الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Guide to Cybersecurity Controls for Critical Systems (CSCC) Implementation (GCSCC– 1: 2023)

Sharing Indicator: white
Document Classification: Public

Disclaimer: This guide was developed by the National Cybersecurity Authority to enable organizations to apply cybersecurity controls for critical systems (CSCC). The National Cybersecurity Authority also disclaims its responsibility to rely on this document only. And emphasizes the need to take into consideration the specific requirements of the entity and its environment; The National Cybersecurity Authority confirms that this document is only a guide that can be used as an example and does not necessarily mean that it is the only way to apply (CSCC) controls, provided that other methods do not conflict with the requirements of the National Cybersecurity Authority. This document contains some examples of outputs related to the application of (CSCC) controls, and the evaluator or auditor has the right to request other evidence as the evaluator or auditor deems appropriate to ensure that all (CSCC) controls are applied.

In the Name of Allah,
The Most Gracious,
The Most Merciful

Traffic Light Protocol (TLP):

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

Red – Personal, Confidential and for Intended Recipient Only

The recipient has no rights to share information classified in red with any person outside the defined range of recipients, either inside or outside the organization, beyond the scope specified for receipt.

Amber – Restricted Sharing

The recipient may share information classified in amber only with intended recipients inside the organization and with recipients who are required to take action related to the shared information.

Green – Sharing within The Same Community

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

White – No Restriction

Table of Contents

List of Figures

Introduction

The National Cybersecurity Authority (referred to in this document as "NCA") has developed a guide for applying the cybersecurity controls stipulated in the Cybersecurity Controls for Critical Systems (CSCC - 1: 2019) (referred to in this document as the "Controls"), in order to contribute in enabling national organizations to implement the requirements of compliance with Cybersecurity Controls for Critical Systems. Where this guide was built based on the information and experiences that NCA has collected and analyzed since the publication of the controls and the alignment of this guide with the leading best practices in cybersecurity to facilitate the application of the controls in the national authorities.

Objectives

The main objective of this guide is to contribute to enabling national entities to achieve the requirements of compliance with the application of cybersecurity controls for critical systems in the entity, with the aim of raising and enhancing their level of cybersecurity, and reducing cybersecurity risks that arise from internal and external cyber threats.

Scope of work and applicability

The scope of work for this guide as mentioned in Cybersecurity Controls for Critical Systems (CSCC-1:2019) is:

- Public entities that own or operate critical systems, whether they are governmental entities inside or outside the Kingdom of Saudi Arabia (e.g. ministries, agencies, institutions, embassies, etc.), entities and their subsidiaries, and private sector entities (all referred to in this document as the "Entity").
- NCA strongly encourages other entities within the kingdom to utilize these controls to implement best practices for enhancing and developing cybersecurity within their respective organizations.

Components and architecture of Cybersecurity Controls for Critical Systems

Figure No. (1) below shows the basic and sub-components of cybersecurity controls for critical systems (CSCC-1:2019)

Cybersecurity Risk Management	1-2	Cybersecurity Strategy	1-1	Cybersecurity Governance	1
Periodical Cybersecurity Review and Audit	1-4	Cybersecurity in Information Technology Projects	1-3		
Cybersecurity in Human Resources			1-5		
Identity and Access Management	2-2	Asset Management	2-1	Cybersecurity Defense	2
Networks Security Management	2-4	Information System and Processing Facilities Protection	2-3		
Data and Information Protection	2-6	Mobile Devices Security	2-5		
Backup and Recovery Management	2-8	Cryptography	2-7		
Penetration Testing	2-10	Vulnerabilities Management	2-9		
Web Application Security	2-12	Cybersecurity Event Logs and Monitoring Management	2-11		
Application Security			2-13		
Cybersecurity Resilience of Business Continuity Management (BCM)			3-1	Cybersecurity Resilience	3
Cloud Computing and Hosting Cybersecurity	4-2	Third-Party Cybersecurity	4-1	Third-Party and Cloud Computing Cybersecurity	4

Figure 1: Basic and sub-components of cybersecurity controls for critical systems

Structure of the Guideline

Figure 2 below shows the structure of the Guidelines for Cybersecurity Controls for Critical Systems (CSCC-1:2019)

<table>
<tr><td colspan="2"> 
Reference number of the Main Domain</td><td>Name of Main Domain</td></tr>
<tr><td colspan="2">Reference No. of the Subdomain</td><td>Name of Subdomain</td></tr>
<tr><td colspan="3">Objective</td></tr>
<tr><td colspan="3">Controls</td></tr>
<tr><td rowspan="3">Control Reference Number</td><td colspan="2">Control Clauses</td></tr>
<tr><td colspan="2">Guidelines:</td></tr>
<tr><td colspan="2">Expected Outputs:</td></tr>
</table>

Figure 2: Structure of the Guidelines for Cybersecurity Controls for Critical Systems (CSCC-1:2019)

General Guidelines for implementing cybersecurity controls for critical systems

General guidelines
• identify all critical systems at the national level using the inventory of critical systems tool published on the website of the National Authority for Cybersecurity and regularly review the sensitivity assessment of these systems. • Develop an inventory of all critical systems and their technical components and review and update them at least annually, or when necessary changes occur. • Inventorying user accounts with critical privileges, who have the ability to manage or access critical systems within the organization, and reviewing them periodically. • Identify and document the cybersecurity critical systems requirements, along with associated roles and responsibilities, and having them approved by the authority holder and reviewed periodically. • Review the ECC guidelines and implement controls related to cybersecurity controls for critical systems. • Develop a plan to implement cybersecurity controls for critical systems, and monitor it continuously.

Guidelines for implementing cybersecurity controls for critical systems

Cybersecurity Governance

1-1	Cybersecurity Strategy
Objective	Ensure containment of work, objectives, projects and local projects
Controls	
1-1-1	In addition to the controls within sub-component 1-1 of the ECC, the cybersecurity strategy of the entity must set a priority to support the protection of critical systems of the entity.
	Related cybersecurity tools: • Template for Cybersecurity Strategy **Guidelines:** • Work to include the protection of the entity's critical systems within the strategic objectives of cybersecurity and align it with the strategic objectives of the entity. • Conduct workshops with the stakeholders and those concerned in the entity to explain the importance of giving priority to supporting the protection of the critical systems of the entity. • Giving priority in implementing projects related to critical systems of the entity over other projects. • Giving priority to securing and protecting critical systems in cybersecurity projects and initiatives and documenting this in the implementation map of the cybersecurity strategy.
	Expected Outputs: • Cybersecurity strategy document approved by the authorized person in the entity (electronic copy or official hard copy). • Presentation of the workshop that was held with the stakeholders and those concerned in the entity to give priority to supporting the protection of the critical systems of the entity. • A roadmap document for the implementation of the cybersecurity strategy, indicating the level of achievement in the implementation of projects and initiatives related to the critical systems of the entity.

<table>
<tr><td></td><td colspan="2">• Inventory review and periodic update of the list of critical systems.</td></tr>
<tr><td>1-2</td><td colspan="2">Cybersecurity Risk Management</td></tr>
<tr><td>Objective</td><td colspan="2">Ensure that cyber security risks are managed in a systematic manner aimed at protecting the information and technical assets of the entity, in accordance with the organizational policies and procedures of the entity and the relevant legislative and regulatory requirements.</td></tr>
<tr><td colspan="3">Controls</td></tr>
<tr><td>1-2-1</td><td colspan="2">In addition to the controls under subcomponent 1-5 of the basic controls for cybersecurity, the methodology for managing cybersecurity risks should include, at a minimum, the following:</td></tr>
<tr><td></td><td>1-2-1-1</td><td>Implementing a Cybersecurity risk assessment on critical systems at least once a year.</td></tr>
<tr><td></td><td colspan="2">Related cybersecurity tools:
• Cybersecurity Risk Management Policy Template
• Cybersecurity Risk Management Procedure Template
Guidelines:
• conduct a cybersecurity risk assessment on critical systems (which were listed within the outputs of control No. 2-1-1-1) in order to identify all potential threats that could affect the integrity of those systems or expose the information they process to any cyber or computer risks or potential vulnerabilities, taking into account the nature of those systems.
• Asses cybersecurity risks for each critical system periodically, so that it is done at least once a year.
• Work on creating reports on cybersecurity risk assessments for each critical system, provided that the following are documented in them:
○ Cyber risks and potential vulnerabilities
○ Probability of risk occurrence
○ Impact ratio
○ Risk level
○ Responsible for the potential risk
○ Description of the risk mitigation plan
○ Impacted assets</td></tr>
</table>

- develop a plan to address the list of cybersecurity risks for each critical system, and give priority in implementation to the plan to address risks related to critical systems over other risks.

Expected Outputs:

- Periodic cybersecurity risk assessment reports on the range of critical systems in the organization.
- Cybersecurity risk treatment plans for each critical system.
- Reports or evidence showing the follow-up of treatment plans and verifying their implementation.

1-2-1-2	Create a cybersecurity risk register for critical systems and follow it up at least once a month.

Related cybersecurity tools:

- Cybersecurity Risk Register Template
- Cybersecurity Risk Management Policy Template

Guidelines:

- Create a cybersecurity risk register for critical systems or include the risks related to critical systems clearly within the entity's general cybersecurity risk register, so that it contains the following:
  - Cyber risks and potential vulnerabilities
  - Probability of risk occurrence
  - Impact ratio
  - Risk level
  - Responsible for the potential risk
  - Description of the risk mitigation plan
  - Impacted assets
- Work to include the cybersecurity risks of critical systems that were identified and evaluated during the risk assessment process in the cybersecurity risk register for critical systems, and assign them to stakeholders.
- Follow-up the cybersecurity risk register of critical systems periodically, at least once a month, so that treatment plans are followed up, their implementation verified, any new risks added, and changes in the register documented.

	Expected Outputs: • Cybersecurity risk register for critical systems. • Record of changes to the cybersecurity risk register for critical systems. • Reports or evidence showing the follow-up of treatment plans and verifying their implementation.	
1-3	**Cybersecurity in Information Technology Project**	
Objective	Ensure that cybersecurity requirements are included in the entity's project management methodology and procedures; To protect the confidentiality and integrity of the entity's information and technical assets, their accuracy and availability; This is in accordance with the regulatory policies and procedures of the entity and the relevant legislative and regulatory requirements.	
Controls		
1-3-1	In addition to the sub-controls within Control 1-6-2 in the ECC, it must cover the cybersecurity requirements for project management and changes to the information and technical assets of critical systems in the entity, with a minimum of the following:	
	1-3-1-1	Carrying out stress testing of the technical components of critical systems (Stress Testing) to ensure the capacity of the various components.
		Related cybersecurity tools: • Cybersecurity Requirements Checklist for IT Projects and Change Management Template **Guidelines:** • Determine stress testing methods for the technical components of critical systems, using one of the following methods: ○ Distributed Stress Testing: It is about distributing stress on several devices that may be in different geographical areas, and testing them at the same time to examine their endurance capacity. ○ Exploratory Stress Testing: It is a test that focuses on detecting and analyzing errors in technical components after testing and analyzing them in different scenarios, which cannot be easily covered in the scope of other tests.

		○ Application Stress Testing: It is a test that focuses on detecting application-related errors, related to performance, network issues, and data blocking. ○ Systemic Stress Testing: It tests many systems running on the server, to detect errors (e.g.: One program blocking another program). ○ Transactional Stress Testing: It is a stress test that is conducted during the transitioning between applications, to ensure that the system is tuned and optimized. • Document the results of stress tests for technical components of critical systems. • Dealing with data based on its classification, so that special data and systems are specified for stress testing, and system data in the production environment is not used in the stress testing process. • Define a plan for improvement based on test results and update implementation status.
		Expected Outputs: • Evaluation and stress test reports for technical components of critical systems. • Document showing sample data used for stress testing of technical components of critical systems and not from production environments data. • Improvement plan and implementation status for stress testing of technical components of critical systems.
	1-3-1-2	Ensure the application of business continuity requirements.
		Related cybersecurity tools: • Cybersecurity Roles and Responsibilities Template • Cybersecurity Requirements Checklist for IT Projects and Change Management Template • Cybersecurity Business Continuity Policy Template **Guidelines:** • Work on conducting a risk assessment for risks that may affect business continuity. • Work on vulnerability remediation to prevent incidents that may impact business continuity.

		• Work on identifying the legislative and regulatory requirements that may impact business continuity. • Work on developing incident response plans that may impact business continuity. • Develop disaster recovery plans for business continuity. • Work to define the roles and responsibilities of third parties related to business continuity in the entity. • Reports of change requests on infrastructure assets to implement business continuity requirements. • Work to use the performance measurement indicator (KPI) to ensure the continuous development and correct and effective use of cybersecurity requirements for business continuity.
		Expected Outputs: • Reports on the results of the risk assessment process affecting business continuity. • Reports on the results of the vulnerability assessment and remediation process affecting business continuity. • Reports or evidence demonstrating the comprehensiveness and coverage of legislative and regulatory requirements related to business continuity. • Cybersecurity Incident Response Plans impacting business continuity. • Disaster recovery plans. • A document of the roles and responsibilities of the parties related to business continuity within the organization. • Reports on change requests within the organization. • Reports on the Key Performance Indicators (KPI) related to business continuity.
1-3-2	In addition to sub controls in the ECC controls 3-6-1	
	1-3-2-1	Security Source Code Review prior to release
		Related cybersecurity tools: • Cybersecurity Requirements Checklist for Software Development Template • Secure Systems Development Life Cycle Policy Template

		Guidelines: • Work on defining the scope of the source code to be reviewed before launching the project. • Work on reviewing the source code either by using technical tools, or reviewing manually, and that the methods of reviewing the source code be effective such as: reviewing gaps in the source code, ensuring that there is no confidential information in the source code, ensuring that there are no security problems in the design Source Code Ensure that unsafe algorithms are not used, and review the source code using OWASP. • Work on documenting the review results and defining a plan to address the source code comments. • Work to fully implement and follow up the treatment plan before launching the project.
		Expected Outputs: • Source code security review procedures, which include: determining the scope of the source code, and the methods taken to conduct the source code security review. • Reports of the results of the security source code review. • Source code improvement plan reports. • Reports showing the implementation and follow-up of the source code improvement plan.
	1-3-2-2	Securing access, storage, and documentation of source code and its versions.
		Related cybersecurity tools: • Cybersecurity Requirements Checklist for Software Development Template • Secure Systems Development Life Cycle Policy Template **Guidelines:** • Work to determine the scope of the source code. • Work to restrict access to the source code to developers and source code reviewers, by specifying access permissions according to the needs, duration, and scope of the work. • Work to define procedures for obtaining access permissions from responsible persons. • Work on reviewing the access permissions to the source code, and revoking the permissions if the work need or duration expires.

		• Work to ensure that the source code is stored and documented in safe and reliable ways.
		Expected Outputs: • Procedures for securing access, storage, and documentation of the source code, which include: determining the scope of the source code, and backup copies of the source code. • Procedures for requesting access to the source code from responsible persons. • A sample of requests for access permissions to the source code. • Reports from reviewing source code access permissions. • A list of restrictions applied to the level of access and storage security of the source code. • A list of previous versions of the source code and the restrictions applied to secure it.
	1-3-2-3	Authenticated API.
		Related cybersecurity tools: • Cybersecurity Requirements Checklist for Software Development Template • Secure Systems Development Life Cycle Policy Template **Guidelines:** • Work on securing the application interface when there is integration with other applications. • Restricting access to the API, such as giving access permissions according to the scope of work. • Verify API access permissions. • Using secure protocols (such as TLS) in the API. • Performing regular penetration tests on the API.
		Expected Outputs: • Screenshot of locking the application interface when there is integration with other applications. • Reports of restricted API access. • Reports of API access verification. • Screenshot of Using secure protocols in the API.

		• Reports from penetration tests on the API.
	1-3-2-4	Safe and reliable transfer of applications from the Testing Environment to the Production Environment, with any data, identities, or passwords associated with the test environments deleted prior to transfer.
		Related cybersecurity tools: • Cybersecurity Requirements Checklist for Software Development Template • Secure Systems Development Life Cycle Policy Template **Guidelines:** • Work to delete any data, identities, or passwords related to the testing environment before transferring to the production environment. • Work to encrypt all critical systems data during transmission. • Work to use safe, updated and approved transfer tools. • Work on providing an action plan to clarify the scope and time of the transfer. • Work on reviewing the implementation of the action plan for safe transportation and ensuring its effectiveness. • Work to develop and approve transportation procedures.
		Expected Outputs: • Reports showing the deletion of any data, identities, or passwords related to the testing environment before the transfer to the production environment. • Reports showing that all critical systems data is encrypted during transmission. • Reports of the tools used for the transfer process. • Action plan for the transportation process. • Review reports on the application of the action plan for the transfer process. • Approved procedures for the transportation process.
1-4	**Cybersecurity Assessment Periodical and Audit**	
Objective	Ensure that the entity's cybersecurity controls are applied and operate in accordance with the entity's regulatory policies and procedures, relevant national legislative and regulatory requirements, and international requirements that are regulatory approved by the entity.	

Controls	
1-4-1	Referring to officer 1-8-1 in the basic controls of cybersecurity, the department concerned with cybersecurity must; Review the implementation of cyber security controls for critical systems, once a year; at least.
	Related cybersecurity tools: • Cybersecurity Review and Audit Policy Template • Compliance with Cybersecurity Legislation and Regulations Policy Template • Audit Plan Risk Register Template **Guidelines:** • Ensure that the plan to review the implementation of cybersecurity requirements includes all critical systems in the entity. • Work on documenting the results of the cyber security review and audit and discussing them with the concerned departments. • Presenting the results to the Cyber Security Supervisory Committee and the authorized person, and the results should include the scope of the review and audit, the observations discovered, recommendations and corrective actions, the evaluation of cyber risks and the plan to identify the observations. • Review the implementation of cyber security controls for critical systems on an annual basis.
	Expected Outputs: • Plan to review the implementation of cybersecurity requirements or controls. • Periodic review reports on the implementation of cybersecurity controls for critical systems in the entity, including a plan for addressing observations. • Meeting notes transcript of the Cybersecurity Supervisory Committee.
1-4-2	Referring to officer 2-8-1 in the basic controls of cybersecurity, the application of cybersecurity controls for critical systems must be reviewed; By parties independent of the department concerned with cybersecurity from within the entity, once; At least every three years.
	Related cybersecurity tools: • Cybersecurity Review and Audit Policy Template

	• Compliance with Cybersecurity Legislation and Regulations Policy Template • Audit Plan Risk Register Template **Guidelines:** • Ensure that the cyber security audit plan by independent parties includes all critical systems in the entity. • Auditing of cybersecurity controls for critical systems is carried out at least every three years.
	Expected Outputs: • Audit reports of cybersecurity controls for critical systems; By parties independent of the department concerned with cybersecurity from within the entity, once; At least every three years. • Plan to review the implementation of cybersecurity controls requirements. • Meeting notes transcript of the Cybersecurity Supervisory Committee • Work on documenting reports and discussing the plan to address observations with the relevant departments.
1-5	**Cybersecurity in Human Resources**
Objective	Ensure that cybersecurity risks and requirements related to workers (employees and contractors) in the entity are effectively identified before, during and at the end/termination of their work, in accordance with the entity's organizational policies and procedures, and the relevant legislative and regulatory requirements.
Controls	
1-5-1	In addition to the sub-controls within Control 3-9-1 in the basic controls of cybersecurity, it must cover the requirements of cybersecurity, before the start of the professional relationship of employees with the entity, at a minimum level; the following:
	1-5-1-1 Screening or Vetting for personnel working on critical systems.
	Related cybersecurity tools:

- Human Resources Cybersecurity Policy Template

Guidelines:

- Determine the job positions related to the critical systems for which the security scan is to be conducted, which includes, e.g.:
  - Database Administrator for critical systems.
  - Network Administrator for critical systems.
  - Domain Administrator for critical systems.
  - System Administrators from the technical and business side for critical systems.
  - All contract employees.
- Developing, documenting, and approving a procedure for conducting security scans on workers on critical systems on a regular basis.
- Conducting security scanning for candidates to work on critical systems as part of the recruitment process, which includes, e.g.:
  - Review the recommendations of previous employers, submitted by the candidate, and ensure their accuracy (for those with experience).
  - Verify the validity of the applicant's CV.
  - Ensure the academic and professional qualifications claimed.
  - Independent verification of identity (personal ID, passport, etc.).
  - Review criminal records from the concerned authorities.
- Verify that a security scan has been performed on existing workers on critical systems. Which may include :
  - Ensure that the candidate is competent enough to perform his role in protecting information.
  - Ensure that the candidate is trusted to assume the job duties.

Expected Outputs:

- Security scanning for personnel working on critical systems, which include e.g.:
  - A list of all personnel working on critical systems from the operational and technical side, indicating their nationalities, roles and responsibilities.
  - Database Administrator security scanning for critical systems.
  - Security scanning of Network Administrators for critical systems.

	○ Security scanning of Domain Administrator for critical systems. ○ Security survey for System Administrators from the technical side (Custodian) and from the business owner side of critical systems.
1-5-1-2	To occupy support functions, and technical development, for critical systems; Competent citizens.
	Related cybersecurity tools: • Human Resources Cybersecurity Policy Template **Guidelines:** • identify critical jobs for those working on critical systems, which include, but are not limited to: ○ Administrative careers. ○ Support careers. ○ Technical development. • Ensure that competency requirements for each job description for those working on critical systems are identified and documented. • Ensure the selection and nomination of highly qualified citizens to fill administrative positions, support positions, and technical development positions related to critical systems.
	Expected Outputs: • The job description of the current employees working on critical systems at the entity, which includes, e.g.: ○ Job title ○ The purpose of the job ○ Duties and responsibilities ○ Required qualifications ○ Preferred qualifications ○ working conditions • Resumes of employees working on critical systems, including administrative positions and technical support and development positions.

2 Cybersecurity Defense

2-1	Asset Management	
Objective	To ensure that the entity has an accurate and up-to-date inventory of assets that includes relevant details of all informational and technical assets available to the entity, in order to support the entity's operational processes and cybersecurity requirements, to achieve the confidentiality, integrity, accuracy, and availability of the informational and technical assets of the entity.	
Controls		
2-1-1	In addition to the controls under subcomponent 2-1 of the basic controls for cybersecurity, the cybersecurity requirements for the management of information and technology assets should include, at a minimum; the following:	
	2-1-1-1	Maintain an annual updated list of all assets of critical systems.
	Related cybersecurity tools: • Asset management policy template • Asset classification standards template • Asset management standard template **Guidelines:** • Work on developing the asset inventory of critical systems in electronic format. Several methods can be applied to store and use an inventory and inventory of assets, including but not limited to: ○ Configuration management database (CMDB). ○ Asset management software. ○ Specialized asset management tool. ○ Spreadsheets. ○ Database. • Ensure that the inventory of informational and technical assets for critical systems includes, for example, the following: ○ The type of assets and the description of the assets.	

- Asset classification level and reclassification date.
- compliance requirements (such as recording whether the assets fall within the scope of privacy, data retention, or other legal obligation).
- Asset site.
- The owner of the assets (e.g. Asset Protection Custodian).

- Ensure that the inventory list is centralized between the department concerned with cybersecurity, information technology, and other concerned departments, and that it is updated and verified at least once a year.

Expected Outputs:

- An inventory of all assets for critical systems and their technical components.
- Annual audit reports of asset inventories for critical systems.

2-1-1-2	Identifying asset owners and involving them in the asset management life cycle of critical systems.

Related cybersecurity tools:

- Asset management policy template

Guidelines:

- Work to identify all asset owners of critical systems and develop a list of all their roles and responsibilities in terms of asset management.
- Work on an awareness program for all asset owners on how to carry out their responsibilities.
- Work on implementing a mechanism to involve all owners in the asset life cycle, for example:
  - Ensure that the assets are included in the inventory list and updated continuously at least annually.
  - Classification of assets.
  - Description of assets.
  - Safe destruction of assets.
  - Changes that occur to assets.

Expected Outputs:

- A document that includes all the owners of the assets of the critical systems and all their duties and responsibilities.

	• A Document procedures for involving owners in the asset life cycle.
2-2	**Identity and Access Management**
Objective	Ensure the protection of cyber security for logical access to the information and technical assets of the entity in order to prevent unauthorized access and restrict access to what is required to complete the work related to the entity.
Controls	
2-2-1	In addition to the sub-controls under item 2-2-3 in the basic controls for cybersecurity, they must cover the cybersecurity requirements related to managing access identities and the permissions for critical systems in the entity, at a minimum:
	2-2-1-1 Prohibiting remote access from outside the Kingdom of Saudi Arabia.
	Related cybersecurity tools: • Identity and Access Management Policy Template **Guidelines:** • The design and settings of the network must not allow remote access from outside the Kingdom to critical systems that are not connected to the Internet, as well as technical support from outside the Kingdom for critical systems, whether connected to the Internet or not. This does not mean that users of critical systems connected to the Internet are not allowed to access them. Such as: (adjusting VPN settings to prevent entry from outside Saudi Arabia).
	Expected Outputs: • A list of technical controls settings to prevent remote access to critical systems from outside the Kingdom.
	2-2-1-2 Restricting remote entry from inside the Kingdom; Provided that it is verified by the security operations center of the entity, at every entry process; and continuously monitor remote access-related activities.
	Related cybersecurity tools: • Identity and Access Management Policy Template

	Guidelines: • Work on developing procedures to restrict remote entry from inside the Kingdom, for example: ○ Entry from inside the Kingdom is automatically denied to all users, and when needed, the reason for the need is presented, and then the necessary approvals are taken from the concerned department and the cybersecurity department according to the procedures approved by the entity. ○ Granting access for a limited period only as needed. ○ Grant access to the system specified in the request only. ○ Granting access from inside the Kingdom through specialized systems approved by the entity, for example: the (VPN) or (MDM) systems. ○ Work to save all activities and records of remote login operations and ensure that they are sent to the operations and monitoring center to ensure that they are constantly monitored by specialized teams by linking login logs with monitoring systems, for example: the (SEIM) system.	
	Expected Outputs: • Procedures document for restricting remote entry from within the Kingdom to critical systems. • A document to set the configuration of remote access systems, for example, the (VPN) system. • A guide explaining the monitoring of remote access events through the entity's security operations center.	
	2-2-1-3	Multifactor authentication (MFA) for all users.
	Related cybersecurity tools: • Identity and Access Management Policy Template **Guidelines:** • Work on developing procedures for logins that contain multi-factor authentication. • Work to activate multi-element verification next to the username and password, which may be, for example:	

		○ One Time Password in a text message sent to the registered user's mobile number. ○ One Time Password is displayed in a random number generator (HardToken) program or device for multi-factor identity verification. ○ Identity verification using biometric features (e.g. fingerprint).
	Expected Outputs: • A guide explaining the implementation of multi-element identity verification requirements for all users on critical systems, including but not limited to: A screenshot showing adjusting the settings of critical systems to ensure confirmation of the multi-element identity verification request.	
	2-2-1-4	Multi-Factor Authentication (MFA) for critical users; And the systems used to manage and monitor the critical systems mentioned in Control 4-1-3-2.
	Related cybersecurity tools: • Identity and Access Management Policy Template • Standards template for user devices with important and critical privileges **Guidelines:** • Determine the important and critical privileges of critical systems (System Administrative), which includes at the level of infrastructure and networks such as: (Network Administrative) and applications such as: (Application Administrative) and databases such as: (Database Administrative) in the entity. • Identify Personnel with Privileged Access . • Work on developing procedures for managing Privileged Access authorities approved in the entity, taking into consideration the following: ○ Multi-factor authentication for all users of critical systems with important and critical privileges. ○ Privileged accounts must not be used for day-to-day operations. ○ Privileged accounts must not be used for internet access ○ Privileged accounts must not be used for email access.	

	○ Preventing the use of Privileged accounts for remote logins, and granting the authority to use after obtaining approval with a practical justification. ○ Default accounts must be disabled. ○ 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 ● Work to identify modern and advanced technologies and mechanisms for managing important and critical privileges. ● Ensure that important and critical privileges are granted based on job tasks after obtaining the necessary approvals, taking into account the principle of separation of duties. ● Work on recording logins on accounts with important and critical privileges for follow-up and monitoring.	
	Expected Outputs: ● An inventory of the accounts of employees who have important and critical privileges. ● A guide explaining the implementation of multi-factor authentication requirements for logins, including but not limited to: A screenshot showing critical system settings to ensure certainty of the multi-factor identity verification request for users with important, critical permissions. ● Requests to grant important and critical privileges and approvals. ● Audit reports on important and critical account activities.	
	2-2-1-5	Prepare password standard controls taking into consideration best practices and implementation.
	Related cybersecurity tools: ● Identity and Access Management Policy Template ● Standards template for managing login identities and permissions, which includes password management.	

Guidelines:

- 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 e.g.:
  - The expiration period of the password is at least 30 days for important and critical and critical privileges, and at least 90 days for the remaining privileges.
  - The password validity period (Expiration Period) is at least 30 days for important and critical and critical, and the rest of the permissions are at least 90 days
  - password complexity
  - password lockout
  - password activation
  - password history
  - The number of attempts allowed is 3
  - The passwords used during the last 12 times should not be repeated
  - Passwords should not be used based on the personal data of the user with permissions and privileges, such as date of birth.
  - The password must be complex and contain at least 4 characters from the following:
    - Upper case letters
    - Lower case letters
    - Numbers(١٢٣٤)
    - Special characters(@*%#)

Expected Outputs:

- Configure configuration include secure password standards for critical systems.

2-2-1-6	Using safe methods and algorithms to store and process passwords, e.g. using hashing functions.

Related cybersecurity tools:

- Identity and Access Management Policy Template

- Standards template for managing login identities and permissions, which includes password management.

Guidelines:

- Working on providing security systems and solutions for saving and processing passwords and ensuring that encryption requirements are met based on national encryption standards, for example :
  - Working on the use of accepted shorthand functions based on national encryption standards, for example: SHA-256.
  - Ensure that the hashing functions are Resistant Inversion, Collision Resistant, and Pre-Resistant image.

Expected Outputs:

- Document the procedures for storing and handling passwords for critical systems.

2-2-1-7	Secure management of Service Accounts between applications and systems; And disable interactive human login through it .

Related cybersecurity tools:

- Identity and Access Management Policy Template

Guidelines:

- Work on developing clear procedures for dealing with service accounts and ensuring that they are managed securely between applications and systems, and disabling interactive human login through them, for example :
  - disable all service accounts and activate only the necessary ones.
  - identify the service accounts needed by the business and to be used by the entity with the concerned departments.
  - Assigning an owner to each service account to ensure that it is managed securely.

Expected Outputs:

- Document the procedures for secure management of service accounts.
- A list of service accounts and their owners, showing their status (activated or disabled).
- Restrictions applicable to access to these accounts.
- Requests to obtain access to service accounts.

	2-2-1-8	With the exception of Database Administrators, access or direct interaction of any user with databases is prohibited. This is done through applications only, and based on the powers conferred on them; Taking into account the implementation of security solutions that limit or prevent database administrators from accessing Classified Data.
	Related cybersecurity tools: • Database Security Policy Template • Database Security Standard Template • Identity and Access Management Policy Template **Guidelines:** • Work on developing procedures for dealing with databases, for example: ○ Do not grant direct access or interaction privileges except to database administrators. ○ Work to identify the users and supervisors who are required to access or interact with the databases and grant them permissions due to the need to work with the concerned department. ○ Work to develop procedures to ensure that the authorized person has access to databases through protected and updated devices that contain all the required security solutions. ○ Work to grant privileges based on need only and give privileges to implement specific work requirements only. ○ Work to determine access or interaction permissions to be through applications only, with the exception of database administrators. ○ Working to provide security technologies and solutions to prevent access to classified data, such as blocking data completely or partially (Data Masking).	
	Expected Outputs: • Procedure document for safe handling of databases for critical systems. • List of databases containing classified data and the classification of data stored on them. • Mechanism for approving access requests to databases. • Requests to obtain access to databases through database administrators.	

	• Restrictions applied to access classified data.
2-2-2	Going back to Control 2-2-3-5 in Basic Controls for Cyber Security, access identities on critical systems should be reviewed, at least once, every three months.
	Related cybersecurity tools: • Identity and Access Management Policy Template **Guidelines:** • Work to review the entry identities and privileges of the critical systems in the entity by conducting a periodic evaluation (according to a documented and approved plan for the review, and based on a specified period of time at least every three months). • Work to review all entry identities and permissions in all respects, for example: ○ The principle of minimum permissions and privileges ○ The principle of separation of duties and the principle of the need for knowledge and use in cooperation with the relevant departments (such as the department concerned with information technology). ○ Granted validity period. ○ The status of the person authorized with the granted permissions, for example: if they are still in the administration or have been transferred to another team, or has resigned from the organization. • Document all reviews and changes made to the entry identities and privileges of critical systems in the entity, for example : ○ Periodic reviews of the privileges and permissions granted. ○ Changes made from the last revision. ○ Changes or modifications required to be changed to the privileges and permissions granted.
	Expected Outputs: • The results of reviewing the entry identities and privileges of the critical systems in the entity. • A document specifying the cycle of reviewing the access identities and privileges of the critical systems in the entity (evaluation table).

<table>
<tr><td>2-3</td><td colspan="2">Information System and Processing Facilities Protection</td></tr>
<tr><td>Objective</td><td colspan="2">To ensure the protection of information systems and information processing facilities (including workstations and infrastructures) against cyber risks.</td></tr>
<tr><td colspan="3">Controls</td></tr>
<tr><td>2-3-1</td><td colspan="2">In addition to the sub-controls under Control 2-3-3 in the Basic Controls of Cybersecurity, they must cover the cybersecurity requirements to protect critical systems, and their information processing devices, at a minimum; the following:</td></tr>
<tr><td></td><td>2-3-1-1</td><td>allow only a specific whitelisting of applications and programs; To work on critical systems.</td></tr>
<tr><td></td><td colspan="2">Related cybersecurity tools:
Server Security Policy Template
Server Security Standard Template
Malware Protection Policy Template
Malware Protection Standard Template
Virtualization Security Standard Template
Advanced Persistent Threats (APT) Standard Template
Guidelines:
Work to determine and approve a list of operating files for applications and programs that are allowed to run on servers for critical systems, by conducting a risk assessment that results in a list of allowed files.
Work on specifying this list as files allowed through the server's security system or directly through the server settings.
Work to link this list to the rules specified in the security information and events management system that monitors server logs, so that any use of operating files outside of this list is followed up.</td></tr>
<tr><td></td><td colspan="2">Expected Outputs :
A list of allowed and approved operating files that have been matched in the system or server for critical systems.</td></tr>
<tr><td></td><td>2-3-1-2</td><td>Protecting servers of critical systems with end-point protection technologies approved by the organization.</td></tr>
</table>

	Related cybersecurity tools: • Server Security Policy Template • Server Security Standard Template • Malware Protection Policy Template • Malware Protection Standard Template • Virtualization Security Standard Template • Advanced Persistent Threats (APT) Standard Template **Guidelines:** • Work to identify protection technologies for critical devices and ensure that it contains appropriate technologies to protect against advanced and continuous attacks. • Work to download these technologies on all servers of critical systems in the entity. • Work on continuously monitoring the protection systems of critical systems and ensuring that alerts for new version updates are activated. • Work on linking the protection system for critical systems with the security information and events management system.	
	Expected Outputs : • List of protection systems for critical systems. • Special protection systems installed on critical systems.	
	2-3-1-3	Applying security fixes and updates patches, at least once a month, to critical external systems connected to the Internet; and at least every three months, for internal critical systems; With following the change mechanisms approved by the entity.
	Related cybersecurity tools: • Server Security Policy Template • Server Security Standard Template • Virtualization Security Standard Template • Patch Management Policy Template • Patch Management Standard Template **Guidelines:** • Determine the procedures for applying security fixes and updates patch at the entity and have them approved by the authority, including : ○ At least once a month, apply patches and updates to critical external systems, including but not limited to: external web applications.	

		○ Apply patches and updates to internal critical systems at least every three months, including but not limited to: Data systems of critical applications. ○ Ensure that the entity's change management approval is part of the approvals required to implement security fixes and update patches for critical systems. • Monitor the application of update patches and security fixes on critical systems on an ongoing basis through the use of tools and techniques for managing update patches and vulnerability management.
		Expected Outputs: • Procedures for applying security patches and patch updates to critical systems. • Patch update and patch application reports as per the planned period for critical systems .
	2-3-1-4	Allocating workstations for technical staff with privileged accounts; Provided that it is isolated in a private management network and that it is not linked to any other network or service (e.g.: e-mail service, the Internet).
		Related cybersecurity tools: • Server Security Policy Template • Server Security Standard Template • Configuration and Hardening Policy Template • Secure Configuration and Hardening Standard Template • Virtualization Security Standard Template **Guidelines:** • identify computers other than the user's computer for those working in technical jobs who have important and critical privileges to manage their critical systems. • isolate these devices in their own network and not be connected to any of the other party's networks. • isolate these devices from the Internet and other services and applications used by users, including, but not limited to: e-mail service, special applications for managing employee information, and applications that are accessed via the Internet. • create accounts for these devices and monitor them continuously among the entity's important and critical accounts.
		Expected Outputs : • Isolated computers designated for accessing critical systems.

	• A list of accounts with access to these devices and the restrictions applied to ensure that they cannot be used on other devices.
2-3-1-5	Encrypt any Non-console administrative access to any of the technical components of critical systems, using secure encryption algorithms and protocols.
	Related cybersecurity tools: • Server Security Policy Template • Server Security Standard Template • Virtualization Security Standard Template • Cryptography Policy Template • Cryptography Standard Template **Guidelines:** • Work to define encryption standards for supervisory access over the network to critical systems and ensure their alignment with national standards for encryption, so that: ○ Secure communication technologies and protocols are identified, including but not limited to: SSH and TLS. ○ The minimum length of the key is specified. • Allocate supervisory access over the network to critical systems and use multi-factor authentication for access.
	Expected Outputs: • An encryption standard for supervisory access over a network.
2-3-1-6	Reviewing the configuration of critical systems and their immunizations (Secure Configuration and Hardening) every six months at least.
	Related cybersecurity tools: • Server Security Policy Template • Server Security Standard Template • Configuration and Hardening Policy Template • Secure Configuration and Hardening Standard Template • Virtualization Security Standard Template **Guidelines:** • Working on defining safe technical standards for setting up, configuring, hardening systems and ensuring that they are obtained from reliable sources, for example: ○ Companies developing these systems. ○ Reference sources for preparation and immunization.

- Work to include safe technical standards for configuration and hardening critical systems, for example:
  - Manage privilege and access sessions.
  - encryption .
  - Records management .
  - Safe system configuration.
- Periodic review of the configuration and hardening of critical systems, according to the specified plan, so that it takes place at least every six months.
- document the results of reviewing the configuration and hardening of critical systems.

Expected Outputs:

- Secure standards for implementing settings up, configuring and hardening critical systems.
- Periodic configuring and hardening application reports according to the planned duration for critical systems.

2-3-1-7	Review and modify the factory configuration (Default Configuration) and ensure that there are no Hard-Coded, backdoor and default passwords as applicable.

Related cybersecurity tools:

- Server Security Policy Template
- Server Security Standard Template
- Configuration and Hardening Policy Template
- Secure Configuration and Hardening Standard Template
- Virtualization Security Standard Template

Guidelines:

- review the Default Configuration of all critical systems of the entity so that they are modified as possible and the results of the review are documented.
- ensure that there are no static, background, and default passwords on critical systems, so that :
  - The source code of the entity's applications is reviewed and any fixed passwords are removed.
  - Review access rights to critical systems and disable any accounts that are not being used or whose creation has expired.
  - Disable or modify the default accounts for critical systems, including, but not limited to: disabling the default account for databases.

	• Work on documenting the results of reviewing and processing passwords for critical systems based on the above.	
	Expected Outputs: • A report on reviewing the factory settings of all critical systems. • Password review reports for critical systems.	
	2-3-1-8	Protect systems' critical records and files from unauthorized access, tampering, alteration, or deletion.
	Related cybersecurity tools: • Server Security Policy Template • Server Security Standard Template • Virtualization Security Standard Template • Endpoint Detection and Response Standard Template • Cybersecurity Event Logs and Monitoring Management Policy Template • Cybersecurity Event Logs and Monitoring Management Standard Template **Guidelines:** • Work to protect system's' critical records and files from unauthorized access, through encryption or setting a password. • Work to allocate access rights to critical system records and files to include a specific group of workers. • Work to protect critical records and files from unauthorized tampering, alteration or deletion by restricting the permissions to write, modify and delete all records and files, including but not limited to: event logs, database files, and application system files. • Work to take backup copies of all critical records and files of critical systems on an ongoing basis.	
	Expected Outputs : • Access to critical records and files of critical systems. • Backup reports of critical logs and files of critical systems.	
2-4	**Networks Security Management**	
Objective	Ensure the protection of the entity's networks from cyber risks.	

<table>
<tr><th colspan="3">Controls</th></tr>
<tr><td rowspan="5">2-4-1</td><td colspan="2">In addition to the sub-controls within Control 3-5-2 in the Basic Controls of Cybersecurity, the cybersecurity requirements for managing the security of networks of critical systems of the entity must cover, at a minimum, the following:</td></tr>
<tr><td>2-4-1-1</td><td>Isolation and physical, or logical, partitioning of networks of critical systems.</td></tr>
<tr><td colspan="2">Related cybersecurity tools:
Network Security Policy Template
Network Security Standard Template
Wireless Network Security Standard Template
Network Detection and Response Standard Template
Guidelines:
Work on the application of isolation and physical or logical division of the network of critical systems, for example:
Isolation using a firewall.
Isolation of critical systems that are accessed from outside the entity in a neutral zone (DMZ).
Isolation of network segments of critical systems by means of a virtual internal network (VLAN).
Work to prevent critical systems from being connected to the Internet if these systems provide an internal service to the entity and there is no need to access the service from outside the entity.
Work on adjusting firewall menu settings so that all types of communications between network parts of critical systems are automatically blocked (Explicitly), and firewall menus are made available based on user request and business requirements and reviewed periodically.</td></tr>
<tr><td colspan="2">Expected Outputs:
Planning and drawing the infrastructure of critical systems networks.
Lists firewall for critical systems and other security configuration for networks</td></tr>
<tr><td>2-4-1-2</td><td>review firewall configuration and lists; Every six months, at least.</td></tr>
</table>

	Related cybersecurity tools: • Network Security Policy Template • Network Security Standard Template • Wireless Network Security Standard Template • Network Detection and Response Standard Template **Guidelines:** • Work on reviewing firewall settings and lists at least every six months for the firewall of critical systems networks, for example but not limited to: ○ Review unused/activated lists within the last 90 days to be deleted and disabled. ○ Update settings according to recent resource versions. ○ Arrange lists according to effectiveness and performance. ○ Review and analyze VPN lists. • Documenting the audit results to include, but not be limited to: ○ Changes after review. ○ Review date. ○ Accreditation.	
	Expected Outputs: • Report of reviewing firewall configuration for critical systems in the entity (evaluation table).	
	2-4-1-3	Prevent direct connection of any device to the local network for critical systems; Only after examining, and ensuring the availability of the verified protection elements, for the acceptable levels of critical systems.
	Related cybersecurity tools: • Network Security Policy Template • Network Security Standard Template • Wireless Network Security Standard Template • Network Detection and Response Standard Template **Guidelines:**	

- Work on providing systems to manage access control devices for networks, for example: Network Access Control (NAC).
- Work on developing procedures, to check devices and directly connect any device to the local network for critical systems after examining it using tools to scan and detect malicious software approved by the entity (End-point protection solutions) and ensure the availability of protection elements that achieve the acceptable level of critical systems, for example:
    - Ensure that protection technologies and mechanisms are capable of detecting all types of malicious software (such as Viruses, Trojan Horses, Worms, Spyware, Adware, and Rootkits) (Root Kits) and other malwares.

Expected Outputs:

- Document procedures for secure connection of critical systems to the local network.
- Proof showing the restrictions in place to ensure direct connection is prevented.

2-4-1-4	Prevent critical systems from connecting to the wireless network.

Related cybersecurity tools:

- Network Security Policy Template
- Network Security Standard Template
- Wireless Network Security Standard Template
- Network Detection and Response Standard Template

Guidelines:

- Work on developing procedures to prevent critical systems from connecting to the wireless network, for example:
    - Isolate the network of critical systems from the rest of the networks in the organization.
    - Adjust configuration for critical systems or configuration for security technologies to prevent access to the wireless network.

Expected Outputs:

	• Document prevention procedures for critical systems from connecting to the wireless network. • A guide showing setting critical systems configuration to prevent connection to the wireless network.
2-4-1-5	Network Advanced persistent threat.
	Related cybersecurity tools: • Network Security Policy Template • Network Security Standard Template • Wireless Network Security Standard Template • Network Detection and Response Standard Template **Guidelines:** • Work to provide protection systems from advanced persistent threats at the network level (Network APT) and update them continuously, for example: ○ Provide advanced protection systems to detect and prevent intrusions such as ((Intrusion Prevention/Detection Systems (IDS/IPS, HIDS/HIPS)) on all parts of the network and update them continuously.
	Expected Outputs: • A list of all available APT protection systems for critical systems.
2-4-1-6	Preventing critical systems from connecting to the Internet if they provide an internal service to the entity; There is no very necessary need to access the service from outside the entity.
	Related cybersecurity tools: • Network Security Policy Template • Network Security Standard Template • Wireless Network Security Standard Template • Network Detection and Response Standard Template **Guidelines:** • Work on developing procedures to prevent the connection of critical systems, for example: ○ Work with the concerned departments to identify critical systems that do not require access to a service from outside the entity.

	○ Working on adjusting network configuration to isolate internal critical systems from Internet connection, for example, but not limited to: adjusting firewall configuration to prevent communication or network design that completely isolates critical systems from Internet connection.	
	Expected Outputs: • Procedures document for isolating critical systems on the Internet document. • Configuration applied at the level of network devices and servers that indicate that access to the Internet is prohibited.	
	2-4-1-7	Provision of critical systems services, through networks independent of the Internet, in the event that the services of those systems are directed to limited parties; Not for individuals .
	Related cybersecurity tools: • Network Security Policy Template • Network Security Standard Template • Wireless Network Security Standard Template • Network Detection and Response Standard Template **Guidelines:** • Working to develop procedures for providing critical systems services that are provided to limited parties via networks independent of the Internet, for example but not limited to: ○ Work with the concerned departments to identify critical systems that provide services outside the entity. ○ Work to provide security solutions to provide services to limited parties securely, including but not limited to: Site-to-Site VPN.	
	Expected Outputs: • Document the procedures for providing critical systems services. • A guide explaining the settings applied at the level of network devices and servers, which describes communication through independent networks.	
	2-4-1-8	Distributed Denial of Service Attack “DDoS"
	Related cybersecurity tools: • Network Security Policy Template • Network Security Standard Template	

- Wireless Network Security Standard Template
- Network Detection and Response Standard Template
- Protection against Distributed Denial of Service (DDOS) attacks Standard template

Guidelines:

- Working to provide protection systems against network disruption attacks (Distributed Denial of Service Attack "DDoS") on critical systems and updating them continuously.
- Adjust firewall settings to protect against Distributed Denial of Service Attacks (DDoS).
- Working to apply the principle of multiple availability (High Availability) to the entity's critical systems that provide an external service, including, but not limited to: firewall systems, Web proxy systems.
- Work on concluding an agreement with the service provider or Internet service provider to implement mechanisms and ensure protection against network disruption attacks (Distributed Denial of Service Attack "DDoS").

Expected Outputs:

- Systems and technologies to protect against network disruption attacks for critical systems.
- List of Distributed Denial of Service Attack "DDoS" configuration and controls.

2-4-1-9	Allow whitelisting only for firewall lists for critical systems .

Related cybersecurity tools:

- Network Security Policy Template
- Network Security Standard Template
- Wireless Network Security Standard Template
- Network Detection and Response Standard Template

Guidelines:

- Develop whitelisting only for firewall lists for critical systems and reviewing them frequently.
- Work on adjusting the firewall list settings so that all types of communications between network parts are automatically blocked (Explicitly), and firewall lists are made available based on user request and business requirements and reviewed periodically.

	Expected Outputs: • A list showing the specific permissions for firewall lists for critical systems.	
2-5	**Mobile Devices Security**	
Objective	Ensure the protection of the party's mobile devices (including laptops, smart phones, and smart tablets) from cyber risks. ensuring safe handling of critical information and information related to the entity's business; And protecting them during transportation and storage when using personal devices for workers in the entity (BYOD principle).	
Controls		
2-5-1	In addition to the sub-controls within Control 2-6-3 in the Basic Controls of Cybersecurity, it must cover the cybersecurity requirements related to the security of mobile devices and (BYOD) devices of the entity, at a minimum; the following:	
	2-5-1-1	Restrict access from mobile devices to critical systems, except for a temporary period only; This is after conducting a risk assessment and obtaining the necessary approvals from the department concerned with cyber security in the entity.
	Related cybersecurity tools: • Workstations, Mobile Devices and BYOD Security Policy Template • User device security standard template • Mobile Devices Security Standard Template **Guidelines:** • Work to prevent access from all mobile devices to critical systems, taking into account that access is intended for other purposes and not access as an end user. • Work on developing procedures to allow access for a temporary period only when needed, for example : ○ Work on developing procedures for assessing the risks of access from mobile devices to critical systems based on business needs and obtaining the necessary approvals from the concerned department and the cybersecurity department according to the approved procedures.	

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

Access is allowed for a temporary period only, and access is immediately disabled once the period expires.
Allow access to a specific system only upon request, not all systems.

Record and monitor access attempts from mobile devices and activities related to accesses.

</td></tr>
<tr><td></td><td>
Expected Outputs:

Critical systems risk assessment procedures document.
Document procedures for granting permissions mechanisms to critical systems.
Samples of approval requests.

</td></tr>
<tr><td></td><td>
<table>
<tr><td>2-5-1-2</td><td>Full Disk Encryption for mobile devices with access to critical systems.</td></tr>
</table>
</td></tr>
<tr><td></td><td>
Related cybersecurity tools:

Mobile Devices Security Standard Template
User device security standard template
Workstations, Mobile Devices and BYOD Security Policy Template

Guidelines:

End-to-end encryption of all portable drives for critical systems using accepted methods based on, but not limited to, National Encryption Standards: AES-256-FIPS.
Work to provide technical systems and security solutions that implement the required encryption requirements.

</td></tr>
<tr><td></td><td>
Expected Outputs:

A guide demonstrating the implementation of cryptographic requirements for critical systems.

</td></tr>
<tr><td>2-6</td><td>Data and Information Protection</td></tr>
<tr><td>Objective</td><td>Ensure the protection of the party's mobile devices (including laptops, smart phones and smart tablets) from cyber risks. Ensuring secure handling of critical information and information related to the entity’s business and protecting it during transportation and storage when using the personal devices of the entity’s employees (the “BYOD” principle).</td></tr>
</table>

<table>
<tr><th colspan="3">Controls</th></tr>
<tr><td rowspan="5">2-6-1</td><td colspan="2">In addition to the sub-controls within Control 2-7-3 in the Basic Controls of Cybersecurity, it must cover the cybersecurity requirements for data and information protection; At a minimum, the following :</td></tr>
<tr><td>2-6-1-1</td><td>Not to use critical system data in a production environment other than the production environment, except after using strict controls to protect that data, such as: data masking techniques or data scrambling techniques .</td></tr>
<tr><td colspan="2">Related cybersecurity tools:
Data Cybersecurity Policy Template
Data Cybersecurity Standard Template
Guidelines:
Work on identifying and classifying critical systems data based on the relevant legislative and regulatory requirements.
Work to identify and use techniques/mechanisms to protect critical systems data when used in a non-production environment, such as: data leakage prevention techniques.</td></tr>
<tr><td colspan="2">Expected Outputs:
Reports on identifying and classifying critical systems data in the entity.
A list of technologies/mechanisms used to protect the data of critical systems in the entity.</td></tr>
<tr><td>2-6-1-2</td><td>Categorize all critical systems data.</td></tr>
<tr><td colspan="2">Related cybersecurity tools:
Data Cybersecurity Policy Template
Data Cybersecurity Standard Template
Guidelines:
Ensure that all critical systems data are classified based on the relevant legislative and regulatory requirements.</td></tr>
</table>

	• Work on defining mechanisms and methods for dealing with data based on its classification.	
	Expected Outputs: • A document showing the classification of all critical systems data with the rules taken based on the classification of the data.	
	2-6-1-3	Protect classified data of critical systems through Data Leakage Prevention techniques.
	Related cybersecurity tools: • Data Cybersecurity Policy Template • Data Cybersecurity Standard Template • Data Loss Prevention Standard Template **Guidelines:** • Work to identify and use techniques/mechanisms to prevent data leakage. • Work on preparing a data loss prevention (DLP) solution based on the entity's data classification mechanism and based on size and type, and activate the alerts feature when an attempt is made to share critical data outside the entity. • Working to develop procedures to deal with cases of data leakage of critical systems.	
	Expected Outputs: • Reports of techniques/mechanisms used to prevent critical systems data leakage. • A screenshot showing the application of data leakage (DLP) technology and activating a feature to receive alerts when an attempt is made to share critical systems data outside the entity. • Procedures for dealing with cases of critical systems data leakage.	
	2-6-1-4	Determine the required retention period for business data related to critical systems; According to the relevant legislation, and only required data is kept in production environments for critical systems .
	Related cybersecurity tools: • Data Cybersecurity Policy Template • Data Cybersecurity Standard Template	

	Guidelines: • Work on holding a workshop with stakeholders of critical systems, in addition to other relevant stakeholders from business units to determine retention periods for business data in critical systems based on data quality, data need and relevant legislation. • Work with relevant departments to delete business data whose required retention period has expired according to the retention periods for business data in critical systems and using tools to ensure data deletion, such as: destroying and destroying devices containing critical data, overwriting critical data (Data Overwrite Method).	
	Expected Outputs: • Reports retention periods for business data in critical systems, based on the quality and need of the data. • Reports of deletion of business data whose required retention period has expired in critical systems. • Reports of tools used to delete critical systems data.	
	2-6-1-5	Prevent the transfer of any production environment data of critical systems to any other environment.
	Related cybersecurity tools: • Data Cybersecurity Policy Template • Data Cybersecurity Standard Template **Guidelines:** • Work to prevent the unauthorized transfer of critical systems data from the production environment to other environments (such as development and testing) through methods such as: restricting access and defining access to the production environment to the team responsible for its operation only, and ensuring that developers or testers do not access the environment production .	
	Expected Outputs:	

	• Procedures for restricting access and defining the privileges of access to the production environment only to the team responsible for its operation.
2-7	**Cryptography**
Objective	Ensuring the proper and effective use of encryption to protect the entity's electronic information assets, in accordance with the entity's regulatory policies and procedures, and the relevant legislative and regulatory requirements.
Controls	
2-7-1	In addition to the sub-controls under Control 2-8-3 of the Basic Cybersecurity Controls, the cryptographic cybersecurity requirements should cover, at a minimum, the following :
2-7-1-1	encrypt all critical systems data; During the transfer (Data-In-Transit).
	Guidelines: • Work to identify appropriate and advanced technologies; To encrypt critical systems data in transit, for example: ○ Using the Transport Layer Security protocol, which is one of the most common encryption protocols (TLS - Transport Layer Security). ○ Applying appropriate and advanced technologies to encrypt critical systems data during transmission at the advanced level in accordance with the standard of the National Cybersecurity Authority. ○ Review the effectiveness of techniques used to encrypt critical systems data in transit.
	Expected Outputs: • Data encryption procedures during transmission at the entity. • Encryption standards approved by the entity. • Protocols and technologies used to encrypt critical systems data in transit. • Reports reviewing the effectiveness of the encryption techniques used.
2-7-1-2	encrypt all critical systems data; While storing (Data-At-Rest) at the level of files, the database, or at the level of specific columns, within the database.
	Guidelines:

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

- Work to identify appropriate and advanced technologies; To encrypt critical systems data during storage, for example:
  - Use transparent data encryption that is used on limited systems with restricted resources (TDE Transparent Data Encryption), including but not limited to: block encryption algorithms.
- Apply appropriate and advanced technologies to encrypt critical systems data during storage.
- Review the techniques used to encrypt critical systems data during storage.

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

Expected Outputs:

- Procedures for encrypting critical systems data during storage, whether at the level of files, the database, or at the level of specific columns within the database, in the entity.
- Protocols and technologies used to encrypt critical systems data during storage.

</td></tr>
<tr><td></td><td>2-7-1-3</td><td>Using updated and secure methods, algorithms, keys, and encryption devices in accordance with what is issued by the NCA in this regard.</td></tr>
<tr><td></td><td colspan="2">

Related cybersecurity tools:

- Cryptography Standard Template

Guidelines:

- Working on defining secure encryption algorithms, keys, and devices by adhering to the correct and updated application standards by reviewing them annually and ensuring that they are in line with the encryption standards issued by the Cybersecurity Authority.
- Using the advanced level of encryption methods and algorithms based on national encryption standards.
- Review the techniques used for the secure management of algorithms, keys, and cryptographic devices.

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

Expected Outputs:

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

	• Cybersecurity procedures that cover the safe management of encryption algorithms, keys, and devices at the entity (example: an electronic copy or an official hard copy). • A document defining the cycle of reviewing the effectiveness of the techniques used; For the secure management of algorithms, keys and encryption devices during their life cycle operations at the entity. • Protocols and technologies used to encrypt critical systems data.
2-8	**Backup and Recovery Management**
Objective	Ensure the protection of the entity's data, information, and technical configuration of the entity's systems and applications from damages resulting from cyber risks, in accordance with the entity's regulatory policies and procedures, and relevant legislative and regulatory requirements.
Controls	
2-8-1	In addition to the sub-controls under Control 3-9-2 in the Basic Cyber Security Controls, it should cover the cyber security requirements for managing backups, at a minimum; the following :
	2-8-1-1 The scope of online and offline backups to include all critical systems.
	Related cybersecurity tools: • Backup Standard Template • Backup Policy Template **Guidelines:** • Work on identifying databases for critical systems. • Work on identifying applications for critical systems. • Work on identifying servers for critical systems. • Work on identifying network devices for critical systems. • Defining technologies for backing up critical systems. • Apply backups to all critical systems.
	Expected Outputs:

	• Online and Offline Backup reports, which includes all critical systems that contain: the scope of the backup, the techniques used for the backup process in the entity. • Reports from applying backups for all critical systems.	
	2-8-1-2	make backups at planned intervals; Based on the entity's risk assessment, the Commission recommends that backup copies of critical systems be made on a daily basis .
	Related cybersecurity tools: • Backup Standard Template • Backup Policy Template **Guidelines:** • Work on the entity's risk assessment in accordance with the entity's regulatory policies and procedures, and in accordance with the relevant legislative and regulatory requirements. • Work to determine the sensitivity of the system and the need for data and its recentness, depending on the result of the risk assessment. • Work on defining an action plan for the periods of making backup copies of critical systems. • Work on implementing the action plan for backing up critical systems at agreed time periods.	
	Expected Outputs: • Reports from the entity's risk assessment. • An action plan for backing up critical systems according to the time plan based on the entity's risk assessment. • screenshot of a backup tool showing the latest backups taken of critical systems at agreed time intervals.	
	2-8-1-3	Secure access, storage, and transmission of backup content and media for critical systems, and protect them from unauthorized destruction, modification, or viewing.

	Related cybersecurity tools: • Storage Media Security Policy Template • Physical Security Policy Template • Backup Standard Template • Backup Policy Template **Guidelines:** • Working to secure unauthorized access, modification, and viewing of the content of backup copies of critical systems and their media, through, but not limited to: limiting access according to need and scope of work, and reviewing access permissions at regular intervals. • Working to secure the storage of backup content and media for critical systems through, but not limited to: storing off-site and physical backup media off-site in a safe and reliable location, and storing online backups separately from production environments. Testing and development. • Work to determine procedures for the safe transfer of the content of backup copies of critical systems and their media, through, but not limited to: encrypting backup data during transfer, and using safe, updated and approved transfer tools.
	Expected Outputs: • Reports of access to storage media for critical systems. • Reports of review of access rights at regular intervals. • Backup procedures. • Reports of encrypted backups in transit. • Reports of tools used to transfer security to backups.
2-8-2	Referring to Control 2-9-3-3 in Basic Cyber Security Controls, a periodic check is required; At least every three months, to determine the effectiveness of restoring backups of critical systems.
	Related cybersecurity tools: • Backup Standard Template • Backup Policy Template **Guidelines:**

	• Work on developing a plan to conduct a periodic examination at least every three months; To measure the effectiveness of restoring backups of critical systems. • Work to ensure the effectiveness of recovery procedures, by conducting a test to restore backup copies of critical systems periodically; At least every three months.
	Expected Outputs: • An action plan to test the effectiveness of backups for critical systems. • Backup Restoration Testing reports for critical systems at least every three months.
2-9	**Vulnerabilities Management**
Objective	Ensuring the protection of the entity's data and information and the technical configuration of the entity's systems and applications from damages resulting from cyber risks, in accordance with the entity's regulatory policies and procedures, and the relevant legislative and regulatory requirements.
Controls	
2-9-1	In addition to the sub-controls under Control 2-10-3 in the Cybersecurity Core Controls, the cybersecurity requirements for vulnerability management for critical systems should cover, at a minimum, the following :
	2-9-1-1 | Use reliable means and tools to find vulnerabilities.
	Related cybersecurity tools: • Cybersecurity Risk Management Procedure Template • Vulnerability Register Template • Vulnerabilities Management Policy Template • Vulnerabilities Management Standard Template **Guidelines:** • Work on identifying the tools used to discover vulnerabilities and review them to ensure their effectiveness • Work on using more than one way to discover vulnerabilities in critical systems, including:

	○ Using more than one tool approved by trusted parties to detect vulnerabilities, including open source tools. ○ Use of globally recognized vulnerability tools that have independent reports on tool effectiveness testing ○ Review vulnerabilities alerts from suppliers related to critical systems ○ Review vulnerability alerts from the National Cybersecurity Authority and the National Cybersecurity Guidance Center ○ Manual scanning to discover vulnerabilities in critical systems ○ Updating the tools used to discover vulnerabilities	
	Expected Outputs: • List of methods and tools used to discover vulnerabilities.	
	2-9-1-2	Vulnerability assessment and remediation (by installing updates and fixes packages) on technical components of critical systems, at least once a month, for critical external systems connected to the Internet; And at least every three months, for critical internal systems.
	Related cybersecurity tools: • Cybersecurity Risk Management Procedure Template • Vulnerability Register Template • Vulnerabilities Management Policy Template • Vulnerabilities Management Standard Template **Guidelines:** • Work to identify external critical systems (i.e. connected to the Internet) and internal critical systems and their technical components according to the entity's inventory of critical systems. • Evaluating vulnerabilities on all components of critical systems, determining their type, classifying their level of severity, and assigning an owner to them to be addressed by installing update and fix packages. • Ensure that the vulnerability treatment plan includes addressing the vulnerabilities discovered on external critical systems and their technical components within one month from the time they are discovered.	

<table>
<tr><td rowspan="6"></td><td colspan="2">

- Ensure that the vulnerability treatment plan includes addressing discovered vulnerabilities on internal critical systems and their technical components within three months from the time they are discovered.

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

Expected Outputs:

- Assessment reports and plans to identify the vulnerabilities discovered in critical systems and reports on the implementation of these plans.

</td></tr>
<tr><td>2-9-1-3</td><td>immediate remediation of newly discovered critical vulnerabilities; Following the change management mechanisms approved by the entity.</td></tr>
<tr><td colspan="2">

Related cybersecurity tools:

- Cybersecurity Risk Management Procedure Template
- Vulnerability Register Template
- Vulnerabilities Management Policy Template
- Vulnerabilities Management Standard Template

Guidelines:

- Ensure that the vulnerability treatment plan includes addressing critical vulnerabilities discovered on critical systems and their technical components as soon as they are discovered or as soon as they are announced by approved system developers, and identify gaps by following up on treatment plans while following the approved procedures for emergency changes by submitting requests and obtaining the necessary approvals.

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

Expected Outputs:

- A plan for the critical vulnerabilities discovered in critical systems.

</td></tr>
<tr><td>2-9-2</td><td>Referring to Control 2-10-3-1 in Basic Cyber Security Controls, vulnerabilities on technical components, of critical systems, should be scanned and discovered once a month; at least.</td></tr>
<tr><td colspan="2">

Related cybersecurity tools:

- Cybersecurity Risk Management Procedure Template

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

	• Vulnerability Register Template • Vulnerabilities Management Policy Template • Vulnerabilities Management Standard Template **Guidelines:** • Ensure that schedule scans and discovering vulnerabilities of critical systems components (including but not limited to applications, encryption devices, databases, network devices) are scheduled at least once a month.
	Expected Outputs: • Schedule scan reports and find vulnerabilities for critical systems.
2-10	**Penetration Testing**
Objective	Ensuring that technical vulnerabilities are discovered in a timely manner and addressed effectively, in order to prevent or reduce the possibility of exploiting these vulnerabilities by cyber-attacks and reduce the effects of the entity's business.
Controls	
2-10-1	In addition to the sub-controls under Control 2-11-3 in the Basic Cyber Security Controls, the cyber security requirements for penetration testing of critical systems should cover, at a minimum; the following :
	2-10-1-1 The scope of penetration testing work, to include all technical components of critical systems, and all services provided internally and externally .
	Related cybersecurity tools: • Penetration Testing Policy Template • Penetration Testing Standard Template **Guidelines:** • Ensure that penetration testing activities include all critical systems and all their technical components, for example : ○ Infrastructure ○ websites

	○ web applications ○ Smartphone and tablet applications ○ E-mail ○ Remote entry	
	Expected Outputs: • List the scope of work for penetration testing activities.	
	2-10-1-2	Penetration testing done by a qualified team.
	Related cybersecurity tools: • Penetration Testing Policy Template • Penetration Testing Standard Template **Guidelines:** • Attracting qualified human resources to perform penetration tests on critical systems, and among these qualifications: ○ Professional certifications in penetration testing (such as CEH, GPEN, OSCP, eCPPT, etc.) ○ Practical experience in penetration testing ○ Saudi citizen ○ Hold an academic degree in a related field ○ Critical vulnerability finder within vulnerability bounty programs	
	Expected Outputs: • Penetration testing team resume for critical systems.	
2-10-2	Referring to officer 2-11-3-2 in Basic Controls for Cyber Security, penetration testing must be done on critical systems, every six months; at least .	
	Related cybersecurity tools: • Penetration Testing Policy Template • Penetration Testing Standard Template **Guidelines:**	

	• Ensure that the penetration testing plan includes conducting penetration tests every six months (at least) on all critical systems and their technical components, which include: ○ Applications ○ Devices and servers ○ Databases ○ Network devices such as routers, switches, and firewalls • Work to address the observations discovered during the penetration test
	Expected Outputs: • Penetration testing work plan for critical systems. • Periodic reports of penetration tests on critical systems. • A guide explaining the follow-up treatment of discovered observations.
2-11	**Cybersecurity Event Logs and Monitoring Management**
Objective	Ensure timely collection, analysis and monitoring of cyber security event logs; For the proactive detection of cyber-attacks and effective risk management; To prevent or reduce the effects of the entity's business.
Controls	
2-11-1	In addition to the subcontrols in ECC control 2-12-3, cybersecurity requirements for event logs and monitoring management for critical systems must include at least the following:
	2-11-1-1 activate event logs for cybersecurity; on all technical components of critical systems.
	Related cybersecurity tools: • Cybersecurity Event Logs and Monitoring Management Policy Template • Cybersecurity Event Logs and Monitoring Management Standard Template **Guidelines:** • Work to provide monitoring systems compatible with the level of risk that collect and analyze the necessary event records, to collect records of cyber events for the

technical assets of critical systems, and these records must contain the following information as a minimum:

- Event Type.
- Event originator (IIS, EDR, AV, Sysmon, security logs, etc...)
- The system from which the event was executed (e.g. mailserver)
- Date and Time of Event.
- The user or tool used to carry out the event.
- The status or outcome of the event (Success vs. Failure).

- Activate and collect Event Logs, Audit Trial, and Login processes for all technical assets of critical systems.
- Create alerts for information and technology assets when predefined security monitoring events occur and/or indicator levels of potential malicious activity are met.

Expected Outputs:

- Event logs configuration for critical systems.

2-11-1-2	Enable alerts and event logs related to File Integrity Management and monitor them.

Related cybersecurity tools:

- Cybersecurity Event Logs and Monitoring Management Policy Template
- Cybersecurity Event Logs and Monitoring Management Standard Template

Guidelines:

- Work to identify and install appropriate technologies to manage and monitor file changes.
- Work on activating alerts and recording events related to managing and monitoring file changes continuously.
- Work to protect cyber security event logs from alteration, disclosure, corruption, unauthorized access and unauthorized release for example: applying encryption and passwords to logs.

	Expected Outputs: • Appropriate techniques for managing and controlling file changes • Configuration event logs to send file change alerts to critical systems for dedicated teams so they can be assured they are constantly monitored and not tampered with.	
	2-11-1-3	"User Behavior Analytics" UBA
	Related cybersecurity tools: • Cybersecurity Event Logs and Monitoring Management Policy Template • Cybersecurity Event Logs and Monitoring Management Standard Template **Guidelines:** • Work on providing specialized systems to monitor and analyze user behaviour. • Work with the concerned departments in the entity to determine the acceptable behaviour of the user on critical systems in order to determine the suspicious behaviour. • Work on developing security procedures (Incident response playbook) to be taken for cases that have been studied and identified with the concerned departments under the framework of suspicious behaviour.	
	Expected Outputs: • A list of all systems and configuration to monitor user behaviour to ensure continuous analysis. • A list of all the cases studied and analyzed. • Security measures (Incident response playbook).	
	2-11-1-4	Monitor event logs of critical systems around the clock.
	Related cybersecurity tools: • Cybersecurity Event Logs and Monitoring Management Policy Template • Cybersecurity Event Logs and Monitoring Management Standard Template **Guidelines:**	

	• Working on monitoring all cyber security events for critical systems around the clock (24/7/365) through specialized teams.	
	Expected Outputs: • Monitor event logs of systems around the clock, for example: a table showing the times of specialized teams for monitoring around the clock.	
	2-11-1-5	maintaining and protecting logs of cybersecurity incidents related to critical systems; Provided that it is comprehensive and includes full details (e.g.: time, date, identity, affected system).
	Related cybersecurity tools: • Cybersecurity Event Logs and Monitoring Management Policy Template • Cybersecurity Event Logs and Monitoring Management Standard Template **Guidelines:** • Work on developing procedures for maintaining records of events, and that they be comprehensive and include full details, with a minimum of the following: ○ Event log type: System, Security, Audit, Kernel, Authorization, Mail, etc. ○ The location and system of the event or record source. ○ The date and timestamp of the event log. ○ affected system. ○ The identity of the user or tool used to perform the event. ○ Event status: successful, failed, active, inactive, allowed, denied, etc. ○ Event Severity Level: Such as Emergency, Alert, Critical, Error, Warning, Informational Notice, or Corrective Notice. ○ Event message: an actual message from the event. • Work to restrict the archiving and deletion of event records and restrict it to authorized users only after the end of the time period specified for keeping the records, and allow the managers concerned with information and technical assets to carry out the process of archiving and deleting event records.	
	Expected Outputs: • Document procedures for maintaining event logs for critical systems.	

2-11-2	Referring to Control 2-12-3-5 in Basic Controls for Cyber Security, the period of retention of event logs related to cyber security, on critical systems, must not be less than 18 months; According to the relevant legislative and regulatory requirements.
	Related cybersecurity tools: • Cybersecurity Event Logs and Monitoring Management Policy Template • Cybersecurity Event Logs and Monitoring Management Standard Template **Guidelines:** • Develop procedures for maintaining event records for a minimum of 18 months for critical assets or for a longer period.
	Expected Outputs: • Document event log retention procedures for critical systems.
2-12	**Web Application Security**
Objective	Ensure the protection of external web applications of the entity from cyber risks.
Controls	
2-12-1	In addition to the sub-controls under Control 2-15-3 in Basic Controls for Cybersecurity, they must cover the cybersecurity requirements, to protect external web applications of the entity's critical systems, at a minimum; the following:
	2-12-1-1 Secure Session Management, including authenticity, lockout, and timeout.

	Related cybersecurity tools:
	• Web Application Protection Policy Template
	• Web Application Security Standard Template
	Guidelines:
	• Defining and documenting a secure session management process, which includes:
	  ○ Authentication of sessions
	  ○ Access
	  ○ Control

	○ Authorization ○ Lockout ○ Timeout • Use a trusted server to generate session identifiers. • Ensure that the logout function completely terminates the connection/session. • Ensure that the session inactivity timeout is as short as possible, and it is recommended that the session timeout be less than several hours.	
	Expected Outputs: • A report of a secure session, which includes: ○ Session reliability. ○ Lockout session. ○ Session timeout.	
	2-12-1-2	Implementing application security and protection standards (OWASP Top Ten) at a minimum.
	Related cybersecurity tools: • Web Application Protection Policy Template • Web Application Security Standard Template **Guidelines:** • Work on establishing a methodology to verify the application of security standards for system applications on a regular basis, with no less than annual updates, according to the OWASP organization. • Work to implement and protect each application security standard, which includes: ○ Broken Access Control service. ○ Cryptographic Failures. ○ Injection ○ Insecure design. ○ Security Misconfiguration error. ○ Vulnerable and Outdated Components. ○ Identification and Authentication Failures.	

	○ Software and Data Integrity Failures. ○ Security Logging and Monitoring Failures. ○ Server-Side Request Forgery.
	Expected Outputs: • A document explaining the application of application security standards, clarifying the minimum and the extent of the entity's compliance with the standards.
2-12-2	Referring to officer 2-15-3-2 in Basic Controls for Cybersecurity, the principle of Multi-tier Architecture must be used, provided that the number of levels is not less than 3 (3-Tier Architecture).
	Related cybersecurity tools: • Web Application Protection Policy Template • Web Application Security Standard Template **Guidelines:** • Work on the use of the multi-tier architecture principle, where critical web application components are separated on at least three levels, which consist of: ▪ Presentation/client tier. ▪ Application/business tier. ▪ Database layer.
	Expected Outputs: • Diagram of the entity's applications, showing the use of the multi-level architecture principle.
2-13	**Application Security**
Objective	Ensuring the protection of internal applications of the entity's critical systems from cyber risks.
Controls	
2-13-1	Cybersecurity requirements must be identified, documented and approved to protect the internal applications of the entity's critical systems from cyber risks.

	Related cybersecurity tools: • Web Application Security Standard Template • Procedure for Development of Cybersecurity Documents Template **Guidelines:** • Work to include and document cybersecurity requirements to protect internal web applications in the entity from cyber risks. These requirements include, for example: ○ Using the multi-tier architecture principle. ○ Use secure protocols such as HTTPS. ○ Clarify the acceptable use policy for users. ○ Secure Session Management, including authenticity, lockout, and timeout. • Developing an action plan to implement all cybersecurity requirements related to the protection of internal web applications. • Include cybersecurity requirements related to the protection of internal applications in the application protection procedures in the entity to ensure compliance with the cybersecurity requirements of all internal and external stakeholders .
	Expected Outputs: • The cybersecurity policy document that covers the requirements for protecting the entity's internal applications from cyber risks (electronic copy or official paper copy). • Official approval of the document by the head of the entity or his representative (for example: via the entity's official e-mail, or by paper or electronic signature). • An action plan document to implement cybersecurity requirements to protect the entity's internal applications. • Evidence confirming the periodic review of the implementation of cybersecurity requirements to protect the entity's internal applications. • A guide explaining the application of the entity's internal application protection controls, including but not limited to: ○ A sample of an application design that demonstrates the use of the multi-level architecture principle. ○ A screenshot of an app demonstrating the use of HTTPS.

	○ A screenshot of the application showing the deployment of the safe usage policy to users. ○ A screenshot of a secure session with it being trusted, locked, and timed out.
2-13-2	Cybersecurity requirements must be applied; To protect the internal applications of the party's critical systems.
	Guidelines: ● Work to implement all cybersecurity requirements when applying application protection measures in the entity, and the entity's application protection measures must cover, at a minimum, the following, for example: ○ Multi-tier Architecture. ○ Use secure protocols such as HTTPS. ○ Clarify the acceptable use policy for users. ○ Secure Session Management, including authenticity, lockout, and timeout. ● Developing an action plan to implement all cybersecurity requirements related to application protection. ● Include cybersecurity requirements related to application protection in the entity's application protection procedures to ensure compliance with cybersecurity requirements for all internal and external stakeholders.
	Expected Outputs: ● Application security procedures document. ● Documents confirming the application of cybersecurity requirements related to the protection of applications that are documented in the policy document. ● An action plan document to implement cyber security requirements to protect applications ● Evidence showing the application of application protection controls, for example: ○ Screenshot showing the use of the multi-level architecture principle in applications. ○ Screenshot of an application showing the use of the HTTPS protocol.

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

Screenshot of the app showing the publication of the Acceptable use policy to users.
Screenshot of a secure session including authoritative, locking, and timing out.

</td></tr>
<tr><td>2-13-3</td><td colspan="2">Cybersecurity requirements must cover; To protect the internal applications of the party's critical systems, at a minimum, the following:</td></tr>
<tr><td></td><td>2-13-3-1</td><td>Using the principle of multi-tier architecture, provided that the number of levels is not less than 3 (3-Tier Architecture).</td></tr>
<tr><td></td><td colspan="2">
Related cybersecurity tools:

Web Application Security Standard Template

Guidelines:

In the case of internal applications purchased and operated by a third party, must be:

Ensure that the supplier adheres to cyber security policies and standards, which include the use of the multi-level architecture principle.

In the event that there are applications that are developed internally or internal applications that were purchased from a third party but are operated by the entity, must be:

Determine the architectural principle levels appropriate to the nature of the web application, which should not be less than three levels:

Presentation/client tier.
Application/business tier.
Database tier.

Work to identify the relevant departments to apply the principle of multi-level architecture.
Work on applying the principle of multi-level architecture, which must not be less than three levels for all internal applications of the entity.

</td></tr>
<tr><td></td><td colspan="2">
Expected Outputs:

Design an internal application that demonstrates the use of the multi-level architecture principle for an internally developed entity-specific application.
Design an internal application that demonstrates the use of the multi-level architecture principle for an application purchased from an external party.

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

	2-13-3-2	Use secure protocols (such as HTTPS).

	Related cybersecurity tools:
	• Web Application Security Standard Template
	Guidelines:
	• In the case of internal applications purchased and operated by a third party, it must:
	  ○ Ensure that the supplier adheres to cyber security policies and standards, which include the use of secure protocols.
	• In the event that there are applications that are developed internally or internal applications that were purchased from a third party but are operated by the entity, it must:
	  ○ Determine the secure communications protocol to be applied to the internal applications of the entity, which include, for example:
	  ▪ Hypertext Transfer Protocol Security (HTTPS)
	  ▪ Secure File Transfer Protocol (SFTP)
	  ▪ Transport Layer Security protocol (TLS)
	  ○ Implementing and downloading secure communication protocols in the internal applications of the entity to protect them.
	  ○ Work to include the application and download of secure communication protocols in the application development life cycle to ensure the protection of applications to be developed in the future.	

	Expected Outputs: • List of secure protocols used in applications • An internal application demonstrating the use of the HTTPS protocol.	
	2-13-3-3	Clarify the acceptable use policy for users.
	Related cybersecurity tools: • Web Application Security Standard Template **Guidelines:** • Work on documenting the policy for the safe use of the entity's internal applications for users. • Work to include a safe usage policy on the application login page. • Ensure that the safe use policy for users is shared on the entity's internal applications.	

	Expected Outputs: • Acceptable use policy for users of internal applications. • A guide explaining the publication of the Acceptable use policy for App users.	
	2-13-3-4	Secure Session Management, including authenticity, lockout, and timeout.

	Related cybersecurity tools:
	• Web Application Security Standard Template
	Guidelines:
	• Defining and documenting a secure session management process, which includes:
	  ○ Authentication.
	  ○ Access
	  ○ Control.
	  ○ Authorization.
	  ○ Lockout.
	  ○ Timeout.
	• Use a trusted server to generate session identifiers.
	• Ensure that the logout function completely terminates the connection/session.
	• Ensure that the session inactivity timeout is as short as possible, and it is recommended that the session timeout be less than several hours.	

	Expected Outputs:
	• Screenshot of one of the secure sessions, including:
	  ○ Session reliability.
	  ○ Lockout the session.
	  ○ Session times out.	

2-13-4	Periodically review the cybersecurity requirements to protect the internal applications of the entity's critical systems.	
	Related cybersecurity tools: • Procedure for Development of Cybersecurity Documents Template **Guidelines:**	

	• Work on reviewing the application of cybersecurity requirements to protect the applications of the entity by conducting a periodic assessment (according to a documented and approved plan for review, and based on a specific period of time "for example, on a quarterly basis") to protect the applications by the department concerned with cybersecurity and in cooperation with relevant departments The relationship (such as the department concerned with information technology). • Application review may be done through traditional channels (such as email) or it may be automated using a compliance management system. The entity may develop a review plan in which it clarifies the schedule for reviewing the application of cybersecurity requirements to protect the applications of the entity. • Periodically review and update the cybersecurity requirements to protect the applications of the entity according to a documented and approved plan for review based on a specific period of time or in the event of changes in the relevant legislative and regulatory requirements. • Documenting the review and changes made to the cybersecurity requirements to protect applications in the entity and having them approved by the head of the entity or his representative .
	Expected Outputs: • The policy document indicates that it has been reviewed and updated, and the changes have been documented and approved by the head of the entity or his representative. • Official approval and approval by the head of the entity or his representative on the updated policy (for example: via the entity's official e-mail, or by paper or electronic signature).

Cybersecurity Resilience

3-1	Cybersecurity Resilience aspects of Business Continuity Management "BCM"	
Objective	Ensuring the availability of cyber security resilience requirements in managing the entity's business continuity. And ensuring that the effects of disturbances in the entity's critical electronic services and its information processing systems and devices are addressed and minimized as a result of disasters resulting from cyber risks.	
Controls		
3-1-1	In addition to the sub-controls within Control 3-1-3 in Basic Controls for Cyber Security, they must cover business continuity management in the entity, at a minimum; the following:	
	3-1-1-1	Develop a disaster recovery center for critical systems.
	Guidelines: • Develop a disaster recovery center for critical systems, which includes: ○ Determine whether the recovery center is established by the entity or is a cloud service provided by a third party, if the service is provided by a third party: ▪ The service provider must be located in the Kingdom of Saudi Arabia. ○ In the event that the entity wanted to establish its own recovery center, it is necessary to prepare and equip the recovery center, which includes, for example : ▪ Separate the disaster recovery center of critical systems from other systems. ▪ Total storage of hardware, software, and other equipment. ▪ Documenting business objectives. ▪ Define and specify the time/limit for failure and data loss. ▪ Recovery center team. ▪ Alternate/backup workspaces. ▪ Activate the remote access option.	

- Secure backups.
- Comprehensive testing strategy.

- Define a geographic area and scope for the disaster recovery center for critical systems away from the data center for critical systems.

Expected Outputs:

- Entity network diagram.
- Designing the entity's recovery center.

3-1-1-2	inclusion of critical systems; within disaster recovery plans.

Guidelines:

- Working to include critical systems; Within disaster recovery plans, it includes:
  - Identify a team for critical systems to activate procedures in disaster recovery plans.
  - Identify and evaluate risks affecting critical systems.
  - Define backup and external storage procedures for critical systems.

Expected Outputs:

- Disaster recovery plans documented and approved by the entity, which include critical systems.

3-1-1-3	conduct periodic examinations; Once a year, to ensure the effectiveness of disaster recovery plans for critical systems; at least.

Guidelines:

- conduct periodic examinations; Once a year, to ensure the effectiveness of disaster recovery plans for critical systems; At a minimum, it includes:
  - Define and document a periodic testing schedule to ensure the effectiveness of disaster recovery plans for critical systems.
  - Determine the documentation of the period of conducting the test periodically, not less than once a year.

	○ Adopting a schedule of periodic tests to ensure the effectiveness of recovery plans by those with authority. ○ Defining and documenting a plan to address feedback discovered during periodic testing to ensure the effectiveness of recovery plans.	
	Expected Outputs: • Updated report for effective testing of disaster recovery plans for critical systems. • A plan to conduct tests of the effectiveness of disaster recovery plans for critical systems in the entity.	
	3-1-1-4	The NCA recommends periodic live testing; Disaster recovery (Live DR Test) for critical systems.
	Guidelines: • NCA recommends conducting periodic live testing; For disaster recovery (Live DR Test) for critical systems, which includes: ○ Determine the Objective, intent and actions to be taken to create the post-test analysis. ○ Determine the scope of the test. ○ Confirm that the test environment is ready, and will not impact production systems or interfere with other activities. ○ Stop and review testing when problems arise and reschedule it if necessary.	
	Expected Outputs: • The live DR Testing Schedule for critical systems approved by the entity. • A recent report of a live disaster recovery test for critical systems.	

4 Third-Party and Cloud Computing Cybersecurity

4-1	Third Party Cybersecurity	
Objective	Ensure the protection of the entity's assets from cybersecurity risks related to third parties (including outsourcing and managed services). In accordance with the entity's regulatory policies and procedures, and relevant legislative and regulatory requirements.	
Controls		
4-1-1	In addition to the controls under subcomponent 4-1 of the Basic Cyber Security Controls, they must cover, at a minimum, the cyber security requirements related to third parties; the following :	
	4-1-1-1	Screening or Vetting for outsourcing companies, outsourcing personnel, and managed services working on critical systems.
	Related cybersecurity tools: • Third-Party Cybersecurity Policy Template **Guidelines:** • Work with the relevant departments to ensure that a security scan (screening or vetting) is conducted for external parties operating on critical systems, by communicating with the concerned authorities (Presidency of State Security, Ministry of Interior, etc...) to verify the criminal record of companies and workers, including: ○ Outsourcing companies. ○ Outsourcing personnel ○ Managed services companies for critical systems. ○ Managed services personnel working on critical systems.	
	Expected Outputs: • An official document from the competent authorities explaining the security scanning procedure for workers on critical systems.	

	4-1-1-2	to be backup services, managed services on critical systems; Through companies and national destinations; In accordance with the relevant legislative and regulatory requirements.
	Related cybersecurity tools: • Third-Party Cybersecurity Policy Template **Guidelines:** • Ensuring that outsourcing services and operations centers for cybersecurity services managed for the operation and monitoring of critical systems are managed by national companies through due diligence and by obtaining the companies recommendation from the National Cybersecurity Authority, and ensuring that local companies and entities comply with the relevant legislative and regulatory requirements.	
	Expected Outputs: • Service Level Agreements (SLA) contracts and agreements with third party outsourcing services and managed cybersecurity services operations centers for the operation and monitoring of critical systems. • An official document proving that the managed cybersecurity services operations centers for operation and monitoring of critical systems are entirely located within the Kingdom of Saudi Arabia (example: its existence as one of the terms of the signed contract, the existence of a service level agreement (SLA) signed between the external party and the entity, or the entity's visit to the service provider's workplace). • An acknowledgment from the provider of support services and the operations centers of cybersecurity services managed to operate and monitor critical systems to adhere to all internal policies and procedures for support services and managed services for the entity and to adhere to the relevant legislative and regulatory requirements.	
4-2	**Cloud Computing and Hosting Cybersecurity**	
Objective	Ensure that cyber risks are addressed and that cyber security requirements for cloud computing and hosting are implemented in an appropriate and effective manner, in accordance with the entity's regulatory policies and procedures, legislative and regulatory requirements, and related	

<table>
<tr><td></td><td colspan="2">orders and decisions. And ensuring the protection of the entity's information and technical assets on cloud computing services that are hosted, processed, or managed by third parties.</td></tr>
<tr><td colspan="3">Controls</td></tr>
<tr><td>4-2-1</td><td colspan="2">In addition to the sub-controls under Control 4-2-3 in the Basic Cyber Security Controls, they must cover the cyber security requirements for the use of cloud computing services and hosting, at a minimum; the following :</td></tr>
<tr><td></td><td>4-2-1-1</td><td>The site for hosting critical systems, or any part of its technical components, must be inside the entity, or in cloud computing services provided by government agencies, or national companies that fulfil the cloud computing controls issued by the NCA, taking into account the classification of the hosted data .</td></tr>
<tr><td></td><td colspan="2">Related cybersecurity tools:
Cloud Computing and Hosting Cybersecurity Policy Template
Guidelines:
Ensure the classification and coding of data in accordance with the classification and coding mechanism in the entity and the relevant legislative and regulatory requirements before hosting it with cloud computing and hosting service providers.
Ensuring that the entity's critical systems, or any part of its technical components, are hosted in a reliable and safe place within the Kingdom of Saudi Arabia, and these places include the following:
The data must be hosted within the entity.
The data is hosted by cloud computing service providers provided by government agencies in the Kingdom of Saudi Arabia.
That the data be hosted by cloud computing service providers provided by private companies, such that they are Saudi companies that have verified cloud computing controls (CCC) issued by the National Cybersecurity Authority.
Adding a feasibility study and risk assessment for private companies and obtaining a recommendation from the National Cybersecurity Authority.</td></tr>
<tr><td></td><td colspan="2">Expected Outputs:</td></tr>
</table>

	• Contracts and agreements of the entity with the cloud computing and hosting service provider for critical systems. • An acknowledgment from the cloud computing service provider that it adheres to all internal policies and procedures for the entity's cloud computing and hosting services and adheres to the relevant legislative and regulatory requirements. • A list of data that was classified before being hosted with cloud computing service providers, including but not limited to: (a file) showing the data that was classified before sharing it with the cloud computing and hosting service provider. • An official document proving that the entity's critical systems, or any part of its technical components, are hosted in a reliable and secure place within the Kingdom of Saudi Arabia.


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority