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 S ructure 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 R sk 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.

<table>
<tr><td></td><td>

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.

</td></tr>
<tr><td></td><td>
Expected deliverables :

The approved cybersecurity risk management methodology (electronic copy or official hard copy).
Approved cybersecurity risk management procedures.

</td></tr>
<tr><td>1-5-2</td><td>The cybersecurity risk management methodology and procedures must be implemented by the cybersecurity function.</td></tr>
<tr><td></td><td>
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.

</td></tr>
<tr><td></td><td>
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.

</td></tr>
<tr><td>1-5-3</td><td>The cybersecurity risk assessment procedures must be implemented at least in the following cases:
<table>
<tr><td>1-5-3-1</td><td>Early stages of technology projects.</td></tr>
</table>
</td></tr>
<tr><td></td><td>Control implementation guidelines:</td></tr>
</table>

	• 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.

<table>
<tr><td rowspan="5">1-6-2</td><td colspan="2">The cybersecurity requirements in project and assets (information/technology) change management must include at least the following:</td></tr>
<tr><td>1-6-2-1</td><td>Vulnerability assessment and remediation .</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.
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.</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 report that outlines the assessment and remediation of cybersecurity vulnerabilities throughout the technical project lifecycle and changes to information and technology assets.</td></tr>
<tr><td>1-6-2-2</td><td>Conducting a configurations ’ review, secure configuration and hardening and patching before changes or going live for technology projects.</td></tr>
<tr><td colspan="2">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.</td></tr>
</table>

<table>
<tr><td></td><td>

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.

</td></tr>
<tr><td>1-6-3</td><td>
The cybersecurity requirements related to software and application development projects must include at least the following:
<table>
<tr><td>1-6-3-1</td><td>Using secure coding standards.</td></tr>
</table>
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

</td></tr>
</table>

		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, approveand 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
	  ○ 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)
	  ○ 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
	  ○ Cybersecurity requirements prior to recruitment
	  ○ Cybersecurity requirements during work
	  ○ 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).

<table>
<tr><td></td><td colspan="2">

- Screening or vetting requests for the personnel of cybersecurity functions and technical functions with privileged access .

</td></tr>
<tr><td rowspan="5">1-9-3</td><td colspan="2">The personnel cybersecurity requirements prior to employment must include at least the following:</td></tr>
<tr><td>1-9-3-1</td><td>Inclusion of personnel cybersecurity responsibilities and non-disclosure clauses (covering the cybersecurity requirements during employment and after termination/ separation) in employment contracts.</td></tr>
<tr><td colspan="2">

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).

</td></tr>
<tr><td>1-9-3-2</td><td>Screening or vetting candidates of cybersecurity and critical/privileged positions.</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.
- Work with relevant departments to ensure Screening or Vetting of all employees in cybersecurity functions.

</td></tr>
</table>

<table>
<tr><td></td><td>

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.

</td></tr>
<tr><td></td><td>
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.

</td></tr>
<tr><td>1-9-4</td><td>
The personnel cybersecurity requirements during employment must include at least the following:
<table>
<tr><td>1-9-4-1</td><td>Cybersecurity awareness (during on-boarding and during employment).</td></tr>
</table>
</td></tr>
<tr><td></td><td>
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 .

</td></tr>
<tr><td></td><td>
Expected deliverables:

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

</td></tr>
</table>

	• 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:

<table>
<tr><td></td><td>

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.

</td></tr>
<tr><td></td><td>
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.

</td></tr>
<tr><td>1-10-3</td><td>The cybersecurity awareness program must cover the latest cyber threats and how to protect against them, and must include at least the following subjects:</td></tr>
<tr><td></td><td>
<table>
<tr><td>1-10-3-1</td><td>Secure handling of email services, especially phishing emails.</td></tr>
</table>
</td></tr>
<tr><td></td><td>
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.

</td></tr>
<tr><td></td><td>
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.

</td></tr>
<tr><td></td><td>
<table>
<tr><td>1-10-3-2</td><td>Secure handling of mobile devices and storage media.</td></tr>
</table>
</td></tr>
<tr><td></td><td>
Control implementation guidelines:

Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.

</td></tr>
</table>

	• 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 :

<table>
<tr><td></td><td colspan="2">

- 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.

</td></tr>
<tr><td rowspan="5">1-10-4</td><td colspan="2">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:</td></tr>
<tr><td>1-10-4-1</td><td>Cybersecurity function's personnel.</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.
- 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:
  - Implement the cybersecurity training plan for the organization in coordination with the Training and Employee Development Department.
  - Assist in the establishment of cybersecurity career paths to allow career progression, deliberate development, and growth within and between cybersecurity career fields.
  - Support in advocating for adequate funding for cybersecurity training resources, to include both internal and industry-provided courses, instructors, and related materials.

</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.
- Approved training plans and programs for the cybersecurity department employees at the organization.
- Cybersecurity training certificates.

</td></tr>
<tr><td>1-10-4-2</td><td>Personnel working on software/application development. and information and technology assets operations.</td></tr>
<tr><td colspan="2">Control implementation guidelines:</td></tr>
</table>

- 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.