ensuring that this does not result in a conflict of

	interest, as per the Generally Accepted Auditing Standard controls (GAAS), and related laws and regulations.
	Relevant cybersecurity tools: • Cybersecurity Review and Audit Template. • Cybersecurity Review and Audit Log Template. Control implementation guidelines: • Review and audit cybersecurity controls implementation at the organization by parties independent of the cybersecurity function, such as the internal audit department, or by third parties that cooperated with independently from the relevant cybersecurity function to achieve the principle of non-conflict of interests when reviewing the implementation of all cybersecurity requirements in the organization. • Perform the review periodically according to a documented and approved plan for review and based on a period specified in the policy (e.g., review must be conducted annually), in order to ensure that the organization's cybersecurity controls are effectively implemented and operate in accordance with the regulatory policies and procedures of the organization, the national laws and regulations approved by NCA, and the international requirements approved by the organization.
	Expected deliverables: • A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. • Approved plan to review and audit the implementation of cybersecurity controls. • Audit reports (by the internal audit department or an independent external auditor) on all cybersecurity requirements of the organization
1-8-3	Results from the cybersecurity audits and reviews must be documented and presented to the cybersecurity steering committee and Authorizing Official. Results must include the audit/review scope, observations, recommendations and remediation plans.
	Relevant cybersecurity tools: • Cybersecurity Review Report Template.

	Control implementation guidelines: ● Review and document results of cybersecurity review and audit. The review report must include: ○ Scope of review and audit. ○ Discovered observations. ○ Recommendations and corrective actions. ○ Observations remediation plan. ● Share and discuss the results of cybersecurity review and audit with the cybersecurity supervisory committee and the representative.
	Expected deliverables: ● A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. ● Audit reports (by the internal audit department or compliance department or an independent external auditor) on all cybersecurity requirements of the organization . ● Evidence that the results of the cybersecurity review and audit presented to the cybersecurity supervisory committee and the representative.

1-9	Cybersecurity in Human Resources
Objective	To ensure that cybersecurity risks and requirements related to personnel (employees and contractors) are managed efficiently prior to employment, during employment and after termination/separation as per organizational policies and procedures, and related laws and regulations.
Controls	
1-9-1	Personnel cybersecurity requirements (prior to employment, during employment and after termination/separation) must be defined, documented and approved.
	Relevant cybersecurity tools: ● Human Resources Cybersecurity Policy Template. Control implementation guidelines:

	• Define and document personnel cybersecurity requirements in the cybersecurity requirements document and approved by the representative . Requirements include, but are not limited to: o Include cybersecurity responsibilities and non-disclosure clauses in the contracts of employees in the organization (to cover the periods during and after the end/termination of the job relationship with the organization). o Conduct screening or vetting for the personnel of cybersecurity functions, technical functions with privileged access, and critical systems functions. • Ensure the comprehensiveness of the cybersecurity requirements related to employees during the employee's lifecycle in the organization, including the following requirements: o Cybersecurity requirements prior to recruitment. o Cybersecurity requirements during work. o Cybersecurity requirements upon completion or termination of work. • Support the organization's policy by the Executive Management .This must be done through the approval of the organization head or his/ her deputy.
	Expected deliverables : • Cybersecurity policy for human resources approved by the representative.
1-9-2	The personnel cybersecurity requirements must be implemented.
	Control implementation guidelines: • Implement all personnel-related cybersecurity requirements that have been identified, documented and approved in the Human Resources Cybersecurity Policy. • Develop an action plan to implement cybersecurity requirements related to the personnel of the organization. • Include personnel cybersecurity requirements in the organization's HR procedures to ensure compliance with cybersecurity requirements for all internal and external stakeholders.
	Expected deliverables : • Documents that confirm the implementation of cybersecurity requirements related to personnel as documented in the HR Cybersecurity Policy. • Cybersecurity Function Personnel Contract Forms (signed copy).

	• Screening or vetting requests for the personnel of cybersecurity functions and technical functions with privileged access .	
1-9-3	The personnel cybersecurity requirements prior to employment must include at least the following:	
	1-9-3-1	Inclusion of personnel cybersecurity responsibilities and non-disclosure clauses (covering the cybersecurity requirements during employment and after termination/ separation) in employment contracts.
	Relevant cybersecurity tools: • Acknowledgment and confidentiality templates. Control implementation guidelines: • Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. • Work with relevant departments to include cybersecurity responsibilities and non-disclosure clauses in the contracts of employees in the organization (to cover the periods during and after the end/termination of the job relationship with the organization). • Include such requirements in the organization's HR procedures to ensure compliance with cybersecurity requirements for all internal and external stakeholders.	
	Expected deliverables: • A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. • Organization personnel contract forms (signed copy). • Cybersecurity Function Personnel Contract Forms (signed copy).	
	1-9-3-2	Screening or vetting candidates of cybersecurity and critical/privileged positions.
	Control implementation guidelines: • Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. • Work with relevant departments to ensure Screening or Vetting of all employees in cybersecurity functions.	

		• Work with relevant departments to ensure the Screening or Vetting of all employees working in technical functions with privileged access, including database management personnel, firewall management personnel, and systems management personnel. • Include such requirements in the organization's HR procedures to ensure compliance with cybersecurity requirements for all internal and external stakeholders.
		Expected deliverables : • A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. • Evidence that the Screening or Vetting of employees working in cybersecurity functions and technical functions with privileged access was performed, including but not limited to: ○ An official document from the relevant authorities indicating the performance of Screening or Vetting.
1-9-4		The personnel cybersecurity requirements during employment must include at least the following:
	1-9-4-1	Cybersecurity awareness (during on-boarding and during employment).
		Control implementation guidelines: • Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. • Work with relevant departments to provide cybersecurity awareness at the beginning and during work through the organization's approved communication channels. • Include such requirements in the organization's HR procedures to ensure compliance with cybersecurity requirements for all internal and external stakeholders. • Support the organization's policy by the Executive Management .This must be done through the approval of the representative.
		Expected deliverables: • A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control.

	• Documents that confirm the provision of awareness content to employees in cybersecurity before work at the organization and providing them with access through e-mails, workshops, or any other means, including but not limited to: ○ Review cybersecurity awareness messages shared with employees through emails ○ Review of content presented in the workshop ○ Review the cybersecurity awareness plan	
	1-9-4-2	Implementation of and compliance with the cybersecurity requirements as per the organizational cybersecurity policies and procedures.
	Control implementation guidelines: • Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. • Inform all employees of the organization and obtain their approval on the cybersecurity policies and procedures, in order to educate the organization's employees of the importance of their role in implementing the cybersecurity requirements. • Include personnel cybersecurity requirements in the organization's HR procedures to ensure compliance with cybersecurity requirements for all internal and external stakeholders.	
	Expected deliverables : • A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. • An acknowledgment form for approving cybersecurity policies by one of the organization's employees (signed copy).	
1-9-5	Personnel access to information and technology assets must be reviewed and removed immediately upon termination/separation.	
	Control implementation guidelines • Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. • Review access of employees and revoke it immediately after the end/termination of their professional service at the organization, which may include the following:	

	○ Define professional end-of-service or termination procedures covering cybersecurity requirements. ○ Ensure the return of all organization's assets and revoke employees' access rights immediately upon the end of their relationship with the organization.
	Expected deliverables: ● A discharge form with a signed and approved sample for the implementation of the procedures.
1-9-6	Personnel cybersecurity requirements must be reviewed periodically.
	Control implementation guidelines: ● Review and update the cybersecurity policy and requirements for personnel in the organization periodically according to a documented and approved plan for review and based on a planned interval (e.g., review must be conducted annually) or in the event of changes in related laws and regulations .Document the review and changes to the cybersecurity requirements for personnel in the organization and approve them by the head of the organization or his/her deputy .
	Expected deliverables: ● An approved document that sets the policy's review schedule. ● Policy indicating that it is up to date and the changes to the cybersecurity requirements for personnel have been documented and approved by the head of the organization or his/her deputy. ● Formal approval by the head of the organization or his/her deputy on the updated policy (e.g., via the organization's official e-mail, paper or electronic signature).

1-10	Cybersecurity Awareness and Training Program
Objective	To ensure that personnel are aware of their cybersecurity responsibilities and have the essential cybersecurity awareness. It is also to ensure that personnel are provided with the required cybersecurity training, skills and credentials needed to accomplish

	their cybersecurity responsibilities and to protect the organization's information and technology assets.
Controls	
1-10-1	A cybersecurity awareness program must be developed and approved. The program must be conducted periodically through multiple channels to strengthen the awareness about cybersecurity, cyber threats and risks, and to build a positive cybersecurity awareness culture.
	Relevant cybersecurity tools: ● Awareness program template. ● Awareness content template for all employees. ● Awareness content form for supervisory and executive positions. ● Information and Technology Assets Operators Awareness Content Form. Control implementation guidelines: ● Develop and approve cybersecurity awareness program and plan in the organization through multiple channels periodically, including but not limited to: ○ Awareness emails. ○ Cybersecurity awareness workshops. ○ Distribution of awareness publications. ○ Awareness presentation through billboards. ○ Launch of a cybersecurity training and awareness platform. ● The program may include a plan to coordinate with the Human Resources department, the Media and Internal Communications department, and the cybersecurity function to raise awareness of cybersecurity, its threats and risks, and build a positive cybersecurity culture. ● The organization's program must be supported by the Executive Management. This must be done through the approval of the representative.
	Expected deliverables: ● The awareness program document approved by the organization.
1-10-2	The cybersecurity awareness program must be implemented.
	Control implementation guidelines:

		● Implement the approved cybersecurity awareness and training program in coordination with the cybersecurity awareness and training department, which may include the following: ○ Implement the approved cybersecurity awareness program in the organization, including but not limited to sending awareness emails or conducting cybersecurity awareness workshops. ○ Evaluate cybersecurity awareness of all personnel and define and address cybersecurity weaknesses.
		Expected deliverables : ● Action plan to implement the cybersecurity awareness program adopted by the organization. ● Awareness programs to be shared with employees. ● List of beneficiaries of awareness programs.
1-10-3		The cybersecurity awareness program must cover the latest cyber threats and how to protect against them, and must include at least the following subjects:
	1-10-3-1	Secure handling of email services, especially phishing emails.
		Control implementation guidelines: ● Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. ● Provide cybersecurity awareness programs that cover the safe handling of e-mail services, especially with emails and social engineering.
		Expected deliverables : ● A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. ● Action plan to implement the cybersecurity awareness program adopted by the organization. ● Evidence of providing awareness content for the safe handling of e-mail services, especially with phishing emails.
	1-10-3-2	Secure handling of mobile devices and storage media.
		Control implementation guidelines: ● Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.

		• Provide cybersecurity awareness programs to cover the safe handling of mobile devices and storage media.
		Expected deliverables : • A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. • Action plan to implement the cybersecurity awareness program adopted by the organization. • Evidence that awareness content is provided for the safe handling of mobile devices and storage media.
	1-10-3-3	Secure Internet browsing.
		Control implementation guidelines: • Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. • Provide cybersecurity awareness programs that cover the safe handling of internet browsing services, especially dealing with suspicious websites such as phantom phishing sites and suspicious websites and links.
		Expected deliverables : • A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. • Action plan to implement the cybersecurity awareness program adopted by the organization. • Evidence that awareness content is provided for the secure handling of internet browsing services.
	1-10-3-4	Secure use of social media.
		Control implementation guidelines: • Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. • Provide cybersecurity awareness programs that cover the safe handling of social media.
		Expected deliverables :

		• A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. • Action plan to implement the cybersecurity awareness program adopted by the organization. • Evidence that awareness content is provided for safe handling of social media.
1-10-4		Essential and customized (i.e., tailored to job functions as it relates to cybersecurity) training and access to professional skillsets must be made available to personnel working directly on tasks related to cybersecurity including:
	1-10-4-1	Cybersecurity function’s personnel.
		Control implementation guidelines: • Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. • Develop and implement an approved cybersecurity training plan for employees of the cybersecurity function in coordination with the training department in the organization, which may include the following: o Implement the cybersecurity training plan for the organization in coordination with the Training and Employee Development Department. o Assist in the establishment of cybersecurity career paths to allow career progression, deliberate development, and growth within and between cybersecurity career fields. o Support in advocating for adequate funding for cybersecurity training resources, to include both internal and industry-provided courses, instructors, and related materials.
		Expected deliverables : • A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. • Approved training plans and programs for the cybersecurity department employees at the organization. • Cybersecurity training certificates.
	1-10-4-2	Personnel working on software/application development. and information and technology assets operations.
		Control implementation guidelines:

- Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.
- Develop and implement an approved training plan in the field of secure program and application development, and the safe management of the organization's information and technology assets for relevant employees in coordination with the training department in the organization. This may include the following:
    - Training plan to develop programs, applications and employees operating the organization's information and technology assets must be implemented in coordination with Training and Employee Development Department.
    - Assistance in defining career paths for software and application developers and the employees operating the organization's information and technology assets must be provided to allow for professional growth and upgrades in professional areas related to software development.
- Provide support in requesting the adequate funding of training resources related to the development of programs, applications and employees operating the organization's information and technology assets, including internal and sector-related courses, trainers and related materials.

Expected deliverables :

- A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control.
- Approved training programs for employees involved in the development of programs, applications, and employees operating the organization's information and technology assets.
- Training certificates in software and application development.

1-10-4-3	Executive and supervisory positions.

Control implementation guidelines:

- Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.
- Develop and implement an approved cybersecurity training plan for employees of the cybersecurity Supervisory and executive functions in coordination with the training department in the organization, which may include the following:

	○ Awareness of the importance of cybersecurity, developing the cybersecurity culture and the key risks and threats, such as phishing emails for supervisory and executive positions (Whale phishing) must be conducted. ○ Training plan for supervisory and executive positions in the organization must be implemented in coordination with the Training and Employee Development Department. ○ Assistance in the establishment of cybersecurity career paths to allow career progression, deliberate development, and growth within and between cybersecurity career fields must be provided. ○ Support in advocating for adequate funding for cybersecurity training resources, including both internal and industry-provided courses, instructors, and related materials must be provided.
	Expected deliverables : • A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. • Security training programs dedicated to supervisory and executive positions in the organization. • Training certificates in supervisory and executive positions.
1-10-5	The implementation of the cybersecurity awareness program must be reviewed periodically.
	Control implementation guidelines: • Review the cybersecurity requirements of cybersecurity awareness and training programs by conducting a periodic assessment (according to a documented and approved plan for review and based on a planned interval (e.g., quarterly)) to implement awareness and training plans by the Cybersecurity function and in cooperation with relevant departments (such as the Awareness and Training Department). • Conduct application review through traditional channels (e.g., email) or automated channels using a compliance management system .The organization may develop a review plan explaining the cybersecurity requirements implementation review schedule for cybersecurity awareness and training programs.
	Expected deliverables:

	• Results of cybersecurity awareness program implementation review in the organization. • A document that defines the cybersecurity awareness and training implementation review cycle (Compliance Assessment Schedule). • Compliance assessment report that shows the assessment of the implementation of cybersecurity requirements for cybersecurity awareness and training programs.

2 Cybersecurity Defense

2-1	Asset Management
Objective	To ensure that the organization has an accurate and detailed inventory of information and technology assets in order to support the organization's cybersecurity and operational requirements to maintain the confidentiality, integrity and availability of information and technology assets.
Controls	
2-1-1	Cybersecurity requirements for managing information and technology assets must be defined, documented and approved.
	Relevant cybersecurity tools: • Asset Management Policy Template. Control implementation guidelines: • Develop and document cybersecurity requirements for information and technology assets management in the organization, including the following: ○ The cybersecurity requirements for types and description of information and technology asset management must be identified. ○ Information and technology asset classification levels requirements in terms of data included and processed, and the criticality of the technology asset from a cybersecurity perspective must be defined. ○ Requirements for the defined stages of the information and technology assets life cycle (including but not limited to: preservation, processing, storage, destruction, etc.) must be defined. ○ Roles and responsibilities requirements for the ownership and management of information and technology assets must be defined. • Support the organization's developed requirements by the Executive Management .This must be done through the approval of the representative.
	Expected deliverables:

	● Information asset management cybersecurity requirements (in form of policy or standard) approved by the organization (e.g., electronic copy or official hard copy). ● Formal approval by the head of the organization or his/her deputy on the requirements (e.g., via the organization's official e-mail, paper or electronic signature).
2-1-2	The cybersecurity requirements for managing information and technology assets must be implemented.
	Control implementation guidelines: ● All cybersecurity requirements to manage information and technology assets of the organization, which may include the following: ○ Approved cybersecurity requirements for the management of information and technology assets in the organization must be implemented, including but not limited to, classifying all information and technology assets of the organization, documenting and approving them in an approved and official document (e.g., a documented record for the management of the organization's information and technology assets), as well as encoding all information and technology assets of the organization based on the approved classification of the organization's information and technology assets. ○ Specific procedures for dealing with assets based on their classification and in accordance with the relevant laws and regulations must be established.
	Expected deliverables: ● Documents that confirm the implementation of cybersecurity requirements related to information and technology asset management as documented in the policy. ● An action plan to implement the cybersecurity requirements of information and technology assets management. ● A documented and up-to-date record of all information and technology assets (e.g., Excel spreadsheet or displayed through automated means using solutions such as CMDB) must be provided . ● Specific procedures for dealing with assets based on their classification and in accordance with the relevant laws and regulations.

2-1-3	Acceptable use policy of information and technology assets must be defined, documented and approved.
	Relevant cybersecurity tools: • Asset Acceptable Use Policy Template. Control implementation guidelines: • Develop acceptable use policy for information and technology assets of the organization, which may include the following: ○ Set of specific regulations for access to and use of assets. ○ A set of clear examples of unacceptable use. ○ Consequences if defined rules of acceptable use of assets are breached. ○ The method used to monitor adherence to the defined rules of acceptable use of the organization's information and technology assets . • Acceptable use policy of the organization's information and technology assets must be communicated to all employees and stakeholders in the organization through, including but not limited to the official email or through the organization's website . • Support the organization's policy by the Executive Management .This must be done through the approval of the organization head or his/ her deputy.
	Expected deliverables: • Approved policy that covers the requirements for acceptable use of the organization's information and technology assets (e.g., electronic copy or official hard copy) . • Acceptable use policy of the organization's information and technology assets must be communicated to all employees and stakeholders in the organization through, including but not limited to the official email or through the organization's website. Evidence that all employees and stakeholders are aware and informed must be provided . • Formal approval by the head of the organization or his/her deputy on the policy (e.g., via the organization's official e-mail, paper or electronic signature).
2-1-4	Acceptable use policy of information and technology assets must be implemented.
	Control implementation guidelines:

	• Cybersecurity policy for the acceptable use policy of the information and technology assets of the organization must be implemented, including the following: ○ Requirements for the acceptable use of information and technology assets by the organization must be implemented, including but not limited to: requesting each employee view and approve the Acceptable Use Policy of information and technology assets. ○ These requirements must be communicated through the organization's approved communication channels to educate the organization's internal and external stakeholders to implement these requirements. ○ Appropriate mechanisms and techniques must be developed to monitor violations of the Acceptable Use Policy requirements and warn of disciplinary actions in the event of violations.
	Expected deliverables: • An action plan to implement the acceptable use requirements of information and technology assets of the organization. • Evidence of communicating these requirements through the communication channels approved by the organization . • A completed and approved form that clarifies the approval of the Acceptable Use Policy by all organization's employees (e.g., scanned physical copy, digital platform, or official hard copy).
2-1-5	Information and technology assets must be classified, labeled and handled as per related law and regulatory requirements.
	Control implementation guidelines: • Define and document the requirements of this ECC in the cybersecurity requirements of information and technology assets management at the organization and must be approved by the representative. • Work with the concerned departments to identify all information and technology assets, including (but not limited to) : ○ Infrastructure (e.g., servers) ○ Applications and services ○ Networks (e.g., router) ○ Workstations

	○ Peripherals (e.g., printers) ○ Operating systems (if any) • Document all information and technology assets in a single register with characteristics such as (asset name, description, owner and criticality). • Work with asset owners to identify, document and approve asset classification in the register in accordance with the relevant laws and regulations. • Work with the concerned departments to ensure the coding of assets based on their classification, including but not limited to labelling the assets or automatically coding them through modern systems. • Work with the concerned departments to ensure that assets are handled according to the defined and approved classification level and based on the approved procedures for dealing with each asset.
	Expected deliverables: • A cybersecurity policy that covers the information and technology asset management requirements of the organization (e.g., electronic copy or official hard copy) . • Formal approval by the head of the organization or his/her deputy on the policy (e.g., via the organization's official e-mail, paper or electronic signature). • A document that outlines the method and system of asset classification, coding and requirements. • An action plan to implement the requirements of classification and coding of information and technology assets (Labelling) in accordance with the relevant laws and regulations. • An up-to-date register that includes all information and technology assets, indicating the level of classification for each asset (e.g., Excel or through automated means using technical solutions such as CMDB). • Evidence that outlines that the organization's assets are classified according to the defined and approved classification level. • Evidence that outlines that the organization's assets have been labelled according to the classification level defined and based on but not limited to the coding labels that demonstrate the coding of all assets within the organization. • Evidence of the implementation of controls on the organization's assets in accordance with their classification level, including but not limited to the procedures followed when dealing with each asset based on its classification.

2-1-6	The cybersecurity requirements for managing information and technology assets must be reviewed periodically.
	Control implementation guidelines: • Review and update cybersecurity requirements for information and technology assets management in the organization periodically according to a documented and approved plan for review and based on a planned interval or in the event of changes in relevant laws and regulations. • Document and approve review and changes to the organization's cybersecurity requirements of the information and technology assets management by the head of the organization or his/ her deputy .
	Expected deliverables: • Results of information and technology assets management cybersecurity requirements implementation review in the organization. • A document that defines the cybersecurity requirements implementation review cycle to manage the information and technology assets of the organization (Compliance Assessment Schedule). • Log of updates and changes to the information and technology asset management cybersecurity requirements. • Compliance assessment report that outlines the results of the cybersecurity requirements implementation assessment for information and technology asset management. • An approved document that sets the policy's review schedule. • Policy indicating that it has been reviewed and updated, and that changes have been documented and approved by the head of the organization or his/her deputy . • Formal approval by the head of the organization or his/her deputy on the updated policy (e.g., via the organization's official e-mail, paper or electronic signature).
2-2	Identity and Access Management

Objective	To ensure the secure and restricted logical access to information and technology assets in order to prevent unauthorized access and allow only authorized access for users which are necessary to accomplish assigned tasks.
Controls	
2-2-1	Cybersecurity requirements for identity and access management must be defined, documented and approved.
	Relevant cybersecurity tools: ● Identity and Access Management Policy Template. Control implementation guidelines: ● Develop and document cybersecurity policy for identity and access management in the organization, which may include, but is not limited to: ○ Grant access, including: - Access to user accounts. - Privileged Access to accounts. - Remote access to the organization's networks and systems. - Define and approve the authority of each type of users. ○ Revoke and Change Access. ○ Review Identity and Access. ○ Manage passwords. ● Support the organization's policy by the Executive Management .This must be done through the approval of the representative.
	Expected deliverables: ● Cybersecurity policy that covers Identity and Access Management (e.g., electronic copy or official hard copy). ● Formal approval by the head of the organization or his/her deputy on the policy (e.g., via the organization's official e-mail, paper or electronic signature).
2-2-2	The cybersecurity requirements for identity and access management must be implemented.

	Control implementation guidelines: • All cybersecurity requirements must be implemented for the organization's approved identity and access management procedures. It is also recommended that the identity and access management cover the following, but not limited to: ○ User Authentication based on user login management. ○ Password management based on the organization's password policy. ○ User authorization management based on a need-to-know and Need-to-use basis. ○ User authorization management based on least privilege and Segregation of Duties. ○ Remote access management to the organization's networks. ○ Access Cancellation and Update Management.
	Expected deliverables: • Action plan for cybersecurity requirements for Identity and Access Management. • Evidence that the identity and access management controls must be implemented on all technical and information assets in the organization, including but not limited to, the configuration of all technical information systems in line with the cybersecurity controls and requirements of identity and access management.
2-2-3	The cybersecurity requirements for identity and access management must include at least the following
	2-2-3-1 User authentication based on username and password.
	Control implementation guidelines: • Define and document the requirements of this ECC in the cybersecurity requirements of identity and access management at the organization and must be approved by the representative. • Ensure all employees have a unique identifier, which may be a job number, employee name, or other naming mechanisms to ensure that usernames are unique.

	• Prepare password standard controls taking into consideration best practices, including but not limited to: ○ Expiration Period ○ Complexity ○ Lockout ○ Activation ○ Password History ○ A secure mechanism to create a password and provide it to the user
	Expected deliverables: • Cybersecurity policy that covers Identity and Access Management (e.g., electronic copy or official hard copy). • Password management policy in the organization (e.g., electronic copy or official hard copy). • Formal approval by the head of the organization or system owner or his/her deputy on such policies (e.g., via the organization's official e-mail, paper or electronic signature). • Evidence that the identity and access management controls must be implemented on all technical and information assets in the organization, including but not limited to, the configuration of all technical information systems in line with the cybersecurity controls and requirements of identity and access management.
	2-2-3-2 Multi-factor authentication for remote access.
	Control implementation guidelines: • Define and document the requirements of this ECC in the cybersecurity requirements of identity and access management at the organization and must be approved by the representative. • Develop procedures for remote access with Multi-Factor Authentication. • Provide appropriate and advanced multi-factor authentication techniques and link them to remote access technologies (e.g., VPN) must be ensured. • Use two of the following authentication elements to apply multi-factor authentication: ○ Something you know, e.g., using the password.

- Something you have, e.g., using One time password through SMS or applications.
- Something you are, e.g., using biometrics such as fingerprint or face recognition.

Expected deliverables:

- Cybersecurity policy that covers Identity and Access Management (e.g., electronic copy or official hard copy).
- Formal approval by the head of the organization or his/her deputy on the policy (e.g., via the organization's official e-mail, paper or electronic signature).
- Evidence that outlines the implementation of multi-factor authentication requirements to remote access, including but not limited to a screenshot showing the configuration of systems to ensure that the multi-factor authentication request for remote access is verified.

2-2-3-3	User authorization based on identity and access control principles: Need-to-Know and Need-to-Use, Least Privilege and Segregation of Duties.

Control implementation guidelines:

- Define and document the requirements of this ECC in the cybersecurity requirements of identity and access management at the organization and must be approved by the representative.
- Define basic authorizations for all organization's employees, such as the authority to use email, internal portal, and human resources system.
- Define and document the requirements of this ECC in the cybersecurity requirements of identity and access management at the organization and must be approved by the representative.
- Manage user authorization to all information and technology assets in the organization via an automated centralized access control system such as Active Directory.
- Develop and adopt specific procedures for granting powers to employees in the organization, as there are requirements to request authority, including:
    - Applicant information (identity)
    - Details of the authority in question (explanation of authority and assets involved)
    - Description of Business Requirements for authorization

<table>
<tr><td rowspan="4"></td><td colspan="2">○ Time required for authorization
○ Approvals required (e.g., Line Manager approval)</td></tr>
<tr><td colspan="2">Expected deliverables:
• Cybersecurity policy that covers Identity and Access Management (e.g., electronic copy or official hard copy).
• Evidence that outlines the implementation of User authorization management requirements, including but not limited to a screenshot showing the configuration of systems to ensure the implementation of user authorization management based on a Need to Know and Need to Use basis and least privilege and Segregation of Duties.</td></tr>
<tr><td>2-2-3-4</td><td>Privileged access management.</td></tr>
<tr><td colspan="2">Control implementation guidelines:
• Define and document the requirements of this ECC in the cybersecurity requirements of identity and access management at the organization and must be approved by the representative.
• Define privileged access at the level of infrastructure, networks, and applications in the organization.
• Identify Personnel with Privileged Access.
• Develop Privileged Access Management procedures by the organization, taking into account the following:
○ Privileged accounts must not be used for normal daily tasks, and a normal user account must be used for this purpose.
○ Privileged accounts must not be used for internet access.
○ Privileged accounts must not be used for email access.
○ Privileged accounts must not be restricted for remote access .
○ Default accounts must be disabled/ deleted.
○ Workstation protection system must be installed and updated on the workstation that will be used to access privileged accounts.
○ Secure versions of operating systems used in the organization must be built and prepared in a secure manner.
○ Protection programs must be installed and unused services must be disabled .These copies must be used to configure desktops and servers.</td></tr>
</table>

	● Define modern and advanced technologies and mechanisms for the Privileged Access Management. ● Grant privileged access based on functional duties after obtaining the necessary approvals, taking into consideration the principle of segregation of duties. ● Continuously monitor cybersecurity event logs for privileged accounts.	
	Expected deliverables: ● Privileged Access Management Policy in the organization (e.g., electronic copy or official hard copy). ● Formal approval by the head of the organization or his/her deputy on the policy (e.g., via the organization's official e-mail, paper or electronic signature). ● Evidence that outlines the implementation of privileged access management requirements, including but not limited to a screenshot showing the configuration of systems to ensure that administrators are granted privileged access.	
	2-2-3-5	Periodic review of users' identities and access rights.
	Control implementation guidelines: ● Define and document the requirements of this ECC in the cybersecurity requirements of identity and access management at the organization and must be approved by the representative. ● Define privileged access at the level of infrastructure, networks, and applications in the organization. ● Identify Personnel with Privileged Access. ● Develop a plan for periodic review of identity and access as follows: ○ Across all applications in the organization ○ Network level ○ Infrastructure and servers level ○ Workstations level ● Review authorities in collaboration with IT department and application managers to revoke access in the following cases (e.g., limited to): ○ Access has not been used for a long period of time (e.g., over 3 months) ○ Access causes conflict of interest ○ The employee's need for access has not been confirmed by his manager	

	○ Expiry of the access period
	Expected deliverables: ● Privileged Access Management Policy in the organization (e.g., electronic copy or official hard copy). ● Formal approval by the head of the organization or his/her deputy on the policy (e.g., via the organization's official e-mail, paper or electronic signature). ● Evidence that outlines the implementation of periodic review requirements of identity and access, e.g., an official and approved document that clarifies the periodic review of the identity and access.
2-2-4	The Implementation of the cybersecurity requirements for identity and access management must be reviewed periodically.
	Control implementation guidelines: ● Review the cybersecurity requirements of identity and access management by conducting a periodic assessment (according to a documented and approved plan for review, and based on a planned interval "e.g., quarterly") to implement identity and access management requirements by the Cybersecurity function and in cooperation with relevant departments (such as IT Department). ● Review and update cybersecurity requirements for identity and access management in the organization periodically according to a documented and approved plan for review and based on a planned interval or in the event of changes in relevant laws and regulations. ● Document the review and changes to the cybersecurity requirements for identity and access management in the organization and approve them by the head of the organization or his/her deputy .
	Expected deliverables: ● Results of identity and access management requirements implementation review in the organization. ● A document that defines the cybersecurity requirements implementation review cycle for identity and access management at the organization (Compliance Assessment Schedule).

	• Compliance assessment report that outlines the assessment of the implementation of cybersecurity requirements for identity and access management in the organization. • An approved document that sets the policy's review schedule. • Policy indicating that it has been reviewed and updated, and that changes have been documented and approved by the head of the organization or his/her deputy . • Formal approval by the head of the organization or his/her deputy on the updated policy (e.g., via the organization's official e-mail, paper or electronic signature).

2-3	Information System and Information Processing Facilities Protection
Objective	To ensure the protection of information systems and information processing facilities (including workstations and infrastructures) against cyber risks.
Controls	
2-3-1	Cybersecurity requirements for protecting information systems and information processing facilities must be defined, documented and approved.
	Relevant cybersecurity tools: • Database Security Policy Template. Control implementation guidelines: • Develop and document cybersecurity policy for Information System and Processing Facilities Protection in the organization, including the following: ○ Modern and advanced protection techniques and mechanisms, providing them and ensuring their reliability. ○ Malware Protection Solution Configuration. ○ Scope of devices to be protected, including all workstations, critical systems in the organization, etc.

	○ Secure copies of the operating systems used in the organization must be built and prepared in a secure manner, protection programs must be installed, and unused services must be disabled. Such copied must be used in the configuration of desktops and servers. ○ Workstations and systems in the organization must be periodically scanned against malware. ○ Use of external storage media and its security must be restricted. ○ Patch management for systems, applications and devices. ○ Central sources of time synchronization in the organization must be defined to be from a reliable source. ● Support the organization's policy by the Executive Management .This must be done through the approval of the organization head or his/ her deputy.
	Expected deliverables: ● Cybersecurity policy that covers the requirements of Information System and Processing Facilities Protection at the organization (e.g., electronic copy or official hard copy). ● Formal approval by the head of the organization or his/her deputy on the policy (e.g., via the organization's official e-mail, paper or electronic signature). ● Secure Configuration and Hardening Policy Template ● Server Security Policy Template ● Malware Protection Policy Template ● Storage Media Policy Template ● Patch Management Policy Template
2-3-2	The cybersecurity requirements for protecting information systems and information processing facilities must be implemented.
	Control implementation guidelines: ● Implement all cybersecurity requirements for Information System and Processing Facilities Protection in the organization. This may include the following: ○ Modern and advanced protection techniques and mechanisms' availability and reliability must be ensured. ○ Scope of devices to be protected and reviewed periodically must be ensured.

<table>
<tr><td></td><td colspan="2">○ Use of external storage media and its security must be restricted.
○ Patches throughout the organization's devices, systems, and applications must be implemented.
○ Central Clock Synchronization and from a reliable source must be implemented.</td></tr>
<tr><td></td><td colspan="2">Expected deliverables:
• Documents that confirm the implementation of cybersecurity requirements related to information systems and processing facilities as documented in the policy.
• An up-to-date list of the organization's virus protection systems and the extent of their download.
• Restrict the use of external storage media and procedures for approving their use.
• Evidence that the scope of patches covers all devices, systems and applications.
• Evidence that the organization uses a central server and a reliable source for timing synchronization.</td></tr>
<tr><td>2-3-3</td><td colspan="2">The cybersecurity requirements for protecting information systems and information processing facilities must include at least the following:</td></tr>
<tr><td></td><td>2-3-3-1</td><td>Advanced, up-to-date and secure management of malware and virus protection on servers and workstations.</td></tr>
<tr><td></td><td colspan="2">Control implementation guidelines:
• Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.
• Provide anti-virus, suspicious programs, and malware protection techniques and mechanisms, including the following :
○ Continuously ensure that the technologies used are current and advanced and contain protection against advanced persistent threat (APT).
○ Determine the domain of the assets on which the protection system will be installed and identify and update their status.
○ Install the protection system throughout the workstations, systems and servers of the organization.</td></tr>
</table>

  - Review the protection system periodically to ensure that the scope of the protection system is comprehensive for all workstations, systems, and servers of the organization through the protection system's control unit.
  - Develop and implement a remediation action plan (when needed) to install the protection system on all devices while taking action against devices and systems where it is frequently observed that the modern and advanced protection system is not installed.
  - Follow up on the protection system periodically to ensure updates are installed and released on all workstations, systems and servers of the organization.

Expected deliverables:

- Documents indicating the identification and documentation of the requirements of this ECC in the policies or procedures of the organization approved by the representative.
- List of antivirus systems and evidence of protection against APT (including but not limited to a screenshot or direct example from the APT Monitoring page of the protection system).
- Reports or evidence of installing the protection technologies across all workstations, systems and servers of the organization.
- Reports or evidence of following-up the scope of installing and periodic updating of these technologies.

2-3-3-2	Restricted use and secure handling of external storage media.

Control implementation guidelines:

- Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.
- Restrict the use of external storage media by :
  - Groups in the privileged access management system must be created according to authority so that the use of external storage media is automatically not activated on all workstations, the organization's systems, and servers .
  - Documented procedures must be defined to provide approval for the use of external storage media (including but not limited to: requesting

approvals via e-mail, paper, or through an internal system). Such procedures include :

- Reason for requesting approval for use.
- Use start and end date.
- Mechanism for handling data stored in storage media so that it is checked prior to use and data is erased after completion.

Expected deliverables:

- A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control.
- Report or evidence indicating the restriction of using external storage media (including but not limited to a screenshot or direct example from access management system showing the vigor restriction of the use of external storage media on workstations and servers).
- Approval procedures for the use of storage media for part of the approved devices.

2-3-3-3	Patch management for information systems, software and devices.

Control implementation guidelines

- Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.
- Define procedures for patch management for systems, devices and applications, which include:
  - The scope of systems where patches are implemented must be defined to include:
    - Workstations
    - Operating Systems
    - Network Devices
    - Databases
    - Applications
  - Time period required to implement patches must be defined according to the quality of operating system, the system criticality, applicable patches, and importance of patches.

	○ Patches procedures must be included in change management methodology or change management must be included into patch management policy. ○ Change management approval must be included as part of patch approval form for all systems, devices and applications, including but not limited to: requesting approvals via e-mail, paper, or through an internal system. ○ Patches must be implemented to the defined scope after obtaining the necessary approval. ○ Implementation of patches must be continuously reviewed to ensure that all necessary patches are implemented to all devices, systems, and applications. ○ Required patches must be periodically monitored to ensure patches by, but not limited to, the protection system, patch management system, and vulnerability alerts sent by email.	
	Expected deliverables: • A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. • Evidence indicating the inclusion of change management in patches (including but not limited to: including patches in change management methodology or enforcing change management by including it in the requirements of Patch Management). • Approval procedures indicate that change management approval is required for patches. • Reports or evidence that the scope of patches covers all devices, systems and applications. • Reports or evidence that the patches are performed according to the period specified in the procedures (including but not limited to: a screenshot or direct example that displays the date and scope for several samples of patches approved by e-mail, internal system or paper that are performed in advance to include all the organization's devices, systems and applications periodically).	
	2-3-3-4	Centralized clock synchronization with an accurate and trusted source (e.g., Saudi Standard controls, Metrology and Quality Organization (SASO)).
	Control implementation guidelines	

	• Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. • Perform time synchronization through the organization's central server NTP. • Configure central server time to synchronize with, but not limited to, one of the following reliable sources: ○ Saudi Standard controls, Metrology and Quality Organization (time.saso.gov.sa). ○ King Abdulaziz City for Science and Technology (KACST)(time.isu.net.sa).
	Expected deliverables: • A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. • Evidence that the organization uses a central server to synchronize timing (including but not limited to: a screenshot or direct example of the presence of this server in the network with all server details) • Evidence of using a reliable and accurate source (including but not limited to: a screenshot or direct example of the configuration of this server that proves the use of the SASO source or others).
2-3-4	The cybersecurity requirements for protecting information systems and information processing facilities must be reviewed periodically.
	Control implementation guidelines • Review the cybersecurity requirements for Information System and Processing Facilities Protection in the organization periodically according to a documented and approved plan for review and based on a planned interval (e.g., periodic review must be conducted annually). • Document the review and changes to the cybersecurity requirements for Information System and Processing Facilities Protection in the organization and approve them by the head of the organization or his/her deputy.
	Expected deliverables: • An approved document that defines the review schedule for the requirements document.

	- Evidence that the periodic review of security requirements is performed to protect information systems and processing facilities in the organization. - Formal approval by the head of the organization or his/her deputy on the updated requirements (e.g., via the organization's official e-mail, paper or electronic signature).

2-4	Email Protection
Objective	To ensure the protection of organization’s email service from cyber risks.
Controls	
2-4-1	Cybersecurity requirements for protecting email service must be defined, documented and approved.
	Relevant cybersecurity tools: - Email Security Policy Template. Control implementation guidelines - Develop and document cybersecurity policy for email protection in the organization, including the following: ○ Modern and advanced protection techniques and mechanisms' availability and reliability must be ensured. ○ Email Protection Solution Configuration Requirements. ○ Email roles and responsibilities requirements for public and joint accounts. ○ Size of incoming and outgoing email attachments and the capacity of the mailbox for each user. ○ Secure design requirements for email infrastructure. - Support the organization's policy by the Executive Management. This must be done through the approval of the organization head or his/ her deputy.
	Expected deliverables: - Email security policy and standard document approved by the organization (e.g., electronic copy or official hard copy).

	• Formal approval by the head of the organization or his/her deputy on the policy (e.g., via the organization's official e-mail, paper or electronic signature).
2-4-2	The cybersecurity requirements for email service must be implemented.
	Control implementation guidelines • Email protection cybersecurity requirements in the organization must be implemented, including: o Approved cybersecurity requirements must be implemented to protect the organization's email, including but not limited to the use of appropriate and advanced technologies to analyze and filter emails. o Advanced technologies must be used to protect the organization's email from phishing emails and spam messages, including but not limited to the presence of an official and effective subscription with email protection service providers. o Email access must be through an intermediary, including but not limited to Load balancer.
	Expected deliverables: • An action plan to implement Email protection cybersecurity requirements at the organization. • Email protection controls in the organization must be implemented, including but not limited to: o Advanced email protection and filtering technologies must be used by the organization to block suspicious messages, such as spam and phishing emails. o Antivirus solutions must be configured to email servers in order to scan all inbound and outbound emails. o Email field of the organization must be documented by using necessary means, such as the Sender Policy Framework, and reliability of incoming mail fields must be ensured through modern technologies such as (Incoming Message DMARC verification).
2-4-3	The cybersecurity requirements for protecting the email service must include at the least the following:

<table>
<tr><td rowspan="6"></td><td>2-4-3-1</td><td>Analyzing and filtering email messages (specifically phishing emails and spam) using advanced and up-to-date email protection techniques.</td></tr>
<tr><td colspan="2">Control implementation guidelines
<ul>
<li>Define and document the requirements of this ECC in the cybersecurity requirements of email security at the organization and must be approved by the representative.</li>
<li>Define and provide advanced technologies to analyze and filter the organization's emails.</li>
<li>Activate analysis and filtering features in the email protection system through the dashboard.</li>
<li>Periodically review the list of suspicious emails such as phishing messages, spam messages, etc. through the system by the specialized team to follow up email protection.</li>
<li>Add new intrusion indicators related to email in the protection system on an ongoing basis.</li>
</ul></td></tr>
<tr><td colspan="2">Expected deliverables:
<ul>
<li>A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control.</li>
<li>Screenshot or direct example showing subscription and use of modern and advanced technologies to analyze and filter emails in the organization.</li>
<li>Screenshot or direct example of the configuration of email to prove the feature of analyzing and filtering emails, including phishing emails and spam emails.</li>
</ul></td></tr>
<tr><td>2-4-3-2</td><td>Multi-factor authentication for remote and webmail access to email service.</td></tr>
<tr><td colspan="2">Control implementation guidelines
<ul>
<li>Define and document the requirements of this ECC in the cybersecurity requirements of email security at the organization and must be approved by the representative.</li>
<li>Activate multi-factor authentication for remote access and organization's webmail access by, but not limited to, one of the following methods:
<ul>
<li>Text messages linked to the email user's number must be used.</li>
<li>Advanced and reliable applications for multi-factor authentication.</li>
</ul></li>
</ul></td></tr>
</table>

	○ Mobile device management applications must be used to allow users' devices (as another element of access) to email for protocols (such as EWS, outlook anywhere protocols) that do not support text messages or applications that provide verification code.	
	Expected deliverables: ● A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. ● Screenshot or direct example of email configuration to prove the activation of multi-factor authentication to access via the organization's email webmail. ● Screenshot or direct example that proves the use of advanced and reliable technologies for multi-factor authentication.	
	2-4-3-3	Email archiving and backup.
	Control implementation guidelines ● Define and document the requirements of this ECC in the cybersecurity requirements of email security at the organization and must be approved by the representative. ● Define technologies compatible with the organization's technical systems and infrastructure to backup and archive the organization's email. ● Define retention period for backup and archiving of the organization's email. ● Perform backup at the level of the organization's email servers. ● Activate archiving of all email boxes of the organization.	
	Expected deliverables: ● A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. ● Screenshot or direct example showing subscription and use of modern and advanced technologies for backup and archiving of email, as well as the approved capacity and duration. ● Backup reports for the organization's email servers. ● Screenshot or direct example that shows the activation of the email boxes archiving feature.	

2-4-3-4 Secure management and protection against Advanced Persistent Threats (APT), which normally utilize zero-day viruses and malware.

Control implementation guidelines

- Define and document the requirements of this ECC in the cybersecurity requirements of email security at the organization and must be approved by the representative.
- Define and provide advanced technologies within the organization to provide email protection against advanced persistent threats and zero-day malware.
- Activate features of advanced persistent threats and zero- day malware in the email protection system.
- Review the list of suspicious emails that have been filtered by the system because they contain advanced persistent threats and zero-day malware.
- Take necessary measures to protect the device of the recipient of the suspicious email message if it is not blocked by the protection system, and factors and indicators of penetration must be blocked.

Expected deliverables:

- A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control.
- Screenshot or direct example showing subscription and use of modern and advanced technologies for email ATP protection in the organization.
- Screenshot or direct example showing email configuration in the organization and the activation of ATP protection.

2-4-3-5 Validation of the organization's email service domains (e.g., using Sender Policy Framework (SPF)).

Control implementation guidelines

- Define and document the requirements of this ECC in the cybersecurity requirements of email security at the organization and must be approved by the representative.
- Create an SPF Record containing servers authorized to send emails to protect the organization from the risk of spoofing.

	○ Create DKIM Record, which uses the digital signature in all emails issued by the organization's domain to ensure the integrity of e-mails. ● Create “Domain-based Message Authentication, Reporting & Conformance (DMARC), which leverages existing email authentication techniques with SPF and DKIM to protect email domains from spoofing attacks. ● Ensure linking the scope of email with the mail documentation service of Haseen platform.
	Expected deliverables: ● A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. ● Screenshot showing the preparation of the SPF Record, which shows the servers authorized to send email from the organization scope.
2-4-4	The cybersecurity requirements for email service must be reviewed periodically.
	Control implementation guidelines ● Review the implementation of cybersecurity requirements for email protection by conducting a periodic assessment (according to a documented and approved plan for review, and based on a planned interval "e.g., quarterly") to implement the organization's email protection procedures by the Cybersecurity function and in cooperation with relevant departments (such as IT Department). ● Conduct application review through traditional channels (e.g., email) or automated channels using a compliance management system. The organization may develop a review plan explaining the cybersecurity requirements implementation review schedule for email protection. ● Review and update Cybersecurity requirements for email protection in the organization must be reviewed and updated periodically according to a documented and approved plan for review and based on a planned interval or in the event of changes in relevant laws and regulations. ● Document the review and changes to the cybersecurity requirements for email protection in the organization and approve them by the head of the organization or his/her deputy.
	Expected deliverables:

	• Results of email protection cybersecurity requirements implementation review in the organization • A document that defines the cybersecurity requirements application review cycle for the organization's email protection (Compliance Assessment Schedule). • Compliance assessment report that outlines the assessment of the implementation of cybersecurity requirements for the organization's email protection • An approved document that sets the policy's review schedule • Policy indicating that it has been reviewed and updated, and that changes have been documented and approved by the head of the organization or his/her deputy. • Formal approval by the head of the organization or his/her deputy on the updated policy (e.g., via the organization's official e-mail, paper or electronic signature).

2-5	Networks Security Management
Objective	To ensure the protection of organization's network from cyber risks.
Controls	
2-5-1	Cybersecurity requirements for network security management must be defined, documented and approved.
	Relevant cybersecurity tools: • Network Security Policy Template. Control implementation guidelines • Develop and document cybersecurity policy for network security in the organization, including the following: ○ Network Access Requirements

	○ Third Parties Access Requirements to the Network ○ Network Protection Requirements ○ Physical and environmental security requirements to ensure that network devices are stored in a secure and appropriate environment ● Security technology standard controls for all network devices used within the organization must be defined, documented and approved. ● Support the organization's policy by the Executive Management. This must be done through the approval of the organization head or his/ her deputy.
	Expected deliverables: ● Network security management policy approved by the organization (e.g., electronic copy or official hard copy). ● Cybersecurity policy that covers the requirements of technical security standard controls and network security management in the organization (e.g., electronic copy or official hard copy). ● Formal approval by the head of the organization or his/her deputy on the policy and technical standard (e.g., via the organization's official e-mail, paper or electronic signature).
2-5-2	The cybersecurity requirements for network security management must be implemented.
	Control implementation guidelines ● Implement all cybersecurity requirements for network security in the organization, including the following: ○ Ensure physical or logical segregation and division of the organization's network parts ○ Use Firewall to protect the organization's networks ○ Implement the principle of multi-stage security defense (Defense-in-Depth) to provide advanced and more effective protection for the organization's network devices ○ Isolate the production environment network from the development and testing networks of the organization ○ Ensure security of navigation and internet connection in the organization, including setting up network devices and restricting access to suspicious websites

		○ Protect the internet browsing channel from advanced persistent threats ○ Ensure the security and protection of wireless networks at the organization ○ Ensure the security of the organization's network ports, protocols, and services restrictions and management ○ Use advanced protection systems to detect and prevent intrusions in the organization's networks ○ Ensure the security of the organization's DNS ● Establish procedures to ensure the continuous implementation of cybersecurity requirements adopted for the organization's network security management in accordance with the relevant laws and regulations.
		Expected deliverables: ● An action plan to implement the cybersecurity requirements of information and technology assets management. ● Sample showing the implementation of the organization's network security management controls, including but not limited to: o Sample that shows the organization's use of modern technologies for network security management, as well as restrictions and management of network ports, protocols and services. o Sample that shows network configuration to prevent critical systems from being connected to the organization's wireless network o Sample showing implementation of logical isolation between production environment network, test environment network, and other networks ● Sample of defined and approved procedures for handling critical network devices and systems of the organization
2-5-3		The cybersecurity requirements for network security management must include at least the following:
	2-5-3-1	Logical or physical segregation and segmentation of network segments using firewalls and defense-in-depth principles.
		Control implementation guidelines ● Define and document the requirements of this ECC in the cybersecurity requirements of network security management at the organization and must be approved by the representative.

	● Define network zones based on trust level e.g., trust in the internet zone is "low", trust level in an internet-isolated zone hosting databases is "high". ● Define necessary procedures to ensure the physical or logical isolation and segregation of network parts in the organization (for example but not limited to procedures for using the internal virtual network to isolate network parts) ● Activate appropriate and advanced technologies for the safe physical or logical isolation and segregation of network parts, including but not limited to: ○ Firewall Isolation ○ Isolation for systems accessed from outside the organization in a neutral zone (DMZ) ○ Insulation of network parts via VLAN ○ Implement the principle of multi-stage security defense (Defense-in-Depth), which includes the implementation of technical controls and administrative controls for protection.	
	Expected deliverables: ● Cybersecurity policy that covers the requirements of network security management in the organization (e.g., electronic copy or official hard copy). ● Formal approval by the head of the organization or his/her deputy on the policy (e.g., via the organization's official e-mail, paper or electronic signature). ● Sample showing the implementation of requirements related to the safe physical or logical isolation and segregation of network parts, including but not limited to: ○ Evidence showing the implementation of requirements related to the safe physical or logical isolation and segregation of network parts and defense in depth strategy (e.g., a screenshot showing evidence of the subscription and use of modern and advanced technologies to implement the physical or logical isolation and segregation of network parts in a secure manner) ○ Sample showing the implementation of the requirements of appropriate and advanced technologies for the safe physical or logical isolation and segregation of network parts and defense in depth (e.g., a screenshot showing evidence of the safe physical or logical isolation and segregation of network parts, as well as viewing and reviewing Network Diagram.	
	2-5-3-2	Network segregation between production, test and development environments.

	Control implementation guidelines • Define and document the requirements of this ECC in the cybersecurity requirements of network security management at the organization and must be approved by the representative. • Network domains must be logically separated to clarify production environment network addresses and development and testing environment networks (e.g., using VLANs). • Network must be configured to ensure that production environment networks are isolated from development and testing environment networks through the use of firewall systems. • Network segregation and network diagram must be documented to illustrate the isolation of production environment networks from development and testing networks.	
	Expected deliverables: • Cybersecurity policy that covers all the requirements of network security management in the organization (e.g., electronic copy or official hard copy). • Formal approval by the head of the organization or his/her deputy on such requirements (e.g., via the organization's official e-mail, paper or electronic signature). • List of server addresses in production environment and development and testing environment. • An up-to-date network diagram document that shows logical segregation and clarifies the isolation between the production environment network from the development and testing networks.	
	2-5-3-3	Secure browsing and Internet connectivity including restrictions on the use of file storage/sharing and remote access websites, and protection against suspicious websites.
	Control implementation guidelines • Define and document the requirements of this ECC in the cybersecurity requirements of network security management at the organization and must be approved by the representative.	

- Define necessary procedures to ensure navigation and internet connection security at the organization, including but not limited to:
  - Procedures for restriction of suspicious websites, file sharing and storage sites, and remote access sites.
  - Configuration of firewall systems to connect by using Proxy to analyze and filter data transmitted to and from the organization.

Expected deliverables:

- Cybersecurity policy that covers all the requirements of network security management in the organization (e.g., electronic copy or official hard copy).
- Formal approval by the head of the organization or his/her deputy on such requirements (e.g., via the organization's official e-mail, paper or electronic signature).
- Sample showing the implementation of requirements related to browsing and internet connection security, including but not limited to:
  - Sample showing the implementation of browsing and internet connection security requirements (e.g., screenshot showing evidence of use of modern and advanced technologies for browsing and internet connection security)
  - Sample showing the implementation of the requirements of appropriate and advanced technologies for browsing and internet connection security (e.g., a screenshot showing evidence that the network settings and firewall systems are conducted and configured to ensure security of browsing and internet connection, evidence of restriction of suspicious websites, file sharing and storage sites, remote access sites)

2-5-3-4	Wireless network protection using strong authentication and encryption techniques. A comprehensive risk assessment and management exercise must be conducted to assess and manage the cyber risks prior to connecting any wireless networks to the organization’s internal network.

Relevant cybersecurity tools:

- Wireless Network Security Standard Template.

Control implementation guidelines

- Define and document the requirements of this ECC in the cybersecurity requirements of network security management at the organization and must be approved by the representative.

- Implement security requirements of wireless networks in the organization, which may include the following:
  - Appropriate and advanced technologies for wireless network security and protection.
  - Verification of username and connect the wireless network to the user's name before granting the user access to the wireless network.
  - Separation of the internal network (LAN) from the wireless network by isolating the two networks from each other, as well as isolating the wireless visitor network from the wireless network of the organization.
- Encrypt wireless communication by configuring wireless network devices to support the highest cryptography standard controls and in line with the relevant laws and regulations.
- Conduct of a thorough study of the risks arising from connecting wireless networks to the organization's internal network in case there is a need to link them, and deal with them in a way that ensures the protection of the organization's technical assets. There must be evidence of risk analysis and study, including but not limited to, providing a thorough report that includes identifying and classifying risks, notes, and remediation plan (e.g., through an advanced automation program or an Excel sheet)

Expected deliverables:

- Wireless Security Standard approved by the organization (e.g., electronic copy or official hard copy).
- Sample showing the implementation of wireless network security and protection requirements, including but not limited to:
  - Sample showing the implementation of wireless network security and protection requirements (e.g., a screenshot showing evidence of subscription and use of modern and advanced technologies to implement wireless network security and protection, including but not limited to wireless network connection cryptography, as well as configuration of network devices and firewall systems in line with the verification of the user's name before granting the access to connect to the organization's wireless network)
  - Sample of conducting a thorough study of the risks arising from connecting wireless networks to the organization's internal network in case there is a need to link them, and deal with them in a way that ensures the protection of the organization's technical assets. There must be evidence of risk analysis and study, including but not limited to, providing a thorough report that

includes identifying and classifying risks, notes, and remediation plan (e.g., through an advanced automation program or an Excel sheet)

  - Sample of separating the internal network (LAN) from the wireless network by isolating the two networks from each other, as well as isolating the wireless visitor network from the wireless network of the organization.

2-5-3-5	Management and restrictions on network services, protocols and ports.

Control implementation guidelines

- Define and document the requirements of this ECC in the cybersecurity requirements of network security management at the organization and must be approved by the representative.
- Implement the requirements of restrictions and management of network ports, protocols and services at the organization, which may include the following:
  - Appropriate and advanced technologies for restrictions and management of network ports, protocols and services.
  - Procedures for managing ports, protocols, network services and access authorities.
- Restrict unused ports and protocols in the organization, including but not limited to:
  - Restriction by firewall systems.
  - Physical closure of unused ports.
- Regularly review and update of protection systems' configuration, including but not limited to:
  - Periodic review at least on an annual basis.
  - Development of all technical controls and standard controls that are reviewed and verified with relation to the configuration of protection systems within an advanced automation program or through Excel Sheet program, and monitor and update them, if necessary, after obtaining the prior approval of the representative.
  - Establishment of approval procedures to update the Firewall Rules to ensure that no update or change is made without the approval of the representative.

Expected deliverables:

- Cybersecurity policy that covers all the requirements of network security management in the organization (e.g., electronic copy or official hard copy).
- Formal approval by the head of the organization or his/her deputy on such requirements (e.g., via the organization's official e-mail, paper or electronic signature).
- Sample showing the implementation of requirements related to network ports, protocols, and services restrictions and management, including but not limited to:
    - Sample showing the implementation of network ports, protocols, and services restrictions and management requirements (e.g., screenshot showing evidence of subscription and use of modern and advanced technologies to apply restrictions and manage network ports, protocols, and services through firewall system)
    - Sample showing the periodic review of the protection systems' configuration and updates on an ongoing basis, including but not limited to periodic review at least on an annual basis, as well as the development of all technical controls and standard controls that are reviewed and verified with relation to the protection systems configuration within the advanced automation program or through Excel Sheet. This is in addition to supporting the review by obtaining prior approval for review and update of the configuration, if necessary.
    - Sample showing approval procedures form to update the Firewall Rules to ensure that no update or change is made without obtaining the approval of the representative. In addition, a sample showing what has been updated on the Firewall Rules.

2-5-3-6	Intrusion Prevention Systems (IPS).

Control implementation guidelines

- Define and document the requirements of this ECC in the cybersecurity requirements of network security management at the organization and must be approved by the representative.
- Implement the requirements of advanced protection systems to detect and prevent intrusions in the organization, which may include the following:
    - Intrusion Prevention System
    - Appropriate and advanced technologies for Intrusion Prevention System

	• Protect the organization by using (IPS/IDS) to cover all infrastructure of the organization, including: ○ Internal Network ○ DMZ. ○ Wireless network. • Periodically review (IPS/IDS) configurations, and all technical controls and standard controls that are reviewed and verified with relation to the configuration of (IPS/IDS) within an advanced automation program or through Excel Sheet, must be developed, followed -up and updated, if necessary, with the prior approval of the representative.	
	Expected deliverables: • Cybersecurity policy that covers all the requirements of network security management in the organization (e.g., electronic copy or official hard copy). • Formal approval by the head of the organization or his/her deputy on such requirements (e.g., via the organization's official e-mail, paper or electronic signature). • Sample showing the implementation of requirements related to (IPS/IDS), including but not limited to: o Sample showing the implementation of (IPS/IDS) (e.g., a screenshot showing evidence of subscription and use of modern and advanced technologies to implement (IPS/IDS), as well as access to technical infrastructure, demonstrating the use of (IPS/IDS) and the comprehensiveness of all the organization's information and technology assets within (IPS/IDS) o Periodic review report on IPS/IDS configuration and development of all technical controls and standard controls must be reviewed and verified in relation to the configuration of (IPS/IDS) within an advanced automation program or through Excel Sheet, as well as supporting the review by obtaining prior approval for review and update of the configuration if required	
	2-5-3-7	Security of Domain Name Service (DNS).
	Control implementation guidelines	

	• Define and document the requirements of this ECC in the cybersecurity requirements of network security management at the organization and must be approved by the representative. • Use DNS Security or DNS Firewall to protect the organization's systems against DNS Poisoning attacks and use documented DNS. • Refrain from using public domain name services such as Google DNS or service provider domain names.	
	Expected deliverables: • Cybersecurity policy that covers all the requirements of network security management in the organization (e.g., electronic copy or official hard copy). • Formal approval by the head of the organization or his/her deputy on such requirements (e.g., via the organization's official e-mail, paper or electronic signature). • Screenshot showing domain name configuration at the organization (DNS) indicating the use of a documented DNS address. • Screenshot of DNS Security that indicates IP range protection at the organization	
	2-5-3-8	Secure management and protection of Internet browsing channel against Advanced Persistent Threats (APT), which normally utilize zero-day viruses and malware.
	Control implementation guidelines • Define and document the requirements of this ECC in the cybersecurity requirements of network security management at the organization and must be approved by the representative. • Implement the requirements of internet browsing channel APT Protection in the organization, which may include the following: ○ Internet browsing channel APT Protection. ○ Appropriate and advanced technologies Internet browsing channel APT Protection and ensure the effectiveness of these technologies. • Implement internet browsing channel APT Protection by using advanced systems and technologies to protect against the risk of Zero-Day Malware, including, but not limited to, subscribing to and securely managing an APT Protection provider.	

	Expected deliverables: • Cybersecurity policy that covers all the requirements of network security management in the organization (e.g., electronic copy or official hard copy). • Formal approval by the head of the organization or his/her deputy on such requirements (e.g., via the organization's official e-mail, paper or electronic signature). • Sample showing the implementation of the requirements related to Internet browsing channel APT Protection, including but not limited to: o Sample showing the implementation of the requirements of Internet browsing channel APT Protection (e.g., a screenshot showing evidence of subscription and use of modern and advanced technologies to implement Internet browsing channel APT Protection and evidence of the APT Protection against zero-day malware.
2-5-4	The cybersecurity requirements for network security management must be reviewed periodically.
	Control implementation guidelines • Review the cybersecurity requirements of network security in the organization by conducting a periodic assessment (according to a documented and approved plan for review, and based on a planned interval "e.g., quarterly") to implement network security management requirements by the Cybersecurity function and in cooperation with relevant departments (such as IT Department). • Conduct application review through traditional channels (e.g., email) or automated channels using a compliance management system. The organization may develop a review plan explaining the implementation of cybersecurity requirements to network security management in the organization. • Review and update cybersecurity requirements for network security management in the organization periodically according to a documented and approved plan for review and based on a planned interval or in the event of changes in relevant laws and regulations. • Document the review and changes to the cybersecurity requirements for network security in the organization and approve them by the head of the organization or his/her deputy.
	Expected deliverables:

	• Results of network security cybersecurity requirements implementation review in the organization • An approved document that defines the cybersecurity requirements implementation review cycle to manage the organization's network security (Compliance Assessment Schedule). • Compliance assessment report that outlines the assessment of the implementation of cybersecurity requirements for the organization's network security. • An approved document that sets the policy's review schedule • Policy indicating that it has been reviewed and updated, and that changes have been documented and approved by the head of the organization or his/her deputy. • Formal approval by the head of the organization or his/her deputy on the updated policy (e.g., via the organization's official e-mail, paper or electronic signature).

2-6	Mobile Devices Security
Objective	To ensure the protection of mobile devices (including laptops, smartphones, tablets) from cyber risks and to ensure the secure handling of the organization's information (including sensitive information) while utilizing Bring Your Own Device (BYOD) policy.
Controls	
2-6-1	Cybersecurity requirements for mobile devices security and BYOD must be defined, documented and approved.
	Relevant cybersecurity tools: • Workstations, Mobile Devices and BYOD Security Policy Template. Control implementation guidelines • Develop and document Cybersecurity policy for mobile devices and BYOD in the organization, including the following: ○ Mobile Devices Cybersecurity Requirements

	○ BOYD Cybersecurity Requirements ● Support the organization's policy by the Executive Management. This must be done through the approval of the organization head or his/ her deputy.
	Expected deliverables: ● Cybersecurity policy and standard for mobile devices and personal devices (BYOD) at the organization (e.g., electronic copy or official hard copy). ● Formal approval by the head of the organization or his/her deputy on the policy and technical standard (e.g., via the organization's official e-mail, paper or electronic signature).
2-6-2	The cybersecurity requirements for mobile devices security and BYOD must be implemented.
	Control implementation guidelines ● All cybersecurity requirements related to the security of mobile devices and BYOD for the organization must be implemented, which may include the following: ○ Ensure the isolation, segregation, and cryptography of data and information of the organization stored on mobile devices and BYOD from the rest of the information and data on the device. ○ Ensure the use must be specified and restricted to the requirements of the organization. ○ Provide us of workstations and mobile devices with privileged access following the principle of least privilege. ○ Ensure that the storage media of critical and sensitive workstations and mobile devices are encrypted and have privileged access. ○ Ensure that data and information of the organization stored on mobile devices and BYOD must be deleted when devices are lost or after the end/termination of the functional relationship with the organization. ○ Ensure the activation of Remote Wipe on all mobile devices that store or process the organization's classified information. ○ Implement the organization's Group Policy and apply it to all workstations and mobile devices to ensure compliance with regulatory and security controls. ○ Provide security awareness to users.

<table>
<tr><td></td><td colspan="2">
<ul>
<li>Centrally manage workstations and mobile devices through, but not limited to, the Active Directory server or through a centralized management system.</li>
<li>Implement secure configuration and hardening controls to workstations and mobile devices in accordance with cybersecurity standard controls.</li>
<li>Establish procedures to ensure the implementation of cybersecurity requirements adopted for the organization's mobile devices and personal devices (BYOD) management in accordance with the relevant laws and regulations.</li>
</ul>
</td></tr>
<tr><td></td><td colspan="2">Expected deliverables:
<ul>
<li>An action plan to implement the cybersecurity requirements for mobile devices and personal devices (BYOD) security management.</li>
<li>Sample showing the implementation of mobile devices and BYOD security controls at the organization, including but not limited to:
<ul>
<li>Sample showing that the organization's use of advanced technologies for mobile devices and personal devices (BYOD) security (e.g., the existence of advanced technologies necessary to separate and encrypt the organization's data and information stored on mobile devices and BYOD).</li>
<li>Sample showing the central management of workstations and mobile devices, including but not limited to a screenshot from the Active Directory server in addition to configuration.</li>
<li>Defined and approved procedures for handling mobile devices and personal devices (BYOD) at the organization.</li>
</ul>
</li>
</ul>
</td></tr>
<tr><td>2-6-3</td><td colspan="2">The cybersecurity requirements for mobile devices security and BYOD must include at least the following:</td></tr>
<tr><td></td><td>2-6-3-1</td><td>Separation and encryption of organization’s data and information stored on mobile devices and BYODs.</td></tr>
</table>

Control implementation guidelines

- Define and document the requirements of this ECC in the cybersecurity requirements of mobile devices and BYOD at the organization and must be approved by the representative.
- Implement the requirements of separating and encrypting the organization's data and information stored on mobile devices and BYOD devices, which may include the following:
  - Separation and cryptography of data and information.
  - Appropriate and advanced technologies for separating and encrypting data and information.
- Use necessary technologies (such as Mobile Device Management) to encrypt the organization's data and information stored on mobile devices and BYOD.

Expected deliverables:

- Cybersecurity policy that covers all the security requirements of mobile devices and personal devices (BYOD) at the organization (e.g., electronic copy or official hard copy).
- Formal approval by the head of the organization or his/her deputy on such requirements (e.g., via the organization's official e-mail, paper or electronic signature).
- Sample showing the implementation of mobile devices and BYOD security requirements, including but not limited to:
  - Sample showing the implementation of the requirements of appropriate and advanced technologies for the security of mobile devices and BYOD (e.g., screenshot showing the use of advanced systems to provide and ensure data cryptography on mobile devices and BYOD at the organization).
  - Defined and approved procedures for encrypting data and information stored on mobile devices and BYOD.

2-6-3-2	Controlled and restricted use based on job requirements.

Control implementation guidelines

- Define and document the requirements of this ECC in the cybersecurity requirements of mobile devices and BYOD at the organization and must be approved by the representative.

	● Implement the specified and restricted use requirements based on the requirements of the organization's business interest. These requirements may include the following: o The use must be specified and restricted to the requirements of the organization. o Appropriate and advanced technologies for specific and restricted use based on the requirements of the organization's business interest. ● Develop necessary procedures to restrict the use of mobile devices and link them to their network based on the requirements of the business interest. ● Assess mobile devices configuration and security controls, including but not limited to the implementation of (Patches, AV) prior to linking them to the organization's domain or network.
	Expected deliverables: ● Cybersecurity policy that covers all the security requirements of mobile devices and personal devices (BYOD) at the organization (e.g., electronic copy or official hard copy). ● Formal approval by the head of the organization or his/her deputy on such requirements (e.g., via the organization's official e-mail, paper or electronic signature). ● Sample showing the implementation of requirements related to the specific and restricted use based on the organization's business interest, including but not limited to: o Sample showing the implementation of the specific and restricted use requirements based on the organization's business interest (e.g., a screenshot showing evidence that the necessary procedures are in place to restrict the use of mobile devices and link them to their network based on the business interest). o Defined and approved procedures for restricting the use of mobile devices (e.g., a form of procedures, as well as a sample report showing evidence of ensuring that the mobile device settings and security controls are assessed, including the implementation of patches and antivirus updates prior to being linked to the network).

	2-6-3-3	Secure wiping of organization’s data and information stored on mobile devices and BYOD in cases of device loss, theft or after termination/separation from the organization.
	Control implementation guidelines ● Define and document the requirements of this ECC in the cybersecurity requirements of mobile devices and BYOD at the organization and must be approved by the representative. ● Ensure that data and information of the organization stored on mobile devices and BYOD must be deleted when devices are lost or after the end/termination of the functional relationship with the organization. ● Use necessary technologies (such as Mobile Device Management) to ensure the deletion of sensitive data and information when the devices are lost, and after the end/termination of the functional relationship with the organization.	
	Expected deliverables: ● Cybersecurity policy that covers all the security requirements of mobile devices and personal devices (BYOD) at the organization (e.g., electronic copy or official hard copy). ● Formal approval by the head of the organization or his/her deputy on such requirements (e.g., via the organization's official e-mail, paper or electronic signature). ● Sample showing the implementation of requirements related to the deletion of data and information stored on mobile devices and BYOD to include, but not limited to: o Sample showing the implementation of deletion requirements for data and information stored on mobile devices and BYOD devices (e.g., a screenshot showing evidence of deleting data and information stored on mobile devices and personal devices when, for example, the subscription with a data deletion service and integrated secure management of mobile devices and BYOD devices provider is no longer valid. o Sample of the followed procedures template showing evidence of ensuring the deletion of data and information stored on mobile devices and personal devices BOYD when they are lost or after the end/termination of the functional relationship with the organization.	

	2-6-3-4	Security awareness for mobile devices users.
	Control implementation guidelines ● Define and document the requirements of this ECC in the cybersecurity requirements of mobile devices and BYOD at the organization and must be approved by the representative. ● Implement security awareness requirements for users, which may include the following: ○ Provide security awareness to users. ○ Appropriate and advanced technologies to provide security awareness to users. ● Implement the requirements of this control by providing security awareness to users on mobile devices and BYOD on a regular basis.	
	Expected deliverables: ● Cybersecurity policy that covers all the security requirements of mobile devices and personal devices (BYOD) at the organization (e.g., electronic copy or official hard copy). ● Formal approval by the head of the organization or his/her deputy on such requirements (e.g., via the organization's official e-mail, paper or electronic signature). ● Sample showing the implementation of security awareness requirements for users, including but not limited to: ○ Sample showing the implementation of security awareness requirements for users (e.g., presentation showing security awareness to the organization's employees regarding the optimal and safe use of mobile devices and BYOD devices or a screen shot from mobile devices' screensaver showing an awareness message to users)	
2-6-4	The cybersecurity requirements for mobile devices security and BYOD must be reviewed periodically.	
	Control implementation guidelines ● Review the implementation of cybersecurity requirements for mobile devices and BYOD security by conducting a periodic assessment (according to a	

	documented and approved plan for review, and based on a planned interval "e.g., quarterly") to implement the organization's mobile devices and BYOD security procedures by the Cybersecurity function and in cooperation with relevant departments (such as IT Department). • Conduct application review through traditional channels (e.g., email) or automated channels using a compliance management system. The organization may develop a review plan outlining the cybersecurity requirements implementation review schedule for mobile devices and BYOD security. • Review and update cybersecurity requirements for mobile devices and BYOD security in the organization periodically according to a documented and approved plan for review and based on a planned interval or in the event of changes in relevant laws and regulations. • Document the review and changes to the cybersecurity requirements for mobile devices and BYOD security in the organization and approve them by the head of the organization or his/her deputy.
	Expected deliverables: • Results of mobile devices and BYOD cybersecurity requirements implementation review in the organization • A document that defines the cybersecurity requirements implementation review cycle for mobile devices and BYOD security (Compliance Assessment Schedule). • Compliance assessment report that outlines the assessment of the implementation of cybersecurity requirements for the organization's mobile devices and BYOD security • An approved document that sets the policy's review schedule • Policy indicating that it has been reviewed and updated, and that changes have been documented and approved by the head of the organization or his/her deputy. • Formal approval by the head of the organization or his/her deputy on the updated policy (e.g., via the organization's official e-mail, paper or electronic signature).

2-7	Data and Information Protection
Objective	To ensure the confidentiality, integrity and availability of organization's data and information as per organizational policies and procedures, and related laws and regulations.
Controls	
2-7-1	Cybersecurity requirements for protecting and handling data and information must be defined, documented and approved as per the related laws and regulations.
	Relevant cybersecurity tools: • Data Security Policy Template Control implementation guidelines • Cybersecurity requirements for data and information protection must be included and documented in line with policies issued by the National Data Management Office, including but not limited to: ○ Data and Information Protection Requirements. ○ Data and Information Ownership Requirements. ○ Data and information Classification and Labelling Requirements. ○ Data and Information Privacy Requirements. • The policy must be supported by the Executive Management. This must be done through the approval of the organization head or his/ her deputy.
	Expected deliverables: • Cybersecurity policy that covers the requirements of Data and Information Protection in the organization (e.g., electronic copy or official hard copy). • Formal approval by the head of the organization or his/her deputy on the policy (e.g., via the organization's official e-mail, paper or electronic signature).
2-7-2	The cybersecurity requirements for protecting and handling data and information must be implemented.
	Control implementation guidelines

	● Implement all cybersecurity requirements to data and information protection procedures in the organization. The data and information protection procedures must cover at least the following, but not limited to: ○ Define data and information ownership. ○ Classify data and information. ○ Label data and information in line with the data and information classification mechanism approved by the organization. ● Develop an action plan to implement all cybersecurity requirements related to data and information protection. ● Implement data protection controls to ensure its protection according to its classification level and impact. ● The organization may also develop an action plan to implement cybersecurity requirements related to data and information protection, in order to ensure that the organization complies with all cybersecurity requirements for all internal and external stakeholders and follow up and monitor them periodically to ensure implementation.
	Expected deliverables: ● Documents that confirm the implementation of cybersecurity requirements related to information and data protection as documented in the policy. ● An action plan to implement cybersecurity requirements for data and information protection. ● Evidence showing the implementation of data and information protection controls, including but not limited to: o Provide a data and information governance matrix that clarifies the ownership of data and information. o Availability of procedures to deal with data according to their classification and impact. o Sample of modern technologies used to protect the organization’s data and information (e.g., the existence of advanced technologies necessary to protect, encrypt, and save the organization's data and information from modification and leakage).
2-7-3	The cybersecurity requirements for protecting and handling data and information must include at least the following:

	2-7-3-1	Data and information ownership.
	Control implementation guidelines • Define data and information ownership requirements in accordance with policies issued by the National Data Management Office and documented in the cybersecurity requirements document and approved by the representative. • Coordinate with relevant departments to identify the owners of data and information and document their ownership in the relevant records (information assets records). • Implement cybersecurity requirements for data and information ownership to ensure compliance with the cybersecurity requirements of all internal and external stakeholders, including but not limited to the following: ○ Identification and definition of data owned by the organization. ○ Identification of data owners in the organization. ○ Contribution of data and information owners in the classification and labelling process in line with the data classification and labelling mechanism approved by the organization. ○ Performance of an impact assessment of the data and discuss it with the data owners to identify potential damages.	
	Expected deliverables: • A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control • An action plan to implement cybersecurity requirements related to data and information ownership. • Evidence showing the implementation of data and information ownership requirements, including but not limited to: o Official document approved by the head of the organization or his/ her deputy indicating the organization's systems, data and information owners. o List of data owned by the organization, indicating the owners of such data.	
	2-7-3-2	Data and information classification and labeling mechanisms.
	Control implementation guidelines	

- Define data and information classification and labelling requirements in accordance with policies issued by the National Data Management Office and documented in the cybersecurity requirements document and approved by the representative.
- Form a taskforce between the cybersecurity function and the data management office in the organization.
- Develop Data and information Classification and Labelling procedures.
- Develop a methodology to classify data and information and its labelling mechanism must be developed, taking into account the main data classification principles issued by the National Data Management Office:
  - Open by default.
  - Necessity and proportionality.
  - Timely classification.
  - Highest level of protection.
  - Segregation of Duties.
  - Need-to-know.
  - Least Privilege.
- Identify appropriate mechanisms and technologies to automate data labelling according to their classification, including but not limited to watermarks.

Expected deliverables:

- A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control
- Data governance document approved by the organization's representative
- Evidence showing the implementation of Data and information Classification and Labelling requirements, including but not limited to:
  - Sample of data that has been classified and labelled according to the classification and labelling mechanism documented and approved by the organization, including data classification and impact activities.

2-7-3-3	Data and information privacy.

Control implementation guidelines

- Identify and document data and information privacy requirements in the cybersecurity requirements document, in alignment with related laws and

	regulations, and must be approved by the representative, which may include the following: ○ Include cybersecurity responsibilities and clauses in protecting data and information privacy. ○ Develop the organization's data privacy procedures to ensure compliance with cybersecurity requirements for all internal and external stakeholders. ● Implement cybersecurity requirements for data and information privacy to ensure compliance with cybersecurity requirements for all internal and external stakeholders.
	Expected deliverables: ● A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. ● Documented and approved procedures by the head of the organization or his/her deputy on how to deal with data and information and its privacy.
2-7-4	The cybersecurity requirements for protecting and handling data and information must be reviewed periodically.
	Control implementation guidelines ● Review the cybersecurity requirements of data and information protection by conducting a periodic assessment (according to a documented and approved plan for review, and based on a planned interval "e.g., quarterly") to implement identity and access management requirements by the Cybersecurity function and in cooperation with relevant departments (such as IT Department). ● Conduct application review through traditional channels (e.g., email) or automated channels using a compliance management system. The organization may develop a review plan explaining the implementation review schedule for data and information protection. ● Review and update cybersecurity requirements for data and information protection in the organization periodically according to a documented and approved plan for review and based on a planned interval or in the event of changes in relevant laws and regulations.

	• Document the review and changes to the cybersecurity requirements for data and information protection in the organization and approve them by the head of the organization or his/her deputy.
	Expected deliverables: • Results of data and information protection cybersecurity requirements implementation review in the organization. • A document that defines the cybersecurity requirements implementation review cycle for the organization's data and information security (Compliance Assessment Schedule). • Compliance assessment report that outlines the assessment of the implementation of cybersecurity requirements for data and information protection in the organization. • An approved document that sets the policy's review schedule • Policy indicating that it is up to date and the changes to the cybersecurity requirements for data and information protection have been documented and approved by the head of the organization or his/her deputy. • Formal approval by the head of the organization or his/her deputy on the updated policy (e.g., via the organization's official e-mail, paper or electronic signature).

2-8	Cryptography
Objective	To ensure the proper and efficient use of cryptography to protect information assets as per organizational policies and procedures, and related laws and regulations.
Controls	
2-8-1	Cybersecurity requirements for cryptography must be defined, documented and approved.
	Relevant cybersecurity tools: • Cryptography Policy Template. Control implementation guidelines

	• Develop and document cybersecurity policy for cryptography in the organization, including the following: ○ Standard controls of approved cryptography solutions and applicable restrictions (technically and regulatorily). ○ Secure management of cryptographic keys during their lifecycle. ○ Information must be encrypted in transit and storage based on classification as well as the relevant laws and regulations. • Support the organization's policy by the Executive Management. This must be done through the approval of the organization head or his/ her deputy.
	Expected deliverables: • Cybersecurity policy that covers all the requirements of cryptography in the organization (e.g., electronic copy or official hard copy). • Formal approval by the head of the organization or his/her deputy on the policy (e.g., via the organization's official e-mail, paper or electronic signature).
2-8-2	The cybersecurity requirements for cryptography must be implemented.
	Control implementation guidelines • Implement all cybersecurity requirements to the organization's approved cryptography procedures. It is also recommended that the cryptography procedures cover the following, but not limited to: ○ Standard controls of approved cryptography solutions and applicable restrictions (technically and regulatorily). ○ Secure management of cryptographic keys during their lifecycle. ○ Information must be encrypted in transit and storage based on classification as well as the relevant laws and regulations. ○ Approved cryptographic hash functions should be defined based on national cryptographic standard controls. ○ Implementation of cryptography to technical and information assets. ○ Use of approved TLS certificates for web servers and public applications issued by a trusted third party.
	Expected deliverables: • An action plan to implement cybersecurity requirements for cryptography

	● Evidence showing the uses modern cryptography technologies in the organization (e.g., the presence of advanced encryption technologies in the organization, security procedures and standard controls that support the implementation of cryptography in the organization).	
2-8-3	The cybersecurity requirements for cryptography must include at least the following:	
	2-8-3-1	Approved cryptographic solutions standard controls and its technical and regulatory limitations.
	Relevant cybersecurity tools: ● Cryptography Standard Template. Control implementation guidelines ● Define and document the requirements of this ECC in the cybersecurity requirements document and must be approved by the representative. ● Define standard controls of approved cryptographic solutions and use NCA's cryptographic standard controls, including, but not limited to: ○ Acceptable symmetric and asymmetric cryptographic fundamentals ○ PKI Procedures ○ Key Cycle Management Procedure ● Define standard controls and technical limitations of approved cryptographic solutions and ensure their compliance with national cryptography standard controls, including but not limited to: ○ Acceptable symmetric and asymmetric cryptographic designs ○ Acceptable common application protocols related to cryptography ○ PKI technologies and tools ○ Key cycle management techniques and tools	
	Expected deliverables: ● Cryptography standard controls document approved by the organization (e.g., electronic copy or official hard copy). ● Formal approval by the head of the organization or his/her deputy on such standard controls (e.g., via the organization's official e-mail, paper or electronic signature).	

	• Evidence showing the implementation of the requirements of the approved technical cryptographic solutions standard controls and the restrictions applied to them (e.g., a screenshot showing evidence of ensuring that modern and advanced technologies are used to implement the standard controls of approved technical cryptography solutions and the restrictions applied to all systems in the organization). • Cryptography standard controls document approved by the organization (e.g., electronic copy or official hard copy). • Formal approval by the head of the organization or his/her deputy on such standard controls (e.g., via the organization's official e-mail, paper or electronic signature). • Evidence showing the implementation of the requirements of the approved technical cryptographic solutions standard controls and the restrictions applied to them (e.g., a screenshot showing evidence of ensuring that modern and advanced technologies are used to implement the standard controls of approved technical cryptography solutions and the restrictions applied to all systems in the organization).	
	2-8-3-2	Secure management of cryptographic keys during their lifecycles.
	Control implementation guidelines • Define and document the requirements of this ECC in the cybersecurity requirements document and must be approved by the representative. • Define and approve procedures for the secure management of cryptographic keys during their lifecycle. • Define and implement appropriate and advanced techniques for the secure management of cryptographic keys during their lifecycle, including, but not limited to: ○ Cryptographic key storage mechanism. ○ Cryptographic key transfer mechanism. ○ key creation and destruction mechanism. • Review the effectiveness of technologies used for the secure management of cryptographic keys.	
	Expected deliverables:	

	• Cybersecurity policy that covers all the requirements of cryptography in the organization (e.g., electronic copy or official hard copy). • Cybersecurity procedure that covers all the requirements of cryptographic keys. management in the organization (e.g., electronic copy or official hard copy). • Document that defines the technology effectiveness review cycle used for the secure management of cryptographic keys during their lifecycle. • Formal approval by the head of the organization or his/her deputy on such documents (e.g., via the organization's official e-mail, paper or electronic signature). • Evidence that the secure management requirements for cryptographic keys are implemented throughout their lifecycle (e.g., a screenshot showing evidence to ensure that cryptographic key settings are configured to the best standard controls for the secure management of cryptographic keys during their lifecycle).	
	2-8-3-3	Encryption of data in-transit and at-rest as per classification and related laws and regulations.
	Control implementation guidelines • Define and document the requirements of this ECC in the cybersecurity requirements document and must be approved by the representative. • Define appropriate and advanced technologies to encrypt data in transit based on their classification, including but not limited to: ○ TLS (Transport Layer Security) must be used • Define appropriate and advanced technologies to encrypt data in transit based on their classification. • Review the effectiveness of technologies used to encrypt data in transit based on classification. • Define appropriate and advanced technologies to encrypt data in storage based on their classification, including but not limited to: ○ TDE (Transparent Data Encryption) must be used • Define appropriate and advanced technologies to encrypt data in storage based on their classification. • Review the effectiveness of technologies used to encrypt data in transit based on classification.	

	Expected deliverables: ● Cryptography of data in transit document approved by the organization (e.g., electronic copy or official hard copy). ● Formal approval by the head of the organization or his/her deputy on such procedures (e.g., via the organization's official e-mail, paper or electronic signature). ● Evidence that data in transit cryptography requirements must be implemented based on their classification (but not limited to a screenshot showing the implementation of data in transit encryption based on its classification). ● Cryptography of data in transit document approved by the organization (e.g., electronic copy or official hard copy). ● Formal approval by the head of the organization or his/her deputy on such procedures (e.g., via the organization's official e-mail, paper or electronic signature). ● Evidence that data in transit cryptography requirements must be implemented based on their classification (but not limited to a screenshot showing the implementation of data in transit encryption based on its classification).
2-8-4	The cybersecurity requirements for cryptography must be reviewed periodically.
	Control implementation guidelines ● Review the cybersecurity requirements of cryptography by conducting a periodic assessment (according to a documented and approved plan for review, and based on a planned interval "e.g., quarterly") to implement identity and access management requirements by the Cybersecurity function and in cooperation with relevant departments (such as IT Department). ● Review and update cybersecurity requirements for cryptography in the organization periodically according to a documented and approved plan for review and based on a planned interval or in the event of changes in relevant laws and regulations. ● Document the review and changes to the cybersecurity requirements for cryptography in the organization and approve them by the head of the organization or his/her deputy.
	Expected deliverables:

	• Results of cryptography requirements implementation review in the organization. • A document that defines the cybersecurity requirements implementation review cycle for cryptography in the organization (Compliance Assessment Schedule). • Compliance assessment report that outlines the assessment of the implementation of cybersecurity requirements for cryptography in the organization. • An approved document that sets the policy's review schedule • Policy indicating that it is up to date and the changes to the cybersecurity requirements for cryptography have been documented and approved by the head of the organization or his/her deputy. • Formal approval by the head of the organization or his/her deputy on the updated policy (e.g., via the organization's official e-mail, paper or electronic signature).

2-9	Backup and Recovery Management
Objective	To ensure the protection of organization’s data and information including information systems and software configurations from cyber risks as per organizational policies and procedures, and related laws and regulations.
Controls	
2-9-1	Cybersecurity requirements for backup and recovery management must be defined, documented and approved.
	Relevant cybersecurity tools: • Backup and Recovery Management Policy Template. Control implementation guidelines • Develop and document cybersecurity policy for backup management in the organization, including the following: ○ Scope and coverage of critical information and technology systems backups

	○ Fast recovery of data and systems after exposure to cybersecurity incidents ○ Periodic inspection of backup recovery effectiveness ○ Time limit for backups ○ Appropriate and advanced technologies for backups must be defined ● Support the organization's policy by the Executive Management. This must be done through the approval of the organization head or his/ her deputy.
	Expected deliverables: ● Cybersecurity policy that covers the requirements of Backup and Recovery Management in the organization (e.g., electronic copy or official hard copy). ● Formal approval by the head of the organization or his/her deputy on the policy (e.g., via the organization's official e-mail, paper or electronic signature).
2-9-2	The cybersecurity requirements for backup and recovery management must be implemented.
	Control implementation guidelines ● All cybersecurity requirements must be implemented for the organization's approved Backup and Recovery Management procedures. It is also recommended that the Backup and Recovery Management procedures cover the following, but not limited to: ○ Appropriate and advanced technologies for backups must be used. ○ Scope and coverage of critical information and technology systems backups. ○ Fast recovery of data and systems after exposure to cybersecurity incidents must be implemented. ○ Periodic inspection of backup recovery effectiveness must be implemented. ○ Period required for backup must be defined, including but not limited to, backup of changing data in the last 24 hours.
	Expected deliverables: ● An action plan to implement cybersecurity requirements for backup and recovery management

	• Evidence such as, but not limited to, a screenshot of a backup tool showing the latest backups taken, schedule and scope of backups.	
2-9-3	The cybersecurity requirements for backup and recovery management must include at least the following:	
	2-9-3-1	Scope and coverage of backups to cover critical technology and information assets.
	Control implementation guidelines • Define and document the requirements of this ECC in the cybersecurity requirements of backups management at the organization and must be approved by the representative. • Define the scope of backups for all critical information and technology assets in the organization, including but not limited to: ○ Databases ○ Applications ○ Servers ○ Network Devices • Define specialized technologies for backup. • Determine the period required to backup all information and technology assets according to sensitivity and classification. • Implement backup to all critical information and technology assets in the organization. • Review the organization backups periodically, to include the aforementioned scope and any information and technology assets that have been identified by the organization.	
	Expected deliverables: • Documents indicating the identification and documentation of the requirements of this ECC in the policies or procedures of the organization approved by the representative. • A report of periodic backups as per the defined duration for all asset domains.	

	2-9-3-2	Ability to perform quick recovery of data and systems after cybersecurity incidents.
	Control implementation guidelines • Define and document the requirements of this ECC in the cybersecurity requirements of backups management at the organization and must be approved by the representative. • Identify appropriate procedures to recover data and systems after exposure to cybersecurity incidents, by but not limited to: o Define the scope of backup recovery, which may contain all devices, systems, and servers, and classify them according to their importance and criticality. o Determine the recovery period according to classification and importance of specified scope. o Use specialized technologies for data and system recovery. o Calculate the period required to recover all backups for all assets domain to ensure rapid recovery of backups in the event of a cyber security incident.	
	Expected deliverables: • Documents indicating the identification and documentation of the requirements of this ECC in the policies or procedures of the organization approved by the representative. • Report on specific procedures for recovery of backups.	
	2-9-3-3	Periodic tests of backup's recovery effectiveness.
	Control implementation guidelines • Define and document the requirements of this ECC in the cybersecurity requirements of backups management at the organization and must be approved by the representative. • Plan for periodic inspection of backup recovery effectiveness must be developed. • Ensure the effectiveness of recovery procedures by conducting a periodic backup recovery test to ensure the ability to recover data and systems	

	according to the period specified in the procedures and according to the period calculated to complete the recovery of backup copies.
	Expected deliverables: ● Documents indicating the identification and documentation of the requirements of this ECC in the policies or procedures of the organization approved by the representative. ● Backup effectiveness test reports showing the difference between the expected duration and the test duration to recover all backups.
2-9-4	The cybersecurity requirements for backup and recovery management must be reviewed periodically.
	Control implementation guidelines ● Review the cybersecurity requirements of Backup and Recovery Management by conducting a periodic assessment (according to a documented and approved plan for review, and based on a planned interval "e.g., quarterly") to implement identity and access management requirements by the Cybersecurity function and in cooperation with relevant departments (such as IT Department). ● Conduct application review through traditional channels (e.g., email) or automated channels using a compliance management system. The organization may develop a review plan explaining the implementation review schedule for Backup and Recovery Management. ● Review and update cybersecurity requirements for backups management in the organization periodically according to a documented and approved plan for review and based on a planned interval or in the event of changes in relevant laws and regulations. ● Document the review and changes to the cybersecurity requirements for Backup and Recovery Management in the organization and approve them by the head of the organization or his/her deputy.
	Expected deliverables: ● Results of backup management requirements implementation review in the organization.

	• A document that defines the cybersecurity requirements application review cycle for backup management at the organization (Compliance Assessment Schedule). • Compliance assessment report that outlines the assessment of the implementation of cybersecurity requirements for Backup and Recovery Management in the organization. • An approved document that sets the policy's review schedule • Policy indicating that it is up to date and the changes to the cybersecurity requirements for Backup and Recovery Management have been documented and approved by the head of the organization or his/her deputy. • Formal approval by the head of the organization or his/her deputy on the updated policy (e.g., via the organization's official e-mail, paper or electronic signature).

2-10	Vulnerabilities Management
Objective	To ensure timely detection and effective remediation of technical vulnerabilities to prevent or minimize the probability of exploiting these vulnerabilities to launch cyber-attacks against the organization.
Controls	
2-10-1	Cybersecurity requirements for technical vulnerabilities management must be defined, documented and approved.
	Relevant cybersecurity tools: • Vulnerabilities Management Policy Template. Control implementation guidelines • Develop and document cybersecurity policy for vulnerabilities management in the organization, including the following: ○ Vulnerabilities assessment and testing requirements for all technology assets. ○ Requirements for periodic vulnerability assessment.

	○ Requirements for the classification of vulnerabilities according to their severity. ○ Requirements to address vulnerabilities using effective tools and methods. ● Support the organization's policy by the Executive Management. This must be done through the approval of the organization head or his/ her deputy.
	Expected deliverables: ● Cybersecurity policy that covers the requirements of vulnerabilities management (e.g., electronic copy or official hard copy). ● Formal approval by the head of the organization or his/her deputy on the policy (e.g., via the organization's official e-mail, paper or electronic signature).
2-10-2	The cybersecurity requirements for technical vulnerabilities management must be implemented.
	Relevant cybersecurity tools: ● Vulnerability Management Process Template. ● Vulnerability Management Log Template. Control implementation guidelines ● Implement all cybersecurity requirements to the organization's approved vulnerabilities management. It is also recommended that the vulnerabilities management procedures cover the following, but not limited to: ○ Periodic vulnerability assessment and detection procedures ○ The mechanism for classifying vulnerabilities according to their severity. ○ Procedures for addressing vulnerabilities based on their classification and associated cyber risks. ○ Mechanism and procedure for escalation of technical vulnerabilities. ○ Methods of linking vulnerabilities management procedures to the security patch management procedures.
	Expected deliverables: ● Vulnerability Management Procedure ● Patch Management Procedures

	• Vulnerabilities detection and testing reports (pre- and post-treatment) indicating classification of vulnerabilities	
2-10-3	The cybersecurity requirements for technical vulnerabilities management must include at least the following:	
	2-10-3-1	Periodic vulnerabilities assessments.
	Control implementation guidelines • Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. • Identify technologies and tools to assess and detect vulnerabilities of information and technology assets. • Install and link vulnerabilities assessment and detection technologies and tools with the organization's information and technology assets. • Develop periodic plan and procedures to inspect and detect vulnerabilities in the information and technology assets in the organization, including: ○ Applications ○ Devices and servers ○ Databases ○ Organization's Networks	
	Expected deliverables: • Cybersecurity policy that covers the periodical assessment and detecting vulnerabilities (based on the plan and planned interval specified in the policy) of the following assets: ○ Applications ○ Devices and servers ○ Databases ○ Organization's Networks (e.g., electronic copy or official hard copy) • Formal approval by the head of the organization or his/her deputy on such requirements (e.g., via the organization's official e-mail, paper or electronic signature).	

	• Vulnerabilities management procedures and a periodic plan to assess and detect vulnerabilities • Periodic reports to assess and detect vulnerabilities	
	2-10-3-2	Vulnerabilities classification based on criticality level.
	Control implementation guidelines • Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. • Prepare and review vulnerabilities assessment reports on the information and technology assets in the organization, including the classification of vulnerabilities based on the following: ○ Description of vulnerabilities and their exploitative potential and the expected impact of the organization ○ Network segmentation ○ Classification of vulnerabilities by concerned assets ○ Classification of vulnerabilities based on Common Vulnerability Scoring System (CVSS)	
	Expected deliverables: • Cybersecurity policy that covers the vulnerabilities classification mechanism and methodology based on their criticality and cyber risks and based on the organization's network segmentation (e.g., electronic copy or official hard copy). • Formal approval by the head of the organization or his/her deputy on such document (e.g., via the organization's official e-mail, paper or electronic signature). • Vulnerabilities management procedures that illustrate the classification mechanism • Vulnerabilities detection and assessment reports indicating the classification of vulnerabilities	
	2-10-3-3	Vulnerabilities remediation based on classification and associated risk levels.
	Control implementation guidelines	

	• Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. • Share the organization's information and technology asset vulnerabilities assessment and detection reports with the relevant departments, including but not limited to: ○ Application management department ○ Workstations' department ○ Infrastructure department ○ Database management department ○ Network department • Ensure that the reports shared contain: ○ Vulnerabilities description ○ Name of the relevant assets in which vulnerabilities were assessed and detected ○ Vulnerabilities classification • Cooperate with the concerned departments to determine a time period and a plan to address the vulnerabilities, taking into account the vulnerabilities classification and classification of the relevant assets. • Develop a mechanism to ensure that vulnerabilities are addressed based on the plan.	
	Expected deliverables: • Cybersecurity policy that covers plans to address the identified vulnerabilities in the organization (e.g., electronic copy or official hard copy). • Formal approval by the head of the organization or his/her deputy on such document (e.g., via the organization's official e-mail, paper or electronic signature). • Vulnerability Management Procedure • Patch Management Procedures • Vulnerability assessment (before and after remedy)	
	2-10-3-4	Security patch management.
	Control implementation guidelines	

- Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.
- Link vulnerabilities management procedures to the security patch management procedures and change procedures.
- Analyze vulnerabilities assessment and detection reports to identify the organization's information and technology assets wo which security patches must be installed.
- Cooperate with the concerned departments to determine a time period and plan to install patches, taking into account the need for updating and classification of the relevant assets.

Expected deliverables:

- Cybersecurity policy and procedures that cover the security patch management requirements to address vulnerabilities. (e.g., electronic copy or official hard copy)
- Formal approval by the head of the organization or his/her deputy on such document (e.g., via the organization's official e-mail, paper or electronic signature).
- Vulnerability Management Procedure
- Patch Management Procedures
- Vulnerability assessment (before and after remedy)

2-10-3-5	Subscription with authorized and trusted cybersecurity resources for up-to-date information and notifications on technical vulnerabilities.

Control implementation guidelines

- Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.
- Identify and register with reliable sources regarding alerts for new and updated vulnerabilities. This includes:
    - National entities (e.g., NCA, NCSC)
    - Suppliers and Information and Technology Asset Manufacturers (OEMs)
    - Specialized cybersecurity groups in general and in the organization's sector

	○ Cybersecurity companies through their tools and technologies
	Expected deliverables: ● Cybersecurity policy that covers this control (e.g., electronic copy or official hard copy). ● Formal approval by the head of the organization or his/her deputy on such document (e.g., via the organization's official e-mail, paper or electronic signature). ● List of communication channels subscribed in to receive alerts on new vulnerabilities.
2-10-4	The cybersecurity requirements for technical vulnerabilities management must be reviewed periodically.
	Control implementation guidelines ● Review the cybersecurity requirements of Vulnerabilities Management by conducting a periodic assessment (according to a documented and approved plan for review, and based on a planned interval "e.g., quarterly") to implement identity and access management requirements by the Cybersecurity function and in cooperation with relevant departments (such as IT Department). ● Conduct application review through traditional channels (e.g., email) or automated channels using a compliance management system. The organization may develop a review plan explaining the implementation review schedule for Vulnerabilities Management. ● Review and update cybersecurity requirements for vulnerabilities management in the organization periodically according to a documented and approved plan for review and based on a planned interval or in the event of changes in relevant laws and regulations. ● Document the review and changes to the cybersecurity requirements for Vulnerabilities Management in the organization and approve them by the head of the organization or his/her deputy.
	Expected deliverables: ● Results of vulnerabilities management cybersecurity requirements implementation review in the organization

	• A document that defines the cybersecurity requirements implementation review cycle for vulnerabilities management in the organization (Compliance Assessment Schedule). • Compliance assessment report that outlines the assessment of the implementation of cybersecurity requirements for the organization's Vulnerabilities Management. • An approved document that sets the policy's review schedule • Policy indicating that it has been reviewed and updated, and that changes have been documented and approved by the head of the organization or his/her deputy. • Formal approval by the head of the organization or his/her deputy on the updated policy (e.g., via the organization's official e-mail, paper or electronic signature).

2-11	Penetration Testing
Objective	To assess and evaluate the efficiency of the organization's cybersecurity defense capabilities through simulated cyber-attacks to discover unknown weaknesses within the technical infrastructure that may lead to a cyber breach.
Controls	
2-11-1	Cybersecurity requirements for penetration testing exercises must be defined, documented and approved.
	Relevant cybersecurity tools: • Penetration Testing Policy Template. Control implementation guidelines • Develop and document cybersecurity policy for penetration testing in the organization, including the following:

	○ Determine the scope of the penetration test in the organization. ○ Define periodic penetration testing requirements. ○ Define penetration testing requirements using effective tools and methods. ○ Define the requirements for the team responsible for performing the penetration testing. ● Support the organization's policy by the Executive Management. This must be done through the approval of the organization head or his/ her deputy.	
	Expected deliverables: ● Cybersecurity policy that covers the requirements of penetration testing management (e.g., electronic copy or official hard copy). ● Formal approval by the head of the organization or his/her deputy on the policy (e.g., via the organization's official e-mail, paper or electronic signature).	
2-11-2	The cybersecurity requirements for penetration testing processes must be implemented.	
	Control implementation guidelines ● Implement all cybersecurity requirements to the organization's approved penetration testing. It is also recommended that the penetration testing cover the following, but not limited to: ○ Perform penetration testing periodically. ○ Determine the scope of the penetration testing in the organization.	
	Expected deliverables: ● Action plan for penetration testing ● Penetration Testing Reports	
2-11-3	The cybersecurity requirements for penetration testing processes must include at least the following:	
	2-11-3-1	Scope of penetration tests which must cover Internet-facing services and its technical components including infrastructure, websites, web applications, mobile apps, email and remote access.

Control implementation guidelines

- Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.
- Identify and document all services provided online at the organization.
- Identify all technical components that support these external services, including:
  - Websites and web applications
  - Smartphones and tablets applications
    - This includes items on Apple Store, Google Play Store and other app stores.
    - This also includes phone applications that are not available on stores, which are specific to the organization.
  - API
  - Servers used for external services (e.g., web servers)
  - Servers used for remote access services
  - Servers used by the email service
  - Network devices used to provide external services
- Develop and implement an action plan for penetration testing, including the above.

Expected deliverables:

- Cybersecurity policy that covers the penetration testing of the following assets: all services provided externally (online) and its technology components including infrastructure, websites, web applications, smartphone and tablet applications, email and remote access.
- Formal approval by the head of the organization or his/her deputy on such document (e.g., via the organization's official e-mail, paper or electronic signature).
- Action plan for penetration testing
- Penetration Testing Reports

2-11-3-2	Conducting penetration tests periodically.

Control implementation guidelines

	• Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. • Develop procedures for penetration testing. • Develop and implement an action plan for the penetration testing showing the annual schedule to be followed for penetration testing on the relevant information and technology assets.
	Expected deliverables: • Cybersecurity policy that covers penetration testing on a regular basis. • Formal approval by the head of the organization or his/her deputy on such document (e.g., via the organization's official e-mail, paper or electronic signature). • Action plan for penetration testing • Penetration Testing Reports
2-11-4	Cybersecurity requirements for penetration testing processes must be reviewed periodically.
	Control implementation guidelines • Review the cybersecurity requirements of penetration testing by conducting a periodic assessment (according to a documented and approved plan for review, and based on a planned interval ("e.g., quarterly") to implement identity and access management requirements by the Cybersecurity function and in cooperation with relevant departments (such as IT Department). • Conduct application review through traditional channels (e.g., email) or automated channels using a compliance management system. The organization may develop a review plan explaining the implementation review schedule for penetration testing. • Review and update cybersecurity requirements for penetration testing in the organization periodically according to a documented and approved plan for review and based on a planned interval or in the event of changes in relevant laws and regulations. • Document the review and changes to the cybersecurity requirements for penetration testing in the organization and approve them by the head of the organization or his/her deputy.

	Expected deliverables: • Results of penetration testing cybersecurity requirements implementation review in the organization • A document that defines the cybersecurity requirements implementation review cycle for penetration testing in the organization (Compliance Assessment Schedule). • Compliance assessment report that outlines the assessment of the implementation of cybersecurity requirements for the organization's penetration testing. • An approved document that sets the policy's review schedule • Policy indicating that it has been reviewed and updated, and that changes have been documented and approved by the head of the organization or his/her deputy. • Formal approval by the head of the organization or his/her deputy on the updated policy (e.g., via the organization's official e-mail, paper or electronic signature).

2-12	Cybersecurity Event Logs and Monitoring Management
Objective	To ensure timely collection, analysis and monitoring of cybersecurity events for early detection of potential cyber-attacks in order to prevent or minimize the negative impacts on the organization's operations.
Controls	
2-12-1	Cybersecurity requirements for event logs and monitoring management must be defined, documented and approved.
	Relevant cybersecurity tools: • Cybersecurity Event Logs and Monitoring Management Policy Template. Control implementation guidelines • Develop and document cybersecurity policy for event logs and cybersecurity monitoring management in the organization, including the following:

	○ Define the scope of information assets to which event logs must be activated. ○ Activate cybersecurity event logs on critical information assets in the organization. ○ Activate cybersecurity event logs of privileged access accounts on critical information assets and events of remote access in the organization. ○ Define technologies to collect activated cybersecurity event logs. ○ Continuous monitor cybersecurity event logs. ○ Define retention period for cybersecurity event logs (not less than 12 months). ● Support the organization's policy by the Executive Management. This must be done through the approval of the organization head or his/ her deputy.
	Expected deliverables: ● Cybersecurity policy that covers the requirements of Event Logs and Monitoring Management (e.g., electronic copy or official hard copy). ● Formal approval by the head of the organization or his/her deputy on such document (e.g., via the organization's official e-mail, paper or electronic signature).
2-12-2	The cybersecurity requirements for event logs and monitoring management must be implemented.
	Control implementation guidelines ● Implement cybersecurity requirements to Information System and Processing Facilities Protection, including, but not limited to, the following: ○ Define the scope of information assets to which event logs are activated, and the organization's information and technology asset register and the assets mentioned in the risk register can be used to determine the scope. ○ Activate cybersecurity event logs on critical information assets in the organization. ○ Activate cybersecurity event logs of privileged access accounts on critical information assets and events of remote access in the organization.

	○ Define technologies to collect activated cybersecurity event logs. ○ Define a team to continuously monitor cybersecurity event logs. ○ Define the retention period for cybersecurity event logs (not less than 12 months) and identify this item in contracts and agreements if the Security Operations Center is at the service provider premises and ensure compliance with it.	
	Expected deliverables: • A visit to the organization's Security Operations Center (if any), where the SIEM is viewed directly. • A copy of the contract or agreement if the Security Operations Center or the monitoring are provided by a service provider. • A report showing the connection of all the organization's devices and systems to the SIEM system. • Organization's shift breakdown table covering the approved monitoring model.	
2-12-3	The cybersecurity requirements for event logs and monitoring management must include at least the following:	
	2-12-3-1	Activation of cybersecurity event logs on critical information assets.
	Control implementation guidelines • Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. • Activate cybersecurity event logs on critical information assets in the organization, which may include, but are not limited to, the following: ○ Network Devices ○ Applications ○ Databases ○ Servers ○ Workstations (through the protection system). • Activate these records through the configuration of the previously mentioned devices and systems that can be controlled through their control panel.	

	● Develop rules in SIEM system to enable the monitoring team to monitor the activated records of critical information assets (after linking them).	
	Expected deliverables: ● A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. ● A screenshot or a direct example from the control panel of the mentioned systems that indicates the activation of event logs. ● Screenshot or a direct example showing the activation of logs through SIEM.	
	2-12-3-2	Activation of cybersecurity event logs on remote access and privileged user accounts.
	Control implementation guidelines ● Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. ● Activate cybersecurity event logs of privileged access accounts (e.g., database and systems management). ○ Information assets, so that all changes made through them are recorded and archived. ○ Remote access events, as these processes must only be for the necessary cases and any remote access must be recorded to follow up on the changes made. ● Develop a number of rules in the SIEM system so that the special team can monitor the activated logs of privileged access accounts (after linking them).	
	Expected deliverables: ● A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. ● Screenshot or a direct example showing the activation of logs for some privileged access accounts on the access management system. ● Screenshot or a direct example showing the activation of logs through SIEM. ● Screenshot or a direct example showing the activation of logs for some privileged access accounts on the remote access system. ● Screenshot or a direct example showing the activation of logs through SIEM.	

<table>
<tr><td rowspan="4"></td><td>2-12-3-3</td><td>Identification of required technologies (e.g., SIEM) for cybersecurity event logs collection.</td></tr>
<tr><td colspan="2">Control implementation guidelines
• Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.
• Provide the necessary technologies (SIEM) to collect cybersecurity event logs.
• Define the scope of devices, systems, and applications that are linked to SIEM based on their sensitivity, including but not limited to:
○ Workstations (through the protection system).
○ Applications
○ Databases
○ Network Devices
○ Servers
• Connect all the organization's critical devices and systems, including those previously mentioned to the Security Information and Event Management System (SIEM).
• Review the periodic linkage of the organization's devices and systems to ensure that all the aforementioned scope and any systems and devices found in the organizations are covered.</td></tr>
<tr><td colspan="2">Expected deliverables:
• A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control.
• A visit to the organization's Security Operations Center (if any), where the SIEM is viewed directly.
• A report showing the connection of all the organization's devices and systems with the SIEM system (including but not limited to a list in Excel or electronic version) and highlighting the addition of any new devices or systems in the organization.
• A contract explaining the above if the Security Operations Center is by a service provider.</td></tr>
<tr><td>2-12-3-4</td><td>Continuous monitoring of cybersecurity events.</td></tr>
</table>

Control implementation guidelines

- Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.
- Identify a team for continuous monitoring of cybersecurity event logs or SIEM and approve the 24/7 monitoring model, so that monitoring is performed around the clock on all days of the week.
- This team may consist of the organization's employees or by contracting an external monitoring service.
- If an external service is contracted for monitoring, the access location of the organization's SIEM system in the Kingdom, taking into consideration that this system is also available within the Kingdom.

Expected deliverables:

- A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control.
- Organization's shift breakdown table covering the approved monitoring model.
- A contract showing the monitoring model followed if the security operations center or the monitoring is provided by a service provider.

2-12-3-5	Retention period for cybersecurity event logs (must be 12 months minimum).

Control implementation guidelines

- Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.
- Define the retention period for cybersecurity event logs to be at least 12 months through SIEM management configurations.
- Provide enough space to keep these records.
- Review stored records periodically to ensure that records that have not been kept for less than one year have not been replaced by the latest and increase the size of the area if this occurs.

Expected deliverables:

	• A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control. • A screenshot or direct directory from the SIEM system showing record-keeping configuration for at least 12 months. • A sample of stored logs extracted from the SIEM system where records have been kept for at least 12 months.
2-12-4	The cybersecurity requirements for event logs and monitoring management must be reviewed periodically.
	Control implementation guidelines • Review the cybersecurity requirements of Cybersecurity Event Logs and Monitoring Management by conducting a periodic assessment (according to a documented and approved plan for review, and based on a planned interval "e.g., quarterly") to implement cybersecurity Event Logs and Monitoring Management requirements by the Cybersecurity function and in cooperation with relevant departments (such as security operations center, if any). • Conduct application review through traditional channels (e.g., email) or automated channels using a compliance management system. The organization may develop a review plan explaining the implementation review schedule for Cybersecurity Event Logs and Monitoring Management. • Review and update cybersecurity requirements for Cybersecurity Event Logs and Monitoring Management in the organization periodically according to a documented and approved plan for review and based on a planned interval or in the event of changes in relevant laws and regulations. • Document the review and changes to the cybersecurity requirements for Cybersecurity Event Logs and Monitoring Management in the organization and approve them by the head of the organization or his/her deputy.
	Expected deliverables: • Results of Cybersecurity Event Logs and Monitoring Management requirements implementation review in the organization. • A document that defines the cybersecurity requirements implementation review cycle for Cybersecurity Event Logs and Monitoring Management within the organization (Compliance Assessment Schedule).

	• Compliance assessment report that outlines the assessment of the implementation of cybersecurity requirements for Cybersecurity Event Logs and Monitoring Management • An approved document that sets the policy's review schedule • Policy indicating that it has been reviewed and updated, and that changes have been documented and approved by the head of the organization or his/her deputy. • Formal approval by the head of the organization or his/her deputy on the updated policy (e.g., via the organization's official e-mail, paper or electronic signature).

2-13	Cybersecurity Incident and Threat Management
Objective	To ensure timely identification, detection, effective management and handling of cybersecurity incidents and threats to prevent or minimize negative impacts on organization's operation taking into consideration the Royal Decree number 37140, dated 14/8/1438H.
2-13-1	Requirements for cybersecurity incidents and threat management must be defined, documented and approved.
	Relevant cybersecurity tools: • Cybersecurity Incident and Threat Management Policy Template. Control implementation guidelines • Develop and document cybersecurity policy for Cybersecurity Incident and Threat management in the organization, including the following: ○ Define a cybersecurity incident response plan. ○ Classify cybersecurity incidents by severity. ○ Define the roles and responsibilities for cybersecurity incident response and how to communicate with all stakeholders. ○ Define a mechanism for notifying the National Cybersecurity Authority in the event of a cybersecurity incident. ○ Share incidents notifications, threat intelligence, intrusion indicators and reports with NCA.

	○ Collect and handle threat intelligence feeds. ○ Periodically review of cybersecurity incident response plan. ● Support the organization's policy by the Executive Management. This must be done through the approval of the organization head or his/ her deputy.
	Expected deliverables: ● Cybersecurity policy that covers the requirements of Cybersecurity Incident and Threat management requirements in the organization (e.g., electronic copy or official hard copy). ● Formal approval by the head of the organization or his/her deputy on such document (e.g., via the organization's official e-mail, paper or electronic signature).
2-13-2	The requirements for cybersecurity incidents and threat management must be implemented.
	Control implementation guidelines ● Implement cybersecurity requirements to Cybersecurity Incident and Threat management, including, but not limited to, the following: ○ Define a cybersecurity incident response plan. ○ Classify cybersecurity incidents by severity. ○ Define the roles and responsibilities for cybersecurity incident response and how to communicate with all stakeholders. ○ Define a mechanism for notifying the National Cybersecurity Authority in the event of a cybersecurity incident. ○ Share incidents notifications, threat intelligence, intrusion indicators and reports with NCA ○ Collect and handle threat intelligence feeds. ○ Periodically review of cybersecurity incident response plan.
	Expected deliverables: ● The approved cybersecurity incident response plan (electronic copy). ● A sample of a previous cybersecurity incident report. ● Cybersecurity incidents classification mechanism based on severity.

2-13-3	The requirements for cybersecurity incidents and threat management must include at least the following:	
	2-13-3-1	Cybersecurity incident response plans and escalation procedures.
	Relevant cybersecurity tools: • Event Management Plan Template. • Event Management Procedure Template. Control implementation guidelines • Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. • Develop cybersecurity incident response plans containing: o Define the types of accidents and their classification according to their level of severity on the organization's business. o Define the roles and responsibilities for cybersecurity incident response and how to communicate with all stakeholders. o Define communication channels and methods for emergencies. o Define a playbook for incident response that contains the following: - Classify the incident by its severity, the level of response required, and entities that should be involved in response activities. - Report cybersecurity threats and incidents to the NCA. - Define workflow procedures for responding to cybersecurity incidents according to NCA's directions. • Develop cybersecurity incident report upon completion of the response including, but not limited to, the following: o Persons involved in responding to the incident and the means of communication. o The key information of the incident, including but not limited to, date and time, scope of incident, severity, etc. o Summary of the incident. o Containment and removal steps. o Current and future recommendations. • Review the response plan periodically and update it if necessary.	

Expected deliverables:

- A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control.
- The approved cybersecurity incident response plan (electronic copy).
- A sample of a previous cybersecurity incident report.

2-13-3-2	Cybersecurity incidents classification.

Control implementation guidelines

- Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.
- Define the organization's cybersecurity incident classification mechanism and ensure its inclusion in the incident response policy and its alignment with the organization's risk classification mechanism.
- Classify incidents if they occur and determine the duration and mechanism of dealing with these incidents based on the adopted classification mechanism.
- Document that classification in the cybersecurity incident report.

Expected deliverables:

- A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control.
- Document that outlines the mechanism for classifying cybersecurity incidents according to sensitivity and risk level.
- Sample from a previous incident report showing incident and reporting classification

2-13-3-3	Cybersecurity incidents reporting to NCA.

Control implementation guidelines

- Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.
- Identify documented procedures to report to NCA in the event of a cybersecurity incident, including:

  - The roles and responsibilities for cybersecurity incident response and how to communicate with all stakeholders.
  - The key information of the incident, including but not limited to, date and time, scope of incident, severity, etc.
  - Summary of the incident.
- Report to NCA the occurrence of a cybersecurity incident through NCA's approved channels, such as Haseen portal and/or the NCA official email for incident reporting "is@nca.gov.sa", and follow up on any updates and instructions that NCA may issue regarding incident reporting on an ongoing basis.

Expected deliverables:

- A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control.
- Copy of the file of the procedures followed to report to NCA cybersecurity incidents.
- Sample of NCA's notification of a previous cybersecurity incident, including but not limited to: a screenshot or direct example of the email sent to NCA.

2-13-3-4	Sharing incidents notifications, threat intelligence, breach indicators and reports with NCA.

Control implementation guidelines

- Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.
- Identify documented procedures to share the following with NCA:
  - Alerts, threat intelligence, and penetration indicators that may increase the level of suspicion of a cybersecurity incident.
  - Cybersecurity incident reports after the incident has been dealt with.
- Share alerts, threat intelligence, penetration indicators, and incident reports with NCA through the official e-mail to register the information sharing membership "info@nca.gov.sa" and follow up on any updates and instructions that the Authority may issue on reporting alerts, threat intelligence, and penetration indicators on an ongoing basis.

Expected deliverables:

- A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control.
- Procedures followed to share alerts, threat intelligence, and penetration indicators with NCA (including but not limited to: a previous email through which the indicators report was sent to NCA).
- Sample of a cybersecurity incident report sent to NCA (including but not limited to a previous email through which a cybersecurity incident report was sent to NCA).

2-13-3-5	Collecting and handling threat intelligence feeds.

Control implementation guidelines

- Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.
- Subscribe in platforms responsible for sending threat intelligence through email or other technical platforms. These platforms include:
  - Computer Emergency Response Team (Saudi CERT).
  - Haseen's information sharing platform.
  - CITC's newsletter.
  - Bulletins provided by cybersecurity companies.
  - Bulletins provided by security and technology service providers that have been previously contracted by the organization.
- Handle alerts sent by these platforms by:
  - Send alerts to the relevant team to deal with (including but not limited to: IT Department, Security Operations Center, update and vulnerability department).
  - Set a time limit for handling these alerts based on the severity level.
  - Continuously monitor to ensure that alerts sent to the relevant team have been handled in a secure manner (including but not limited to ensuring that the sent vulnerabilities patches are applied).

Expected deliverables:

- A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control.
- Screenshot or direct example showing the organization's subscription in a platform.

	• Screenshot or direct example of alerts that have been dealt with in advance according to the necessary procedures.
2-13-4	The requirements for cybersecurity incidents and threat management must be reviewed periodically.
	Control implementation guidelines • Review the cybersecurity requirements of cybersecurity incident and threat management by conducting a periodic assessment (according to a documented and approved plan for review, and based on a planned interval "e.g., quarterly") to implement cybersecurity incident and threat management requirements by the Cybersecurity function and in cooperation with relevant departments (such as IT Department). • Conduct application review through traditional channels (e.g., email) or automated channels using a compliance management system. The organization may develop a review plan explaining the implementation review schedule for cybersecurity incident and threat management. • Review and update cybersecurity requirements for cybersecurity incident and threat management in the organization periodically according to a documented and approved plan for review and based on a planned interval or in the event of changes in relevant laws and regulations. • Document the review and changes to the cybersecurity requirements for cybersecurity incident and threat management in the organization and approve them by the head of the organization or his/her deputy.
	Expected deliverables: • Results of Cybersecurity Incident and Threat management requirements implementation review in the organization. • A document that defines the cybersecurity requirements implementation review cycle for cybersecurity incident and threat management within the organization (Compliance Assessment Schedule). • Compliance assessment report that outlines the assessment of the implementation of cybersecurity requirements for cybersecurity incident and threat management.

2-14	Physical Security
Objective	To ensure the protection of information and technology assets from unauthorized physical access, loss, theft and damage.
Controls	
2-14-1	Cybersecurity requirements for physical protection of information and technology assets must be defined, documented and approved.
	Relevant cybersecurity tools: • Physical Security Policy Template. Control implementation guidelines • Include and document cybersecurity requirements for information and technology assets protection against unauthorized physical access and cyber risks, including, but not limited to: ○ Authorized access to critical areas within the organization. ○ CCTV. ○ Protection of facility entry/exit and surveillance records. ○ Secure destruction and re-use of physical assets that hold classified information. ○ Security of devices and equipment inside and outside the organization's facilities. • Cybersecurity requirements for the protection of information and technology assets in the organization against unauthorized physical access must be supported by the Executive Management. This must be done through the approval of the organization head or his/ her deputy.
	Expected deliverables: • A cybersecurity policy that covers the information and technology asset protection requirements against unauthorized physical access and cyber risks (e.g., electronic copy or official hard copy).

	• Formal approval by the head of the organization or his/her deputy on such document (e.g., via the organization's official e-mail, paper or electronic signature).
2-14-2	The cybersecurity requirements for physical protection of information and technology assets must be implemented.
	Control implementation guidelines • Implement all cybersecurity requirements for information and technology assets protection against unauthorized physical access, loss, theft, and vandalism. The procedures must cover at least the following, but not limited to: ○ Authorized access to critical areas within the organization. ○ CCTV. ○ Protection of facility entry/exit and surveillance records. ○ Secure destruction and re-use of physical assets that hold classified information. ○ Security of devices and equipment inside and outside the organization’s facilities. • Develop an action plan to implement all cybersecurity requirements for the protection of information and technology assets against unauthorized physical access, loss, theft and vandalism. • Include cybersecurity requirements for the protection of information and technology assets against unauthorized physical access, loss, theft, and vandalism in the protection procedures to ensure compliance with cybersecurity requirements for all internal and external stakeholders.
	Expected deliverables: • Documents that confirm the implementation of cybersecurity requirements related to the protection of information and technology assets against unauthorized physical access, loss, theft, and vandalism as documented in the policy. • An action plan to implement cybersecurity requirements for information and technology assets protection against unauthorized physical access, loss, theft, and vandalism.

	• Evidence that clarifies the implementation of information and technology asset protection controls against unauthorized physical access, loss, theft and vandalism, including, but not limited to: o An approved user access request form. o Schedule of a visit to CCTV log room to assess the monitoring process and the devices used. o Schedule of a visit to the secure storage room containing archived records. o Sample of the digital media destruction implementation (e.g., email). o Documented and approved procedures for the security of devices and equipment inside and outside the organization's facilities approved by the representative	
2-14-3	The cybersecurity requirements for physical protection of information and technology assets must include at least the following:	
	2-14-3-1	Authorized access to sensitive areas within the organization (e.g., data center, disaster recovery center, sensitive information processing facilities, security surveillance center, network cabinets).
	Control implementation guidelines • Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. • Identify the scope of the organization's critical areas, including (but not limited to): o Data centers. o Disaster Recovery Center. o Sensitive information processing facilities. o Security Control Center. o Network communication rooms. o Supply areas for hardware and technology hardware. • Develop access request form for critical areas, including (but not limited to): o Name of the concerned person. o Reason for requesting access. o Access duration • Develop approval procedures for the access request by administrators.	

- Identify access mechanism to critical areas (e.g., card access, fingerprint access, face access, etc.).
- Restrict the authority of managing the physical access system to individuals with specific authorities that can be audited and reviewed.
- Create a periodic schedule to review and update physical access authorities for critical areas.
- Review access authorities based on the established periodic table.
- Revoke access authorities after the expiry of the period documented in the application form approved by the representative.
- Ensure that third parties are not granted physical access to the organization's facilities until security requirements are met, provided that their arrival is monitored in the places where this is required.

Expected deliverables:

- A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control
- An approved user access request form.
- Schedule of visit to a critical area (data center but not limited to) to assess access
- Evidence of revoking access authorities after the expiry of the period documented on the approved application form (e.g., by email)

2-14-3-2	Facility entry/exit records and CCTV monitoring.

Control implementation guidelines

- Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.
- Define the scope of access and monitoring logs including (but not limited to):
  - All organization's buildings, including the main building and all its branches.
  - Critical areas based on risk assessment, which include data centers and communication rooms.
- Provide monitoring records for all buildings at the organization in several aspects, including:
  - Inside the building.

  - Outside the building.
  - Building corridors.
  - Entry and exit doors.

Expected deliverables:

- A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control
- Schedule of a visit to CCTV log room to assess the monitoring process and the devices used.
- Schedule of visit to the organization's buildings that contain surveillance cameras to assess their effectiveness, locations and monitoring.

2-14-3-3	Protection of facility entry/exit and surveillance records.

Control implementation guidelines

- Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.
- Adopt a separate location that includes access and monitoring logs to ensure their protection.
- Take the necessary measures to avoid loss of records (e.g., backups).
- Protect logs, information sources, and DVR from unauthorized access.
- Document and set a retention period for access and monitoring records.
- Develop periodic plan to archive access and monitoring records.
- Archive access and monitoring logs as per the periodic plan in a secure storage room containing CCTV monitoring devices.

Expected deliverables:

- A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control
- Schedule of a visit to the CCTV logroom to ensure that access and monitoring logs are protected in a separate location and secure access.
- Schedule of a visit to the secure storage room containing archived records.

	2-14-3-4	Secure destruction and re-use of physical assets that hold classified information (including documents and storage media).
	Control implementation guidelines • Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. • Identify the scope of physical assets containing classified information, including (but not limited to): o Paper documents. o Storage media. • Develop methodology and procedures for the destruction of physical assets containing classified information. • Provide the necessary devices for the destruction of physical assets containing classified information, including (but not limited to): o Shredder machine. o Hard Disk Destruction Machine. • Develop methodology and procedures for the reuse of physical assets containing classified information, including methods to erase and delete information such as degaussing and zero filling. • Document and approve procedures for reusing physical assets with classified information.	
	Expected deliverables: • A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control • Sample of the paper document destruction implementation (e.g., an email addressed to stakeholders confirming the destruction of the sample). • Sample of the digital media destruction implementation (e.g., email). • Procedures for reusing physical assets containing classified information documented and approved by the representative • Sample of the implementation of a physical asset reuse procedure containing classified information (e.g., a copy of the paper documents that have been destroyed and shared).	

2-14-3-5 Security of devices and equipment inside and outside the organization’s facilities.

Control implementation guidelines

- Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.
- Identify the scope of devices and equipment inside and outside the organization's buildings, including (but not limited to):
  - Data centers.
  - Disaster Recovery Center.
  - Sensitive information processing facilities.
  - Security Control Center.
  - Network communication rooms.
  - Supply areas for hardware and technology hardware.
- Develop procedures for the security of devices and equipment inside and outside the organization's premises.
- Develop documented and approved plan for the maintenance of devices and equipment inside and outside the organization's premises.
- Utilize technical solutions and equipment protection programs inside and outside buildings.
- Maintain equipment and devices inside and outside buildings periodically.
- Develop and approve physical security and safety regulations and procedures in the organization to include a precise definition of duties and tasks to serve as a general safety service framework to protect lives, assets and information.

Expected deliverables:

- A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control
- Documented and approved procedures for the security of devices and equipment inside and outside the organization’s facilities approved by the representative
- Sample of the implementation of the security of devices and equipment inside and outside the organization's buildings (e.g., maintenance schedule with review dates)

2-14-4	The cybersecurity requirements for physical protection of information and technology assets must be reviewed periodically.
	Control implementation guidelines ● Review the implementation of cybersecurity requirements for the organization's information and technology assets protection against unauthorized physical access, loss, theft, and vandalism by conducting a periodic assessment (as per a documented and approved audit plan, and based on a planned interval ("e.g., quarterly") to protect the organization’s information and technology assets against unauthorized physical access, loss, theft and vandalism by the cybersecurity function and in cooperation with relevant departments (such as the Security and Safety Department). ● Conduct application review through traditional channels (e.g., email) or automated channels using a compliance management system. The organization may develop a review plan explaining the implementation review schedule for the organization's information and technology assets protection against unauthorized physical access, loss, theft, and vandalism. ● Review and update cybersecurity requirements for information and technology assets protection against unauthorized physical access, loss, theft, and vandalism in the organization periodically according to a documented and approved plan for review and based on a planned interval or in the event of changes in relevant laws and regulations. ● Document the review and changes to the cybersecurity requirements for the information and technology assets protection against unauthorized physical access, loss, theft, and vandalism in the organization and approve them by the head of the organization or his/ her deputy.
	Expected deliverables: ● Results of information and technology assets protection against unauthorized physical access, loss, theft, and vandalism requirements implementation review in the organization. ● a document that defines the cybersecurity requirements implementation review cycle for information and technology assets protection against unauthorized physical access, loss, theft, and vandalism requirements implementation review in the organization (Compliance Assessment Schedule).

	• A compliance assessment report that shows the assessment of the implementation of cybersecurity requirements for information and technology assets protection against unauthorized physical access, loss, theft, and vandalism • An approved document that sets the policy's review schedule • Policy indicating that it has been reviewed and updated, and that changes have been documented and approved by the head of the organization or his/her deputy. • Formal approval by the head of the organization or his/her deputy on the updated policy (e.g., via the organization's official e-mail, paper or electronic signature).

2-15	Web Application Security
Objective	To ensure the protection of external web applications against cyber risks.
Controls	
2-15-1	Cybersecurity requirements for external web applications must be defined, documented and approved.
	Relevant cybersecurity tools: • Web Application Protection Policy Template. Control implementation guidelines • Include and document cybersecurity requirements for the organization's external web applications security against cyber risks, including, but not limited to: ○ Web Application Firewall. ○ Multi-tier Architecture. ○ Use secure protocols such as HTTPS. ○ Use of applications development and update standards and testing them. ○ Clarify secure user usage policy. ○ Multi-Factor Authentication of users' access.

	○ Screening for application-specific vulnerabilities (Vulnerability Assessment). ○ Regular backups in secure locations (Backup Log Files). ○ Regular screening of open ports, services, processes, and unused protocols. ● Cybersecurity requirements for the security of external web applications must be supported by the Executive Management. This must be done through the approval of the organization head or his/ her deputy.
	Expected deliverables: ● A cybersecurity policy that covers the requirements for the organization's external web applications security against cyber risks (electronic copy or official hard copy). ● Formal approval by the head of the organization or his/her deputy on such document (e.g., via the organization's official e-mail, paper or electronic signature).
2-15-2	The cybersecurity requirements for external web applications must be implemented.
	Control implementation guidelines ● Implement all cybersecurity requirements to External web applications security procedures in the organization. The External web applications security procedures must cover at least the following, but not limited to: ○ Web Application Firewall. ○ Multi-tier Architecture. ○ Use secure protocols such as HTTPS. ○ Clarify secure user usage policy. ○ Multi-Factor Authentication of users' access. ● Develop an action plan to implement all cybersecurity requirements related to external web applications security. ● Include cybersecurity requirements for external web applications security in the organization's external web applications security procedures to ensure compliance with cybersecurity requirements for all internal and external stakeholders.
	Expected deliverables:

	• Documents that confirm the implementation of cybersecurity requirements related to the protection of external web applications as documented in the policy. • An action plan document to implement the cybersecurity requirements for external web applications security • Evidence showing the implementation of external web applications security controls, including but not limited to: o Screenshot of web application firewall used by the organization. o Sample of web application designs that demonstrate the use of a multi-tier architecture principle for the organization's web application. o Screenshot from a web application showing the use of HTTPS in its link. o Screenshot from the organization's website indicating the publication of the secure usage policy for users. o Multiple screenshots showing entry process including MFA.	
2-15-3	The cybersecurity requirements for external web applications must include at least the following:	
	2-15-3-1	Use of web application firewall.
	Control implementation guidelines • Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. • Web applications must be identified, including: o Purchased external applications. o Internally developed applications. • If there are web applications purchased and operated by a third party, the following must be done: o Ensure the supplier's compliance with cybersecurity policies and standard controls including the use of a web application firewall system. • If there are internally developed applications or external applications purchased from a third-party that are operated by the organization, the following must be done:	

    - Identify the firewall technologies that the organization wishes to acquire, including but not limited to:
        - Firewall with pre-managed rules managed by the system itself.
        - A firewall with the option to customize the rules by the organization.
    - Identify and assign several application firewall systems that include the technologies supplied by the organization, while defining the positive and negative aspects of each system separately.
    - Identify and assign a specific firewall system to be used for the organization's external web applications
    - Implement and install the firewall system for all web applications operated by the organization.
- Include an application and install the firewall in the application development lifecycle to ensure the protection of future applications.

Expected deliverables:

- A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control
- Documents indicating the identification and documentation of the requirements of this ECC in the policies or procedures of the organization approved by the representative (e.g., electronic copy or official hard copy)
- Screenshot of web application firewall used by the organization.

2-15-3-2	Adoption of the multi-tier architecture principle.

Control implementation guidelines

- Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.
- Web applications must be identified, including:
    - Purchased external applications.
    - Internally developed applications.
- Current web applications used in the organization must be identified.
- If there are web applications purchased and operated by a third party, the following must be done:
    - Ensure the supplier's compliance with cybersecurity policies and standard controls including the use of multi-tier architecture principle.

- If there are internally developed applications or external applications purchased from a third-party that are operated by the organization, the following must be done:
  - Determine the tiers of the architecture principle appropriate to the nature of the web application, which must not be less than three tiers:
    - Database Tier
    - Business Tier
    - Presentation/Client Tier
  - Identify relevant departments to implement the multi-tiered architecture principle.
  - Apply the principle of multi-tier architecture, which must not be less than three tiers for all web applications of the organization.
- Include and use the multi-tier architecture principle in the application development life cycle to ensure the protection of future applications.

Expected deliverables:

- A document approved policy indicating the identification and documentation of the requirements related to this control
- A document approved procedure indicating the identification and documentation of the requirements related to this control
- Sample of web application designs that demonstrate the use of a multi-tier architecture principle for the organization's web application.
- Sample of web application designs that demonstrate the use of a multi-tier architecture principle for the organization's web application purchased from a third party.

2-15-3-3	Use of secure protocols (e.g., HTTPS).

Control implementation guidelines

- Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.
- Web applications must be identified, including:
  - Purchased external applications.
  - Internally developed applications.
- Current web applications used in the organization must be identified.

- If there are web applications purchased and operated by a third party, the following must be done:
    - Ensure the supplier's compliance with cybersecurity policies and standard controls including the use of secure protocols.
- If there are internally developed applications or external applications purchased from a third-party that are operated by the organization, the following must be done:
    - Define the secure communication protocol to be applied to the organization's web applications, including but not limited to:
        - Hypertext Transfer Protocol Secure (HTTPS)
        - Secure File Transfer Protocol (SFTP)
        - Transport Layer Security Protocol (TLS)
    - Implement and install secure communication protocols in the organization's external web applications to protect them.
- Include an application and install the secure communication protocols development lifecycle to ensure the protection of future applications.

Expected deliverables:

- A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control
- Screenshot from a web application showing the use of HTTPS in its link.

2-15-3-4	Clarification of the secure usage policy for users.

Control implementation guidelines

- Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.
- Document the secure use policy for the organization's web applications for users.
- Ensure that the secure use policy is shared on the organization's web applications through the external network (extranet) and not the intranet.

Expected deliverables:

- A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control

	• Secure Use of Web Application Users Policy. • Screenshot from the organization's website indicating the publication of the secure usage policy for users.	
	2-15-3-5	Multi-factor authentication for users’ access.
	Control implementation guidelines • Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. • Multi-Factor Authentication of user access to web application. (Whether web applications are purchased and operated by a third party, developed internally, or web applications purchased from a third party but operated by the organization). • Include the implementation requirement for multi-factor authentication in the application development lifecycle to ensure the protection of future applications.	
	Expected deliverables: • A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control • Multiple screenshots showing entry process including MFA.	
2-15-4	The cybersecurity requirements for external web applications must be reviewed periodically.	
	Control implementation guidelines • Review the cybersecurity requirements of external web applications security by conducting a periodic assessment (according to a documented and approved plan for review, and based on a planned interval ("e.g., quarterly") to implement identity and access management requirements by the Cybersecurity function and in cooperation with relevant departments (such as IT Department). • Conduct application review through traditional channels (e.g., email) or automated channels using a compliance management system. The organization may develop a review plan explaining the implementation review schedule for external web applications protection.	

	• Review and update cybersecurity requirements for external web applications security in the organization periodically according to a documented and approved plan for review and based on a planned interval or in the event of changes in relevant laws and regulations. • Document the review and changes to the cybersecurity requirements for external web applications security in the organization and approve them by the head of the organization or his/her deputy.
	Expected deliverables: • Results of external web applications protection requirements implementation review in the organization. • a document that defines the cybersecurity requirements application review cycle for the organization's external web applications (Compliance Assessment Schedule). • Compliance assessment report that outlines the assessment of the implementation of cybersecurity requirements for external web applications security • An approved document that sets the policy's review schedule • Policy indicating that it has been reviewed and updated, and that changes have been documented and approved by the head of the organization or his/her deputy. • Formal approval by the head of the organization or his/her deputy on the updated policy (e.g., via the organization's official e-mail, paper or electronic signature).

3 Cybersecurity Resilience

3-1	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)
Objective	To ensure the inclusion of the cybersecurity resiliency requirements within the organization's business continuity management and to remediate and minimize the impacts on systems, information processing facilities and critical e-services from disasters caused by cybersecurity incidents.
Controls	
3-1-1	Cybersecurity requirements for business continuity management must be defined, documented and approved.
	Relevant cybersecurity tools: ● Cybersecurity Business Continuity Policy Template Control implementation guidelines ● Include and document cybersecurity requirements within the organization's business continuity management, including but not limited to: ○ Ensure the continuity of cybersecurity-related systems and procedures. ○ Develop cybersecurity incident response plans that may affect the business continuity of the organization. ○ Develop Disaster Recovery Plan. ● Cybersecurity requirements within business continuity management must be supported by the Executive Management. This must be done through the approval of the organization head or his/ her deputy.
	Expected deliverables: ● Cybersecurity policy that covers the requirements of business continuity management (e.g., electronic copy or official hard copy). ● Formal approval by the head of the organization or his/her deputy on such document (e.g., via the organization's official e-mail, paper or electronic signature).

3-1-2	The cybersecurity requirements for business continuity management must be implemented.
	Control implementation guidelines ● Implement cybersecurity requirements within business continuity management that have been identified, documented, and approved in the policy. ● Develop an action plan to implement all cybersecurity requirements to ensure BCM in the organization. ● Include cybersecurity requirements for BCM in the organization's BCM procedures to ensure compliance with cybersecurity requirements for all internal and external stakeholders.
	Expected deliverables: ● Documents that confirm the implementation of cybersecurity requirements related to BCM as documented in the policy. ● An action plan to implement cybersecurity requirements for BCM in the organization. ● Evidence showing the implementation of BCM controls at the organization, including but not limited to: o Documented and approved business continuity plans for the organization. o Approved plans to respond to cybersecurity incidents that may affect the business continuity of the organization. o Reports on the implementation of disaster recovery plans tests at the organization.
3-1-3	The cybersecurity requirements for business continuity management must include at least the following:
	3-1-3-1 Ensuring the continuity of cybersecurity systems and procedures.
	Control implementation guidelines ● Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.

- Laws and regulations related to business continuity in the organization must be defined.
- Include high-risk cybersecurity incidents as a rationale for activating the organization's business continuity plan.
- Develop Business Continuity Management Program in the organization.
- Document and approve business continuity plans, including but not limited to:
  - Procedures for assessing risks that may affect the organization's business continuity.
  - Business Impact Analysis.
  - Definition of the cybersecurity systems, procedures and assets and their importance to the organization.
  - Cybersecurity-related systems continuity procedures, including technical requirements such as high availability, and regulatory requirements, such as the presence of a deputy that replaces the operators of cybersecurity systems when needed.
  - Definition of cybersecurity services and their importance to the organization and develop a plan to ensure the continuity of these services.
- Review the organization's business continuity plans periodically and update them if necessary.

Expected deliverables:

- A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control
- Documented and approved business continuity management program for the organization.
- Documented and approved business continuity plans for the organization.
- Formal approval by the head of the organization or his/her deputy on such documents (e.g., via the organization's official e-mail, paper or electronic signature).
- Reports on the implementation of the organization's business continuity plans tests.
- Report showing the sharing of the periodic meetings for sharing cybersecurity business continuity plans with the enterprise business continuity and involvement of stakeholders

	3-1-3-2	Developing response plans for cybersecurity incidents that may affect the business continuity.

Control implementation guidelines

- Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.
- Develop the plans for cybersecurity incident response that may affect the organization's business continuity, including (but not limited to):
    - An explanation of the types of accidents and their classification according to their impact on the organization's business continuity.
    - Roles and responsibilities for responding to cybersecurity incidents affecting the organization's business continuity.
    - Definition of incident response phases, including (but not limited to):
        - Planning and Preparation
        - Detection and Analysis
        - Containment, Eradication and Recovery
        - Review and Learn
    - Utilizing NCA published incident response playbooks.
- Include high-risk cybersecurity incidents as a rationale for activating the cybersecurity incident response plans.
- Draft a report on cybersecurity incidents affecting the organization's business continuity upon the completion of the response to include (but not limited to):
    - Persons involved in responding to the incident and the means of communication.
    - Basic information of the incident, including but not limited to:
        - Date and time.
        - Scope of incident.
        - Severity Level.
    - Summary of the incident.
    - Containment and removal steps.
    - Current and future recommendations.
- Review the response plans for cybersecurity incidents that may affect the organization's business continuity periodically and update them if necessary.

	Expected deliverables: ● A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control ● Approved plans to respond to cybersecurity incidents that may affect the business continuity of the organization. ● Formal approval by the head of the organization or his/her deputy on such documents (e.g., via the organization's official e-mail, paper or electronic signature).	
	3-1-3-3	Developing disaster recovery plans.
	Control implementation guidelines ● Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative. ● Develop disaster recovery plans, including (but not limited to): ○ Identify disaster recovery team. ○ Identify and assess disaster risk. ○ Conduct Business Impact Analysis (BIA) to identify critical systems within the organization. ○ Define backup and external storage procedures. ○ Test disaster recovery plans. ● Establish a disaster recovery center for critical systems. ● Conduct periodic tests to ensure the effectiveness of disaster recovery plans. ● Identify the requirements of periodic copies of the organization's systems to the recovery center.	
	Expected deliverables: ● A document (such as approved policy or procedure) indicating the identification and documentation of the requirements related to this control ● Organization -approved disaster recovery plans. ● Reports on the implementation of disaster recovery plans tests at the organization.	

	● Formal approval by the head of the organization or his/her deputy on such documents (e.g., via the organization's official e-mail, paper or electronic signature).
3-1-4	The cybersecurity requirements for business continuity management must be reviewed periodically.
	Control implementation guidelines ● Review and update cybersecurity requirements for business continuity in the organization periodically according to a documented and approved plan for review and based on a planned interval or in the event of changes in relevant laws and regulations. ● Document the review and changes to the cybersecurity requirements for business continuity management in the organization and approve them by the head of the organization or his/her deputy.
	Expected deliverables: ● An approved document that sets the policy's review schedule ● Policy indicating that it is up to date and the changes to the cybersecurity requirements for business continuity have been documented and approved by the head of the organization or his/her deputy. ● Formal approval by the head of the organization or his/her deputy on the updated policy (e.g., via the organization's official e-mail, paper or electronic signature).

4 Third-Party and Cloud Computing Cybersecurity

4-1	Third-Party Cybersecurity
Objective	To ensure the protection of assets against the cybersecurity risks related to third-parties including outsourcing and managed services as per organizational policies and procedures, and related laws and regulations.
Controls	
4-1-1	Cybersecurity requirements for contracts and agreements with third-parties must be identified, documented and approved.
	Relevant cybersecurity tools: ● Third-party Cybersecurity Policy Template. Control implementation guidelines ● Develop and document cybersecurity policy for Third-Party Cybersecurity in the organization, including the following: ○ Cybersecurity requirements within contracts and agreements with third parties. ○ Third-party risk assessment procedures. ○ Data and Information Protection. ○ Cybersecurity Incident Management. ● Support the organization's policy by the Executive Management. This must be done through the approval of the organization head or his/ her deputy.
	Expected deliverables: ● Cybersecurity policy that covers the requirements of contracts and agreements with third- parties (e.g., electronic copy or official hard copy). ● Formal approval by the head of the organization or his/her deputy on the policy (e.g., via the organization's official e-mail, paper or electronic signature).

4-1-2

The cybersecurity requirements for contracts and agreements with third-parties (e.g., Service Level Agreement (SLA)) -which may affect, if impacted, the organization's data or services- must include at least the following:

4-1-2-1 Non-disclosure clauses and secure removal of organization's data by third parties upon end of service.

Control implementation guidelines

- Define and document the requirements of this control in the cybersecurity requirements and approve them by the representative, provided that the cybersecurity requirements include non-disclosure requirements and secure removal by the third party of the organization's data upon service termination.
- Include in the organization's contracts with third party's clauses stating the third party's commitment to maintain the confidentiality of the information.
- Include in the organization's contracts with third parties clauses stating that the third party must be obligated to safely remove the organization's data upon the expiry of the contract/service period.

Expected deliverables:

- Cybersecurity policy that covers the requirements of contracts and agreements with third- parties (e.g., electronic copy or official hard copy).
- Signed sample of a contract or agreement with third parties indicating the inclusion of confidentiality clauses and secure removal of data (hard copy or electronic copy).

4-1-2-2 Communication procedures in case of cybersecurity incidents.

Control implementation guidelines

- Define and document the requirements of this control in the cybersecurity requirements document and approve them by the representative, provided that they include the requirements of the communication procedures in the event of a cybersecurity incident.
- Include in the organization's contracts with third parties clauses stating the third party's obligation to define the communication procedures in the event of a cybersecurity incident.

- Ensure that third parties develop communication procedures with the organization, including communication means and data in the event of a cybersecurity incident that may affect the organization's data or service provided by the third party. These requirements include:
  - Communication data (e.g., e-mail).
  - The mechanism for reporting the cybersecurity incident (and its classification) to the organization.
  - Escalation mechanisms.

Expected deliverables:

- Cybersecurity policy that covers the requirements of contracts and agreements with third- parties (e.g., electronic copy or official hard copy).
- Procedures adopted with third parties to communicate in the event of a cybersecurity incident through which the organization's data or service may be affected.

4-1-2-3	Requirements for third-parties to comply with related organizational policies and procedures, laws and regulations.

Control implementation guidelines

- Define and document the requirements of this control in the cybersecurity requirements document and approve them by the representative, provided that they include the requirements of third parties' obligation to apply the organization's cybersecurity requirements and policies and the relevant laws and regulations.
- Include in the organization's contracts with third parties clauses stating that the third party must be obligated to implement the organization's cybersecurity requirements and policies and the relevant laws and regulations.

Expected deliverables:

- Cybersecurity policy that covers the requirements of contracts and agreements with third- parties (e.g., electronic copy or official hard copy).
- Signed sample of a contract or agreement with third parties indicating the obligation of third parties to apply the organization’s cybersecurity requirements and policies and the relevant laws and regulations.

<table>
<tr><td rowspan="6">4-1-3</td><td colspan="2">The cybersecurity requirements for contracts and agreements with IT outsourcing and managed services third-parties must include at least the following:</td></tr>
<tr><td>4-1-3-1</td><td>Conducting a cybersecurity risk assessment to ensure the availability of risk mitigation controls before signing contracts and agreements or upon changes in related regulatory requirements.</td></tr>
<tr><td colspan="2">Control implementation guidelines
● Define and document the requirements of this control in the cybersecurity requirements document and approve them by the representative, provided that they include the requirements of conducting a cybersecurity risk assessment, and ensuring that there is a guarantee to control those risks before signing contracts and agreements or in the event of changes in the relevant laws and regulations.
● Conduct a third-party cybersecurity risk assessment by the organization in the following cases:
○ Before the organization signs any contracts or agreements with third parties.
○ In the event of changes in relevant laws and regulations.</td></tr>
<tr><td colspan="2">Expected deliverables:
● Cybersecurity policy that covers the requirements of contracts and agreements with third- parties (e.g., electronic copy or official hard copy).
● Sample of the third-party cyber risk assessment report before signing the contract or in the event of changes in relevant laws and regulations.</td></tr>
<tr><td>4-1-3-2</td><td>Cybersecurity managed services centers for monitoring and operations must be completely present inside the Kingdom of Saudi Arabia.</td></tr>
<tr><td colspan="2">Control implementation guidelines
● Define and document the requirements of this control in the cybersecurity requirements document and approve them by the representative, provided that they include the requirements for the managed operation and monitoring cybersecurity operations centers, which use remote access method, to be located within the Kingdom.</td></tr>
</table>

	• Ensure that Cybersecurity operation centers managed for operation and monitoring are located within the Kingdom. • Ensure that remote access to Cybersecurity operation centers managed for operation and monitoring is performed within the Kingdom. • Include a clause in the contract or service level agreement signed with the third party that obliges the third party to have operations centers for operating and monitoring cybersecurity services, which use remote access within the Kingdom.
	Expected deliverables: • Cybersecurity policy that covers the requirements of contracts and agreements with third- parties (e.g., electronic copy or official hard copy). • A sample of the evidence of hosting or managing the cybersecurity operations center within the Kingdom (e.g., as an item of the signed contract or having a Service Level Agreement (SLA) signed between the third party and the organization).
4-1-4	The cybersecurity requirements for contracts and agreements with third-parties must be reviewed periodically.
	Control implementation guidelines • Review and update cybersecurity requirements for third party cybersecurity in the organization periodically according to a documented and approved plan for review and based on a planned interval or in the event of changes in relevant laws and regulations. • Document the review and changes to the cybersecurity requirements for third party cybersecurity in the organization and approve them by the head of the organization or his/her deputy.
	Expected deliverables: • An approved document that sets the policy's review schedule • Policy indicating that it has been reviewed and updated, and that changes have been documented and approved by the head of the organization or his/her deputy.

	• Formal approval by the head of the organization or his/her deputy on the updated policy (e.g., via the organization's official e-mail, paper or electronic signature).

4-2	Cloud Computing and Hosting Cybersecurity
Objective	To ensure the proper and efficient remediation of cyber risks and the implementation of cybersecurity requirements related to hosting and cloud computing as per organizational policies and procedures, and related laws and regulations. It is also to ensure the protection of the organization’s information and technology assets hosted on the cloud or processed/managed by third-parties.
Controls	
4-2-1	Cybersecurity requirements related to the use of hosting and cloud computing services must be defined, documented and approved.
	Relevant cybersecurity tools: • Cloud Computing and Hosting Cybersecurity Policy Template Control implementation guidelines • Develop and document cybersecurity policy for cloud computing and hosting services in the organization, including the following: o Cloud computing and hosting services providers contract requirements. o Requirements for the location of hosting and storing the organization's systems and data. o Requirements for data removal and retrieval. o Classification of data prior to hosting/ storing on cloud computing or hosting services. o inclusion of Service Level Agreement "SLA". o Inclusion of Non-disclosure Clauses. • Support the organization's policy by the Executive Management. This must be done through the approval of the organization head or his/ her deputy.
	Expected deliverables:

	• Cybersecurity policy that covers the requirements of the use of cloud computing and hosting services (e.g., electronic copy or official hard copy). • Formal approval by the head of the organization or his/her deputy on the policy (e.g., via the organization's official e-mail, paper or electronic signature).
4-2-2	The cybersecurity requirements related to the use of hosting and cloud computing services must be implemented.
	Control implementation guidelines • Implement cybersecurity requirements for cloud computing and hosting services for the organization, including, but not limited to: ○ Ensure that the location of hosting and storing the organization's information is within the Kingdom. ○ Ensure the activation of event logs on hosted information assets. ○ Ensure that cloud computing and hosting service providers must return data (in a usable format) and remove it in a non-recoverable manner upon termination/expiry of the service. ○ Ensure that the organization's environment (including virtual servers, networks and databases) is separated from other entities' environments in cloud computing services. ○ Ensure that data and information transmitted to, stored in, or transmitted from cloud services are encrypted in accordance with the relevant laws and regulations of the organization. ○ Ensure that the cloud computing and hosting service provider must periodically backup and protect backups in accordance with the organization's backup policy. • The organization may also develop an action plan to implement cybersecurity requirements related to cloud computing and hosting service, in order to ensure that the organization complies with all cybersecurity requirements for all internal and external stakeholders and follow up and monitor them periodically to ensure implementation. • Ensure continuous compliance with cloud computing cybersecurity controls for (CCC).
	Expected deliverables:

	• An action plan to implement the cybersecurity requirements for cloud computing and hosting services. • A signed sample of the agreement or contract between the organization and the cloud service provider. • Evidence by the cloud computing service provider of the implementation of the cybersecurity requirements of cloud computing and hosting services.	
4-2-3	In line with related and applicable laws and regulations, and in addition to the applicable ECC controls from main domains (1), (2), (3) and subdomain (4-1), the cybersecurity requirements related to the use of hosting and cloud computing services must include at least the following:	
	4-2-3-1	Classification of data prior to hosting on cloud or hosting services and returning data (in a usable format) upon service completion.
	Control implementation guidelines • Ensure that data is classified before being hosted by cloud computing and hosting service providers, ensuring that such data is handled according to that classification and that such data is returned by the service provider upon the expiry of the contract/service with the organization through the following steps: o Identify all data to be sent to the cloud computing service provider. o Classify and label the identified data in line with the data classification and labelling mechanism in the organization and the related laws and regulations. o Share this data with the cloud service provider for cloud hosting. o Develop procedures to ensure data is returned by the cloud computing service provider (in a usable format) after the contract/service ends.	
	Expected deliverables: • Cybersecurity policy that covers the requirements of the use of cloud computing and hosting services (e.g., electronic copy or official hard copy). • Sample of the data list that was classified before hosting it with cloud computing service providers, including but not limited to (a file) showing the data that were classified, prior to sharing with the cloud service provider • A signed sample of the agreement or contract between the organization and the cloud service provider.	

		● Approved procedures for data return after the termination of cloud computing services. ● Classification policies and procedures for data to be hosted on computing and hosting services. ● Up to date list of hosted services and their classification
	4-2-3-2	Separation of organization’s environments (specifically virtual servers) from other environments hosted at the cloud service provider.
		Control implementation guidelines ● Define the organization's environment separation requirements (especially virtual servers) from other entities' environments in cloud computing services. ● Include in the organization's contracts with cloud computing and hosting providers clauses stating that the organization's environment must be separated from other entities' environments in the cloud computing services.
		Expected deliverables: ● Cybersecurity policy that covers the requirements of the use of cloud computing and hosting services (e.g., electronic copy or official hard copy). ● Evidence that outlines the separation of the organization's environment from other entities' environments in cloud computing services (e.g., as an item of the signed contract or having an agreement signed between the service provider and the organization). ● Evidence by the cloud computing service provider' that the organization's environment is separated from other entities' environments in cloud computing services.
	4-2-3-3	Organization’s information hosting and storage must be inside the Kingdom of Saudi Arabia.
		Control implementation guidelines ● Ensure that the documented and approved policy includes the requirements for the location of hosting and storing the organization's information and must be within the Kingdom.

	• Ensure that the location of hosting and storing the organization's information is within the Kingdom by, but not limited to: ○ Include a clause in the contract or service level agreement signed with the service provider that data storage must be within the Kingdom. ○ Include a clause regarding the service provider's compliance with the controls of NCA related to cloud computing and hosting services, taking into account the classification of hosted data.
	Expected deliverables: • Cybersecurity policy that covers the requirements of the use of cloud computing and hosting services (e.g., electronic copy or official hard copy). • Evidence of the location of hosting and storing the organization's information within the Kingdom (e.g., one of the clauses of the signed contract or service level agreement (SLA) signed between the service provider and the organization). • Evidence by the service provider proving the storage of data within the Kingdom.
4-2-4	The cybersecurity requirements related to the use of hosting and cloud computing services must be reviewed periodically.
	Control implementation guidelines • Review and update the cybersecurity policy that covers the requirements of using cloud computing and hosting services periodically according to a documented and approved plan for review based on a planned interval (e.g., periodic review must be conducted annually). • Review and update the cybersecurity policy covering the requirements of using cloud computing and hosting services in the event of changes in the relevant laws and regulations (for example, when a new cybersecurity law is issued that applies to the organization). • Document the review and changes to the cybersecurity requirements for cloud computing and hosting services in the organization and approve them by the head of the organization or his/her deputy.
	Expected deliverables: • An approved document that sets the policy's review schedule

	● Policy indicating that it is up to date and the changes to the cybersecurity requirements for cloud computing and hosting services have been documented and approved by the head of the organization or his/ her deputy. ● Formal approval by the head of the organization or his/her deputy on the updated policy (e.g., via the organization's official e-mail, paper or electronic signature).

5 Industrial Control Systems Cybersecurity

5-1	Industrial Control Systems (ICS) Protection
Objective	To ensure the appropriate and effective cybersecurity management of Industrial Controls Systems and Operational Technology (ICS/OT) to protect the confidentiality, integrity and availability of the organization's assets against cyber attacks (e.g., unauthorized access, destruction, spying and fraud) in line with the organization's cybersecurity strategy and related and applicable local and international laws and regulations.
Controls	
5-1-1	Cybersecurity requirements related to Industrial Controls Systems and Operational Technology (ICS/OT) must be defined, documented and approved.
	Relevant cybersecurity tools: • Industrial Control Systems (ICS) Cybersecurity Policy Template. Control implementation guidelines • Develop and document cybersecurity policy for ICS/OT in the organization, including the following: ○ Requirements for the protection of industrial production networks and requirements for linking them with other networks. ○ Requirements for the protection of ICS and restrict access. ○ Requirements for Cybersecurity Incident Management for Industrial Control Systems. • Support the organization's policy by the Executive Management. This must be done through the approval of the organization head or his/ her deputy.
	Expected deliverables: • Cybersecurity policy that covers the requirements of the protection of ICS/OT (e.g., electronic copy or official hard copy). • Formal approval by the head of the organization or his/her deputy on the policy (e.g., via the organization's official e-mail, paper or electronic signature).

5-1-2		The cybersecurity requirements related to Industrial Controls Systems and Operational Technology (ICS/OT) must be implemented.
		Control implementation guidelines • Implement all cybersecurity requirements for the protection of ICS/OT, including operational systems cybersecurity controls. • Develop an action plan to implement all cybersecurity requirements for the protection of ICS/OT. • Include cybersecurity requirements for the protection of ICS/OT in the organization's procedures to ensure compliance with cybersecurity requirements for all internal and external stakeholders.
		Expected deliverables: • An action plan to implement the cybersecurity requirements for the protection of ICS/OT. • Sample of the design plan of the industrial production network (electronic or hard copy). • Protection procedures for ICS/OT
5-1-3		In addition to the applicable ECC controls from the main domains (1), (2), (3) and (4), the cybersecurity requirements related to Industrial Controls Systems and Operational Technology (ICS/OT) must include at least the following:
	5-1-3-1	Strict physical and virtual segmentation when connecting industrial production networks to other networks within the organization (e.g., corporate network).
		Control implementation guidelines • Ensure that the approved documented policy includes the requirements of restriction and physical and logical segregation when connecting industrial production networks (ICS/OT) with other networks in the organization. • All ICS/OT networks in the organization must be defined. • Identify cyber risks associated with connecting industrial production networks with other networks.

- Isolate industrial production networks (ICS/OT) from other networks physically or logically based on cyber risks, including:
  - Corporate network
  - Industrial demilitarized zone
- Ensure that industrial production networks are not linked with other networks in the organization except for necessary communications and ensure the restriction and physical and logical segregation in the event of connectivity.

Expected deliverables:

- Cybersecurity policy that covers the requirements of the protection of ICS/OT (e.g., electronic copy or official hard copy).
- The design plan of the industrial production network (electronic copy or hard copy) indicating how it connects to the organization's corporate network.

5-1-3-2	Strict physical and virtual segmentation when connecting systems and industrial networks with external networks (e.g., Internet, remote access, wireless).

Control implementation guidelines

- Ensure that the approved documented policy includes the requirements of restriction and physical and logical segregation when connecting industrial systems or networks with external networks.
- All ICS/OT systems and networks in the organization must be defined.
- Identify and assess the cyber risks of connecting industrial systems and networks with external networks
- Isolate industrial systems and networks from external networks physically or logically based on cyber risks, including:
  - The Internet
    - Proxy and DMZ access
  - Remote Access
    - Use of secure remote access (VPN), jump server and MFA
  - Wireless Network
    - Use secure wireless protocols based on national cryptography standard controls (NCS-1:2020)

	• Ensure that industrial production networks are not linked with other networks in the organization except for necessary communications and ensure the restriction and physical and logical segregation in the event of connectivity.	
	Expected deliverables: • Cybersecurity policy that covers the requirements of the protection of ICS/OT (e.g., electronic copy or official hard copy). • The design plan of the industrial production network (electronic copy or hard copy) indicating how it connects to the external networks.	
	5-1-3-3	Continuous monitoring and activation of cybersecurity event logs on the industrial networks and its connections.
	Control implementation guidelines • Ensure that the approved documented policy includes the requirements for activating and continuously monitoring the cybersecurity event logs of industrial network and its associated communications. • All ICS/OT networks in the organization must be defined. • Enable the collection of cybersecurity event logs for industrial network and its associated communications as much as possible. • Link the cybersecurity event logs of industrial network and the associated communication to SIEM, taking into account: o The system must be qualified by the suppliers of industrial systems and networks in the organization o The system must be isolated (at least logical) • Cooperate with the organization's industrial systems and networks vendors and industrial system and network specialists to identify rules and use cases for industrial network cybersecurity event logs and associated communications. • Assign a dedicated team to monitor records 24/7.	
	Expected deliverables: • Cybersecurity policy that covers the requirements of the protection of ICS/OT (e.g., electronic copy or official hard copy). • Screenshot of the activation of the cybersecurity event logs of the associated network.	

- Evidence of continuous monitoring of event logs (e.g., the team that is approved and dedicated to monitoring and controlling these logs).

5-1-3-4 Isolation of Safety Instrumental Systems (SIS).

Control implementation guidelines

- Ensure that the approved documented policy includes requirements for the isolation of Safety Instrumented System.
- All safety equipment systems in the organization must be defined.
- Identify and assess the cyber risks associated with connecting Safety Instrumented Systems with other systems.
- Isolate Safety Instrumented Systems from other systems based on the following:
    - Physical or logical isolation based on cyber risks and Safety Instrumented Systems guidelines and providers.
    - Type of isolation to be applied, including:
        - Safety Instrumented Systems (SIS) isolation from engineering workstations
        - Safety Instrumented Systems isolation from industrial systems
        - Safety Instrumented Systems isolation from other networks

Expected deliverables:

- Cybersecurity policy that covers the requirements of the protection of ICS/OT (e.g., electronic copy or official hard copy).
- Design plan of the approved Safety Instrumented Systems network (electronic copy or hard copy).

5-1-3-5 Strict limitation on the use of external storage media.

Control implementation guidelines

- Ensure that the approved documented policy includes requirements for restricted use of external storage media.
- Configure systems and technologies to prevent the use of external storage media automatically. This may include:
    - Configure industrial systems protection techniques to prevent the use of external storage media automatically; or

  - Configure central service system (e.g., Active Directory) to prevent the use of external storage media automatically; or
  - Configure devices registry to prevent the use of external storage media automatically
- Develop and approve procedures to use external storage media, (including, but not limited to, requesting approvals via e-mail, paper, or through an internal system). Such procedures include:
  - Reason for requesting approval for use.
  - Usage duration.
- Define the mechanism for handling data stored in storage media to be inspected before use and erased after completion.

Expected deliverables:

- Cybersecurity policy that covers the requirements of the protection of ICS/OT (e.g., electronic copy or official hard copy).
- Screenshot showing the restriction of the use of external storage media on industrial systems.
- Procedures for restricting the use of external storage media on industrial systems, while proving the application of these procedures (e.g., procedures for approving use through emails, a hard copy or electronic copy of the use approval form).

5-1-3-6	Strict limitation on connecting mobile devices to industrial production networks.

Control implementation guidelines

- Ensure that the approved documented policy includes requirements for the restriction of mobile device connectivity to the industrial production network.
- Identify, implement and control appropriate technologies for network access control.
- Define appropriate and advanced technologies to authenticate mobile devices (e.g., RADIUS, MAC Authentication).
- Ensure that the mobile devices' connectivity to the industrial production network is not basically activated and that this connectivity is restricted if there is a need to activate it.

- Develop and approve procedures to use mobile devices, (including, but not limited to, requesting approvals via e-mail, paper, or through an internal system). Such procedures include:
  - Reason for requesting approval for use.
  - Usage duration.
- Define the mechanism for handling data stored in mobile devices to be inspected before use and erased after completion.

Expected deliverables:

- Cybersecurity policy that covers the requirements of the protection of ICS/OT (e.g., electronic copy or official hard copy).
- Screenshot showing the restriction of connectivity of mobile devices to industrial systems.
- Procedures for restricting the connectivity of mobile devices to the industrial production network, while proving the application of these procedures (e.g., procedures for approving potential connectivity through emails, a hard copy or electronic copy of the approval form).

5-1-3-7	Periodic review and secure configuration and hardening of industrial, automated, support systems, and devices.

Control implementation guidelines

- Ensure that the approved documented policy includes the requirements to periodically review the Secure Configuration and Hardening of industrial systems, support systems and industrial machinery.
- Identify all industrial systems, support systems and industrial machinery in the organization.
- Develop hardening standard controls for industrial systems, support systems, and industrial machinery in cooperation with system providers and manufacturers.
- Document and implement an action plan to review Secure Configuration and Hardening of industrial systems, support systems and industrial machinery on a regular basis or using automated tools.
- Work with the concerned departments to develop a corrective plan for configuration and hardening review results.

	Expected deliverables: • Cybersecurity policy that covers the requirements of the protection of ICS/OT (e.g., electronic copy or official hard copy). • Reports on the review of Secure Configuration and Hardening of industrial systems, support systems, and industrial machinery, indicating their periodic application.	
	5-1-3-8	Vulnerability management for industrial control systems and operational technology (ICS/OT).
	Control implementation guidelines • Ensure that the approved documented policy includes the requirements for ICS/OT Vulnerability Management. • ICS in the organization must be defined. • Identify appropriate technologies for ICS/OT vulnerabilities assessment, provided that they are qualified by industrial systems providers and manufacturers. • Analyze the impact of the ICS/OT vulnerabilities assessment and determine whether it is invasive or non-invasive and develop a contingency plan. • Schedule and conduct vulnerabilities assessment based on the approved plan. • Work with the concerned departments to develop a plan to address vulnerabilities.	
	Expected deliverables: • Cybersecurity policy that covers the requirements of the protection of ICS/OT (e.g., electronic copy or official hard copy). • ICS/OT Vulnerability review report, outlining the procedures used to manage vulnerabilities.	
	5-1-3-9	Patch management for industrial control systems and operational technology (ICS/OT).
	Control implementation guidelines	

	• Ensure that the approved documented policy includes requirements for ICS/OT Patch Management. • Identify the organization's ICS/OT and determine their criticality, in accordance with the relevant laws and regulations. • Identify approved communication channels in the organization with the systems suppliers and manufacturers to know the latest security ICS/OT Patch. • Develop approved procedures and plans for the management of patches for industrial systems. • Analyze the impact of implementing patches on industrial systems while developing a contingency plan. • Work with the concerned departments to test patches according to the approved procedures. • Schedule and implement ICS/OT Patch based on the approved plan.	
	Expected deliverables: • Cybersecurity policy that covers the requirements of the protection of ICS/OT (e.g., electronic copy or official hard copy). • ICS/OT Patch review report outlining the patch management procedures.	
	5-1-3-10	Cybersecurity applications management related to the protection of the industrial systems from viruses and malware.
	Control implementation guidelines • Ensure the approved documented policy includes the requirements to manage industrial cybersecurity programs for protection against viruses, suspicious malware and malicious malware • Identify the organization's ICS/OT and determine their criticality, in accordance with the relevant laws and regulations. • Identify appropriate technologies for protection against viruses, suspicious malware and malicious malware, provided that they are approved by industrial systems providers and manufacturers. • Implement and develop antivirus and malware protection tools for industrial systems based on the procedures of industrial systems providers and manufacturers.	

	• Review the tools for industrial systems protection against viruses and suspicious malware and malicious malware periodically to ensure the comprehensiveness of the protection tools. • Develop procedures for the safe management of antivirus and suspicious malware and malicious malware protection tools.
	Expected deliverables: • Cybersecurity policy that covers the requirements of the protection of ICS/OT (e.g., electronic copy or official hard copy). • Updated list of industrial systems protection against viruses, suspicious malware and malicious malware. • Reports on the update of protection against viruses, suspicious malware and malicious malware.
5-1-4	The cybersecurity requirements related to Industrial Controls Systems and Operational Technology (ICS/OT) must be reviewed periodically.
	Control implementation guidelines • Review and update the cybersecurity policy and requirements for ICS/OT in the organization periodically according to a documented and approved plan for review and based on a planned interval (e.g., review must be conducted annually) or in the event of changes in relevant laws and regulations. Document the review and changes to the cybersecurity requirements for ICS/OT protection in the organization and approve them by the head of the organization or his/her deputy.
	Expected deliverables: • An approved document that sets the policy's review schedule • Policy indicating that it is up to date and the changes to the cybersecurity requirements for ICS/OT protection have been documented and approved by the head of the organization or his/her deputy. • Formal approval by the head of the organization or his/her deputy on the updated policy (e.g., via the organization's official e-mail, paper or electronic signature).

الهيئـــة الوطنيـــة
للأمـــن السيبـــراني
National Cybersecurity Authority