



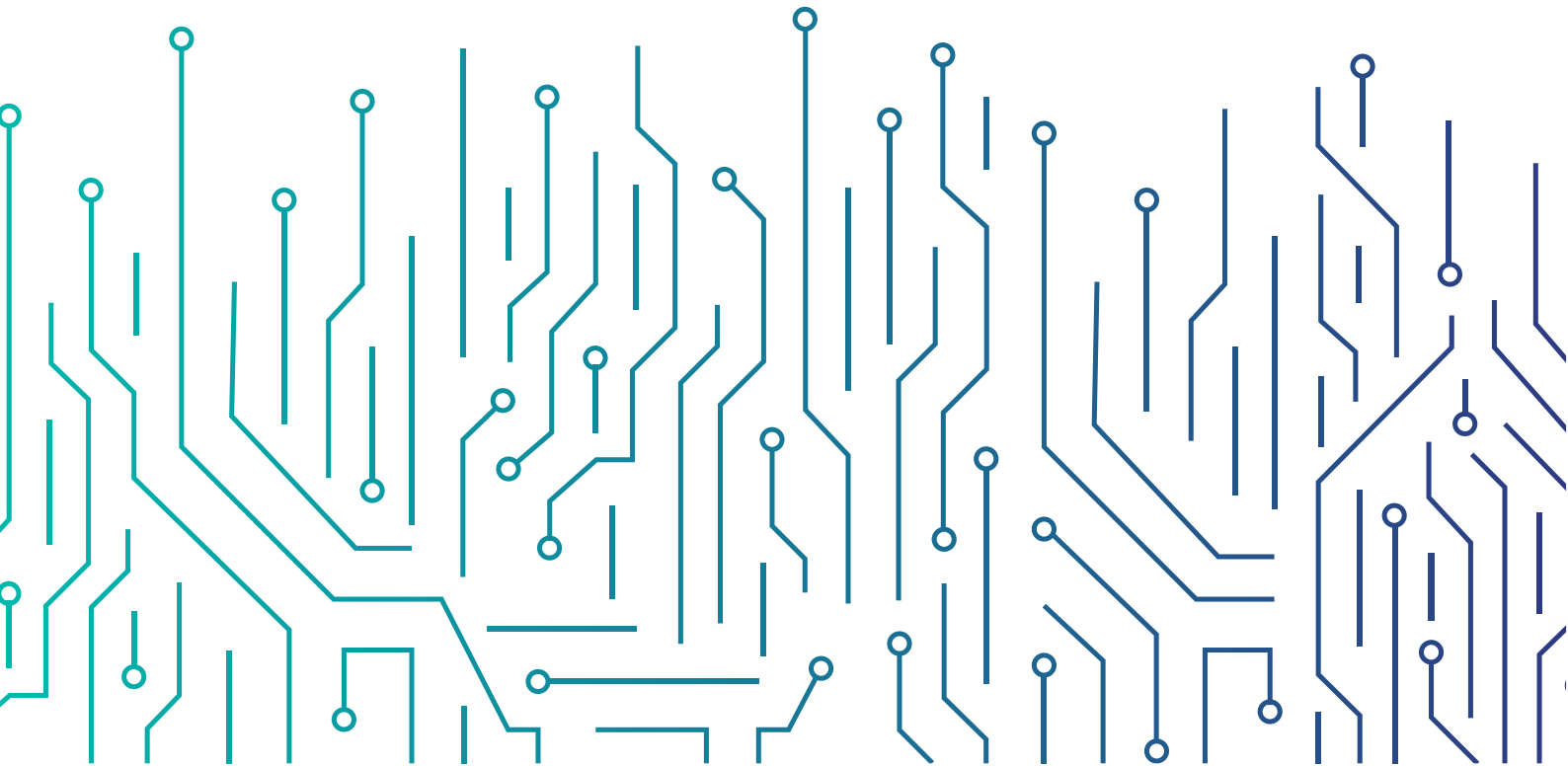
الهيئة الوطنية للأمن السيبراني  
National Cybersecurity Authority

# Operational Technology Cybersecurity Controls (OTCC -1: 2022)

---

Sharing Notice: **White**  
Document Classification: **Public**

---





**DISCLAIMER:** The following controls will be governed by and implemented in accordance with the laws of the Kingdom of Saudi Arabia, and must be subject to the exclusive jurisdiction of the courts of the Kingdom of Saudi Arabia. Therefore, the Arabic version will be the binding language for all matters relating to the meaning or interpretation of this document.



**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 Restrictions**

## Table of Contents

Executive Summary	8
Introduction	9
Objectives	9
Scope of Work and Applicability	10
Scope of work	10
Statment of Applicability	10
Implementation and Compliance	11
Update and Review	11
OTCC Methodology and Mapping	12
OTCC Controls & Sub-controls Levels	12
OTCC Domains and Subdomains	14
Structure	15
Operational Technology Sybersecurity Controls (OTCC)	16
Appendcies	37
Appendix (A): Terms and Definitions	37
Appendix (B): List of the Abbreviations	41

## List of Tabels

Table 1: OCTT Controls and Subcontrols Levels	12
Table 2: OTCC Structure	15
Table 3: Terms and Definitions	40
Table 4: List of Abbreviations	42

## Table of Figures

Figure 1: OTCC Controls and Subcontrols Levels	13
Figure 2: OTCC Main and Subdomains	14
Figure 3: Controls Coding Scheme	15
Figure 4: OTCC Structure	15

## Executive Summary

The mandate and duties of National Cybersecurity Authority (referred to in this document as “NCA”) fulfill the strategic and regulatory cybersecurity needs related to the development of national cybersecurity policies, governance mechanisms, frameworks, standards, controls, and guidelines in the kingdom of Saudi Arabia. These mandates also fulfill the need to continuously monitor the compliance of organizations to support the important role of cybersecurity, which has increased with the rise of security risks in cyberspace more than any time before.

The world witnesses a rapid advancement in Industrial Control Systems (ICS), which imposes a continuous increase in cyber threats towards these systems. This demands the necessity to have cybersecurity controls tailored for Industrial Control Systems (ICS) in order to increase the protection of critical infrastructures that operates or depends on these systems with accordance to international best practices.

From this prospective, Operational Technology Cybersecurity Controls (OTCC-1:2022) is developed to increase the protection of OT/ICS environment. These controls must be implemented as an extension to NCA’s Essential Cybersecurity Controls (ECC-1: 2018). However, the term Industrial Control Systems (ICS) includes all devices, systems, or networks used to operate and/or automate industrial processes

All applicable organizations must implement all necessary measures to ensure continuous compliance with these controls as per item 3 of Article 10 of NCA’s mandate and, as per the Royal Decree number 57231, dated 10/11/1439AH.



## Introduction

The National Cybersecurity Authority (NCA) developed Operational Technology Cybersecurity Controls (OTCC-1:2022) after completing conducting a comprehensive study of multiple national and international cybersecurity frameworks and standards. In addition to that, NCA has reviewed and leveraged international OT/ICS cybersecurity guidance, standards, and controls.

The Operational Technology Cybersecurity Controls (OTCC) contains the following:

- 4 Main Domains.
- 23 Subdomains.
- 47 Main Controls.
- 122 Subcontrols.

## Objectives

These controls are developed as an extension to the ECC in order to achieve higher levels of national cybersecurity goals by focusing on Industrial Control Systems (ICS) and defining its cybersecurity requirements. This enables national organizations to fulfill mandated cybersecurity requirements to increase the protection of its critical infrastructure and its readiness level towards cybersecurity risks.

OTCC document addresses the below four main cybersecurity pillars:

- Strategy
- People
- Process
- Technology

## Scope of Work and Applicability

### Scope of Work

These controls are applicable to Industrial Control Systems (ICSs) that reside in facilities that are deemed critical and owned and/or operated by government organizations (including ministries, authorities, establishments, and others), as well as private sector organizations owning, operating or hosting Critical National Infrastructures (CNIs), whether they are in the kingdom or abroad, which are all referred to herein as “Organization”. Critical facilities are defined as the facilities where their destruction and/or dysfunction may lead to the disruption or discontinuity of the organization’s operation. Additionally, the term Industrial Control Systems (ICS) includes all devices, systems, or networks used to operate and/or automate industrial processes.

NCA strongly encourages all other organizations in the Kingdom to leverage these controls to implement best practices to improve and enhance their OT cybersecurity.

### Statement of Applicability

Every organization within the scope of this document that owns or operates Industrial Control Systems (ICS) technologies must comply with all applicable controls in this document after ensuring that applying applicable controls will not jeopardize the continuity of the organization’s operation.

## Implementation and Compliance

To comply with item 3 of article 10 of NCA's mandate and per the Royal Decree number 57231, dated 10/11/1439H, all organizations within the scope of these controls must comply with all applicable cybersecurity controls in accordance with the appropriate control levels.

Compliance with Essential Cybersecurity Controls (ECC 1:2018) is a mandatory prerequisite for the organization.

NCA evaluates the organization's compliance with the (OTCC:1-2022) through multiple means such as self-assessment by the Organization and/or audit field visits by NCA or designated third-parties in accordance with the mechanisms approved by NCA.

### Assessment and Compliance Tool

NCA issues a tool (OTCC:1-2022 Assessment and Compliance Tool) to organize the process of the evaluation and compliance measurement against the OTCC controls.

### Facility Level Identification Tool

NCA issues a tool (OTCC:1-2022 Facility Level Identification Tool) to organize the process of the assigning the appropriate levels to the critical facility within the scope of this document.

## Update and Review

NCA will periodically review and update the OTCC (in addition to any supplement documents related to the OTCC) as per the cybersecurity requirements and related industry updates. NCA will communicate and publish the updated version of OTCC for implementation and compliance.

## OTCC Methodology and Mapping

NCA developed the OTCC Methodology and Mapping Annex, which is part of the OTCC document. The OTCC Methodology and Mapping Annex consists of the following:

- Design principles and methodology of the OTCC.
- Relationship between OTCC and ECC Domain 5.
- Relationships to multiple international standards and best practices.
- Methodology of designing OTCC main domains and subdomains.
- Methodology of defining OTCC Controls & Sub-Controls levels.

## OTCC Controls & Sub-controls Levels

There are 3 levels defined in the Operational Technology Cybersecurity Controls (OTCC) that are dependent on the following criteria:

- The criticality, consequences, and impact on the organization's business and services' availability.
- The negative impact on Health, Safety, and/or Environment (HSE) of the organization.
- The negative Impact on national economy, national security or social influence.

**Table (1) illustrates the 3 OTCC control levels based on the outcome of the facility level identification tool:**

Level	Definition	Number of Controls
Level 1 (L1)	The criticality level of the facility is <b>high</b> and have severe adverse effects, consequences, and/or impacts to operations, catastrophic or assets, resources, or Health, Safety, and Environment (HSE) of the organization.	151 controls and sub-controls (including L2 and L3 controls).
Level 2 (L2)	The criticality level of the facility is <b>moderate</b> and have significant effects, consequences, and/or impacts to operations, assets, resources, or Health, Safety, and Environment (HSE) of the organization.	117 controls and sub-controls (including L3 controls).
Level 3 (L3)	The criticality level of the facility is <b>low</b> and have moderate adverse effects, consequences, and/or impacts to operations, assets, resources, or Health, Safety, and Environment (HSE) of the organization.	56 controls and subcontrols.

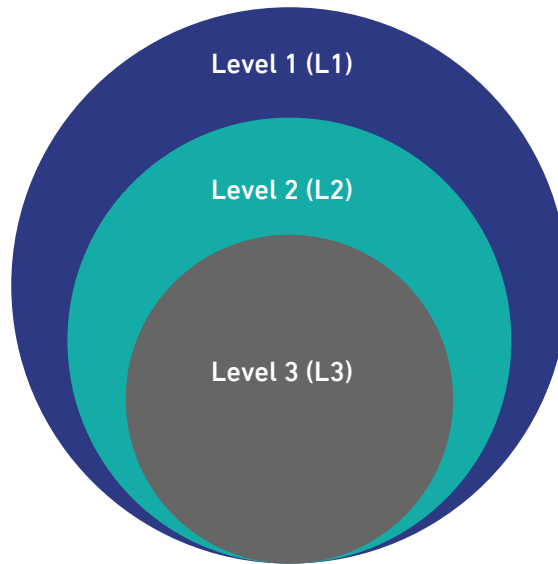


Figure 1: OTCC Controls and Subcontrols Levels

Subcontrols levels are provided in OTCC Methodology and Mapping Annex. More information and examples of how the organization can define and utilize OTCC controls and

## OTCC Domains and Subdomains

Figure (2) below shows the Main Domains and Subdomains of OTCC.

1. Cybersecurity Governance	1-1	Cybersecurity Policies and Procedures	1-2	Cybersecurity Roles and Responsibilities
	1-3	Cybersecurity Risk Management	1-4	Cybersecurity in Industrial Control System Project Management
	1-5	Cybersecurity in Change Management	1-6	Periodical Cybersecurity Review and Audit
	1-7	Cybersecurity in Human Resources	1-8	Cybersecurity Awareness and Training Program
2. Cybersecurity Defense	2-1	Asset Management	2-2	Identity and Access Management
	2-3	System and Processing Facility Protection	2-4	Network Security Management
	2-5	Mobile Device Security	2-6	Data and Information Protection
	2-7	Cryptography	2-8	Backup and Recovery Management
	2-9	Vulnerability Management	2-10	Penetration Testing
	2-11	Cybersecurity Event Logs and Monitoring Management	2-12	Cybersecurity Incident and Threat Management
	2-13	Physical Security		
3. Cybersecurity Resilience	3-1	Cyber Resilience Aspects of Business Continuity Management (BCM)		
4. Third-Party Cybersecurity	4-1	Third-Party Cybersecurity		

Figure 2: OTCC Main and Subdomains

## Structure

Figure (3) and (4) below show the meaning of controls codes:

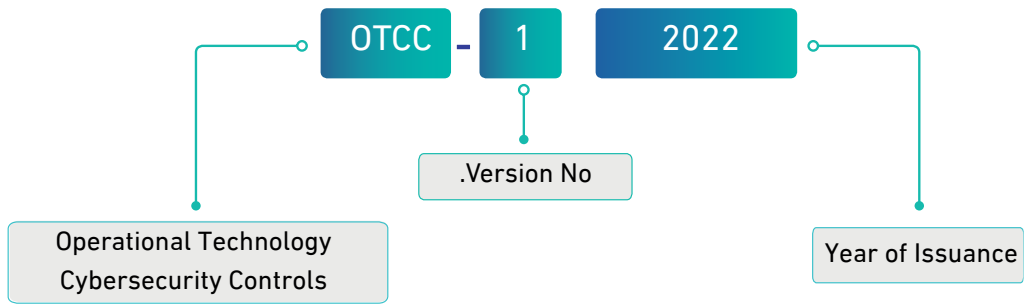


Figure 3: Controls Coding Scheme

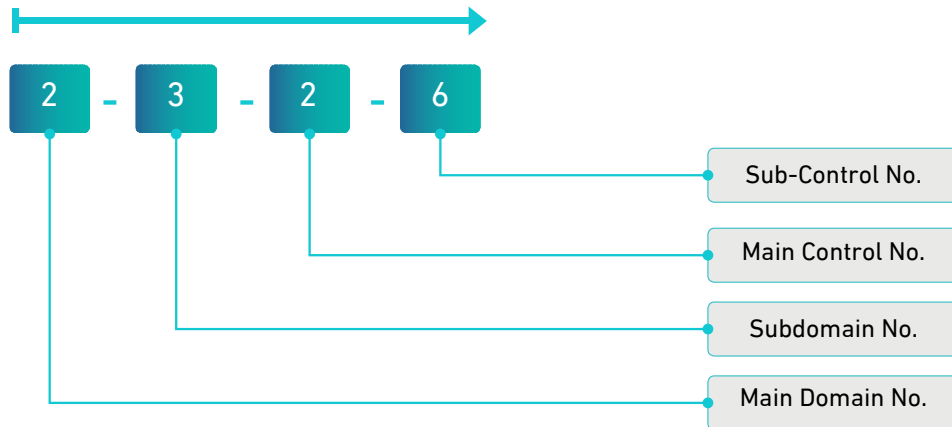


Figure 4: OTCC Structure

Table (2) below shows the methodological structure of OTCC

	Name of Main Domain			
Reference number of the main Domain				
Reference No. of the Subdomain	Name of Subdomain			
Objective				
Controls	مستوى الضابط			
	L1	L2	L3	
Control Reference Number	Control Clauses	✓	✓	✓

Table 2: OTCC Structure

## Operational Technology Cybersecurity Controls (OTCC)

### 1 **Cybersecurity Governance**

1-1	Cybersecurity Policies and Procedures			
Objective	To ensure that OT/ICS cybersecurity requirements are documented, communicated, and complied with by the organization as per related laws and regulations, and organizational requirements.			
Controls		Control level		
		L1	L2	L3
1-1-1	With reference to the ECC controls <a href="#">1-3-1</a> and <a href="#">1-3-2</a> , the organization must document, approve, and implement a customized set of cybersecurity policies and procedures for OT/ICS systems or assets.	✓	✓	✓
1-1-2	With reference to the ECC control <a href="#">1-3-3</a> , the cybersecurity OT/ICS policies and procedures must be supported by cybersecurity requirements such as vendor recommendations, implementation guidelines, and configuration management guidelines.	✓	✓	✓
1-1-3	With reference to the ECC control <a href="#">1-3-4</a> , OT/ICS cybersecurity policies and procedures must be reviewed periodically and/or when there is a change in the risks landscape, organizational structure, and/or process changes.	✓	✓	✓



1-2		Cybersecurity Roles and Responsibilities		
Objective	To ensure that roles and responsibilities are defined for all parties participating in implementing the operational technology cybersecurity controls (OTCC) within the organization.			
Controls		Control level		
		L1	L2	L3
1-2-1	In addition to the ECC subdomain 1-4, cybersecurity requirements for Cybersecurity Roles and Responsibilities in OT/ICS must include, at a minimum, the following: 1-2-1-1 Cybersecurity roles and responsibilities (RACI) assignment for all stakeholders of the OT/ICS assets must be defined, documented, communicated and approved by the Authorizing Official while ensuring there is no conflict of interest.	✓	✓	✓
	1-2-1-2 Cybersecurity roles and responsibilities related to OT/ICS assets must be assigned to the cybersecurity function in the organization.	✓	✓	
1-3		Cybersecurity Risk Management		
Objective	To ensure managing cybersecurity risks in a methodological approach in order to protect the organization's OT/ICS assets as per organizational policies and procedures, and related laws and regulations.			
Controls		Control level		
		L1	L2	L3
1-3-1	In addition to the ECC subdomain 1-5, cybersecurity requirements for cybersecurity risk management in OT/ICS must include, at a minimum, the following: 1-3-1-1 OT/ICS cybersecurity risk management methodology must be included as part of the organization's risk management and safety risk management methodologies.	✓	✓	✓

1-3-1	1-3-1-2 Cybersecurity risk assessment for OT/ICS assets must be conducted periodically while ensuring to include risks associated with signing contracts and agreements with OT/ICS related third-party organizations and/or upon changes in related regulatory requirements as part of the assessment.	✓	✓	✓
	1-3-1-3 Risk register for OT/ICS cybersecurity risks must be included as part of the organization's risk register.	✓	✓	✓
	1-3-1-4 Appropriate level assignment to facilities which include (OT/ICS) must be conducted based on approved methodology.	✓	✓	✓
	1-3-1-5 Include a qualitative analysis of cybersecurity risks within the Process Hazard Analysis (PHA) which is applied with any change in operations and/or procedures in Plants.	✓		
	1-3-1-6 In the event that cybersecurity requirements cannot be implemented within the OT/ICS environment, the specific justifications for not applying those requirements must be documented and approved by the respective cybersecurity function and the Authorizing Official.	✓	✓	✓
	1-3-1-7 In the event of risk acceptance, alternative cybersecurity controls must be clearly defined, documented, approved by the Authorizing Official, and implemented effectively for a defined-period of time while reassessing the risk continuously.	✓	✓	✓
1-4	Cybersecurity in Industrial Control System Project Management			
Objective	To ensure that cybersecurity requirements are included in project management methodology and procedures in order to maintain safe operations, confidentiality, integrity, and availability of OT/ICS assets as per organization policies and procedures, and related laws and regulations.			

Controls		Control level		
		L1	L2	L3
1-4-1	In addition to the ECC controls 1-6-2 and 1-6-3, cybersecurity requirements in OT/ICS project management must include, at a minimum, the following: 1-4-1-1 Cybersecurity requirements must be part of OT/ICS project's lifecycle.	✓	✓	✓
	1-4-1-2 Cybersecurity requirements must be included as part of any functional and acceptance testing and evaluation process (such as Factory Acceptance Testing "FAT", Site Acceptance Testing "SAT", Commissioning Testing, Change Testing, Integration Testing and Source Code Review).	✓	✓	
	1-4-1-3 Secure-by-design principles must be included as part of security architectural designs for OT/ICS environments.	✓	✓	✓
	1-4-1-4 System development environments including testing environment and integration platforms must be protected.	✓	✓	
1-4-2	Cybersecurity requirements within the organization's OT/ICS project management must be reviewed, and their implementation effectiveness is measured and evaluated periodically.	✓	✓	
1-5	<b>Cybersecurity in Change Management</b>			
Objective	To ensure that cybersecurity requirements are included in change management methodology and procedures in order to maintain safe implementation of change requests in OT/ICS environment by exercising due diligence analysis and control of the changes.			
Controls		Control level		
		L1	L2	L3
1-5-1	Cybersecurity requirements within the organization's OT/ICS change management must be defined, documented, and approved. The cybersecurity requirements must be a key part of the overall requirements of OT/ICS change management.	✓	✓	✓

1-5-2	Cybersecurity requirements within the organization's OT/ICS change management lifecycle must be implemented.	✓	✓	✓
1-5-3	In addition to the ECC controls 1-6-2 and 1-6-3, cybersecurity requirements in OT/ICS change management must include, at a minimum, the following: 1-5-3-1 Cybersecurity requirements are part of the change management lifecycle.	✓	✓	✓
	1-5-3-2 Changes are validated in a separate environment prior to implementing the changes on the production environment.	✓	✓	
	1-5-3-3 In the event that OT/ICS devices are replaced with different, but functionally equivalent devices, whether in design, testing, or operation environments, the cybersecurity of the replacement device must be validated prior to being utilized in operational environment.	✓	✓	
	1-5-3-4 Restricted processes for exceptional changes must be implemented.	✓	✓	✓
	1-5-3-5 Automated configuration and asset change detection mechanisms must be implemented.	✓	✓	
1-5-4	Cybersecurity requirements within the organization's OT/ICS change management requirements must be reviewed, and their implementation effectiveness is measured and evaluated periodically.	✓	✓	
1-6	Periodical Cybersecurity Review and Audit			
Objective	To ensure that OT/ICS cybersecurity controls are implemented and in compliance with organizational policies and procedures, as well as related national and international laws, regulations and agreements.			
Controls		Control level		
		L1	L2	L3
1-6-1	With reference to ECC control 1-8-1, the organization's cybersecurity function must review the implementation of (OTCC-1:2022) controls at least annually.	✓	✓	✓

1-6-2	With reference to ECC control 1-8-2, the implementation of (OTCC-1:2022) controls must be reviewed by independent parties within the organization, outside the cybersecurity function at least once every three years.	✓	✓	✓
1-7	Cybersecurity in Human Resources			
Objective	To ensure that cybersecurity risks and requirements related to OT/ICS personnel (employees and third party personnel) are managed efficiently prior to employment, during employment, after termination/separation as per organizational policies and procedures, and related laws and regulations.			
Controls		Control level		
		L1	L2	L3
1-7-1	In addition to subcontrols in the ECC control 1-9-3, cybersecurity requirements related to human resources for OT/ICS environment must include, at a minimum, screening or vetting of all personnel (including employees, contractors and subcontractors) who have access or can utilize OT/ICS assets prior to granting them access.	✓	✓	
1-7-2	With reference to the ECC control 1-9-6, the cybersecurity requirements for cybersecurity in human resources in OT/ICS must be reviewed, and their implementation effectiveness is measured and evaluated periodically.	✓	✓	
1-8	Cybersecurity in Human Resources			
Objective	To ensure that personnel are aware of their cybersecurity responsibilities and have the required cybersecurity awareness. It is also to ensure that personnel is provided with the required cybersecurity training, skills, and credentials needed to accomplish their cybersecurity responsibilities and to protect the organization's OT/ICS assets.			
Controls		Control level		
		L1	L2	L3
1-8-1	In addition to subcontrols in the ECC control 1-10-3, the cybersecurity awareness program must include a secure and safe interaction with the OT/ICS assets or systems.	✓	✓	✓
1-8-2	In addition to subcontrols in the ECC control 1-10-4, cybersecurity requirements in OT/ICS cybersecurity awareness and training program must include, at a minimum, the following: 1-8-2-1 customized training, qualifications, knowledge, and professional skillsets must be provided to all personnel with access to the OT/ICS assets. The organization is encouraged to utilize the reference material provided in the Saudi Cybersecurity Workforce Framework (SCyWF).	✓	✓	
	1-8-2-2 Participation in OT/ICS authorized and/or specialized organizations and groups must be encouraged to stay up-to-date on common cybersecurity practices.	✓	✓	

## 2 Cybersecurity Defense

2-1	Asset Management			
Objective	To ensure that the organization has an accurate and detailed inventory of OT/ICS assets in order to support the organization’s cybersecurity and operational requirements to maintain the production uptime, safe operations, confidentiality, integrity, and availability of OT/ICS assets.			
Controls				Control level
		L1	L2	L3
2-1-1	In addition to the controls in ECC subdomain 2-1, cybersecurity requirements for asset management in OT/ICS environment must include, at a minimum, the following: 2-1-1-1 OT/ICS assets inventory must be developed in electronic format for all OT/ICS assets, and reviewed periodically.	✓	✓	✓
	2-1-1-2 Automated solution to collect asset inventory information must be utilized.	✓		
	2-1-1-3 OT/ICS asset inventory must be stored securely.	✓		
	2-1-1-4 Asset owners for all OT/ICS assets must be identified and involved throughout the relevant asset inventory management lifecycle.	✓	✓	
	2-1-1-5 Criticality rating for all assets must be assigned, documented, and approved by asset owners.	✓	✓	
2-1-2	With reference to the ECC control 2-1-6, the cybersecurity requirements for managing OT/ICS assets must be reviewed, and their implementation effectiveness is measured and evaluated periodically.	✓	✓	
2-2	Identity and Access Management			
Objective	To ensure secure and restricted logical access to OT/ICS assets in order to prevent unauthorized access and allow only authorized access for users, which are necessary to accomplish assigned tasks.			

Controls		Control level		
		L1	L2	L3
2-2-1	In addition to subcontrols in ECC control 2-2-3, cybersecurity requirements for identity and access management in OT/ICS environment must include, at a minimum, the following: 2-2-1-1 Identity and access management lifecycle for OT/ICS is separated and independent from Information Technology (IT) including centrally managed identity and access management solutions.	✓		
	2-2-1-2 Service accounts must be managed securely for OT/ICS services, applications, systems, and devices that are separated and disconnected from interactive users account logins.	✓	✓	
	2-2-1-3 Default credentials for all OT/ICS assets must be changed, disabled, or removed.	✓	✓	✓
	2-2-1-4 Sessions must be managed securely, including session authenticity, session lockout, and session timeout termination.	✓		
	2-2-1-5 Automatic disabling/removing of service accounts, programs, or accounts related to (OT/ICS) assets must be prevented, except for monitoring systems.	✓		
	2-2-1-6 Dual approval and explicit privilege escalation mechanisms for sensitive actions within the OT/ICS environment must be employed.	✓		
	2-2-1-7 Remote access to the OT/ICS networks must be restricted and exceptionally enabled when necessary and justified. A cybersecurity risk assessment must be conducted prior to granting a remote access and its associated risks are monitored and managed. The granted access must be through trusted multi-factor authenticated and encrypted channel for a defined period of time and with limited access privilege. The remote access session must be monitored and recorded while its time duration and granted user's privilege must be in accordance with the cybersecurity risk assessment.	✓	✓	
	2-2-1-8 Secure and complex password standards must be implemented.	✓	✓	

2-2-1	2-2-1-9 Secure mechanisms to store OT/ICS assets' passwords must be used.	✓		
	2-2-1-10 With reference to the ECC subcontrol 2-2-3-5, users' identities and access rights must be reviewed in response to cybersecurity incidents, personnel roles changes, or whenever there is a change in OT/ICS system architecture.	✓	✓	
	2-2-1-11 Access shall be immediately revoked when no longer needed.	✓	✓	
2-2-2	With reference to the ECC control 2-2-4, the cybersecurity requirements for identity and access management in OT/ICS environment must be reviewed, and its implementation effectiveness is measured and evaluated periodically.	✓	✓	
2-3	System and Processing Facilities Protection			
Objective	To ensure the protection of OT/ICS systems and processing facilities (including workstations, servers and Safety Instrumented Systems "SIS") against cyber risks.			
Controls		Control level		
		L1	L2	L3
2-3-1	In addition to subcontrols in the ECC control 2-3-3, cybersecurity requirements for system and processing facility protection in OT/ICS environment must include, at a minimum, the following: 2-3-1-1 Advanced, up-to-date protection mechanisms and techniques must be utilized and securely managed to block and protect from malware, Advanced Persistent Threats (APT), malicious files, and activities.	✓	✓	
	2-3-1-2 Periodic security configurations' review and hardening must be conducted in alignment with the vendor implementation guidance or recommendations with respect to cybersecurity and organization's formal change management mechanisms.	✓		
	2-3-1-3 Periodic security patches and upgrades must be implemented in alignment with vendor implementation guidance or recommendations with respect to cybersecurity and organization's formal change management mechanisms.	✓		
	2-3-1-4 Principles of least privilege and least functionality must be applied.	✓	✓	



2-3-1	2-3-1-5 Safety Instrumented Systems (SIS) controllers must be configured in appropriate modes at all times, which prevent any unauthorized changes, and changes to improper modes are limited to exceptional cases with a specific period of time.	✓	✓	
	2-3-1-6 Application whitelisting techniques or other similar techniques must be deployed to limit the applications that are allowed to run in OT/ICS environment.	✓	✓	
	2-3-1-7 OT/ICS assets must be managed through dedicated, segmented and hardened Engineering Workstation (EWS) and Human-Machine Interface (HMI) for management purposes and maintenance.	✓		
	2-3-1-8 External storage media is scanned and analyzed against malware and APT. The scan must be executed in an isolated and secure environment.	✓	✓	
	2-3-1-9 Usage of external storage media in the production environment must be restricted unless secure mechanisms for data transfer are developed and properly implemented.	✓	✓	✓
	2-3-1-10 Systems' logs and critical files must be protected from unauthorized access, tampering, illegitimate modification and/or deletion.	✓		
	2-3-1-11 Unauthorized applications, scripts, tasks, and changes must be detected and analyzed.	✓	✓	
	2-3-1-12 New communications sessions and commands execution must be detected and analyzed.	✓	✓	
	2-3-1-13 Direct communications between the OT/ICS environment and external hosts must be detected and analyzed.	✓	✓	✓
2-3-2	With reference to the ECC control 2-3-4, the cybersecurity requirements for system and processing facilities protection in OT/ICS environment must be reviewed, and their implementation effectiveness is measured and evaluated periodically.	✓	✓	
2-4	Networks Security Management			
Objective	To ensure the protection of the organization's OT/ICS networks from cyber risks.			

Controls		Control level		
		L1	L2	L3
2-4-1	In addition to subcontrols in ECC control 2-5-3, cybersecurity requirements for network security management in OT/ICS environment must cover, at a minimum, the following: 2-4-1-1 OT/ICS environment must be segmented logically or physically from other environments or networks.	✓	✓	✓
	2-4-1-2 Different zones within the OT/ICS environment must be segmented logically or physically in accordance with the zone's appropriate level that isolates data flows and directs traffic to "Choke Points".	✓		
	2-4-1-3 Safety Instrumented Systems (SIS) must be segmented logically or physically from other OT/ICS networks.	✓	✓	✓
	2-4-1-4 Wireless technologies (such as Wi-Fi, Bluetooth, cellular, satellite, etc.) must be restricted, and to only be used when the technology meets specific business requirements and is properly secured.	✓	✓	
	2-4-1-5 Wireless technologies must be segmented logically or physically from other OT/ICS networks.	✓	✓	
	2-4-1-6 Network communications, services, and connection points between different zones must be limited to the minimum to meet operational, maintenance, and safety requirements.	✓	✓	✓
	2-4-1-7 Direct exposure of common remote authentication and access management services on external-facing hosts must be prevented.	✓	✓	✓
	2-4-1-8 Only authorized business-critical services are accessible from the internal OT/ICS networks, and accessibility to services with known vulnerabilities must be limited to the greatest extent possible.	✓	✓	✓
	2-4-1-9 Direct communications between corporate zone and OT/ICS zones must be prevented, and direct all the required connections through dedicated, secured, and hardened jump host/solution in the DMZ zone.	✓	✓	

2-4-1	2-4-1-10 Remote access point in the DMZ zone must not be connected to the OT/ICS networks unless needed, while ensuring that the session is multi-factor authenticated, recorded, and established for a defined period of time only.	✓	✓	
	2-4-1-11 Proxies must be employed between the corporate and OT/ICS zones for all machine-to-machine traffic.	✓	✓	
	2-4-1-12 Dedicated gateways must be used to segment OT/ICS networks from corporate zone.	✓		
	2-4-1-13 Dedicated DMZ zone must be used to reside any system that needs services provided by corporate zone.	✓	✓	✓
	2-4-1-14 Strict limitation on enabling/usage of industrial protocols and ports to the minimum to meet operational, maintenance, and safety requirements.	✓	✓	✓
	2-4-1-15 Periodic patches and upgrades for production assets must be certified by respective vendor and tested in a separate environment prior to implementation.	✓	✓	
	2-4-1-16 Details related to network architecture and topology, zones, network data flows, connectivity, and interdependencies must be documented, updated, and maintained.	✓	✓	✓
2-4-2	With reference to the ECC control 2-5-4, the cybersecurity requirements for network security management in OT/ICS environment must be reviewed, and their implementation effectiveness is measured and evaluated periodically.	✓	✓	
2-5	Mobile Devices Security			
Objective	To ensure the protection of mobile devices (including laptops, handheld configuration devices, network test devices, etc.) from cyber risks and to ensure the secure handling of sensitive data and the organization's information.			

Controls		Control level		
		L1	L2	L3
2-5-1	In addition to subcontrols in the ECC control 2-6-3, cybersecurity requirements for mobile device security in OT/ICS must cover, at a minimum, the following: 2-5-1-1 Usage of mobile devices for OT/ICS must be restricted unless specifically required. A cybersecurity risk assessment must be conducted where risks must be defined and managed. A management approval must be granted by respective cybersecurity function for a defined period of time only in alignment with organization's formal access management mechanisms.	✓	✓	
	2-5-1-2 Mobile devices must only be used for their intended purposes and in compliance with cybersecurity requirements of its respective zones prior to being connected to OT/ICS environment, and are hardened and updated with the latest security patches and scanned against malware and APT.	✓	✓	
	2-5-1-3 Limited and approved list of mobile devices must be defined while ensuring that only these mobile devices can be connected to OT/ICS environment.	✓	✓	
	2-5-1-4 Centralized management of mobile devices must be deployed.	✓		
	2-5-1-5 Encryptions mechanisms must be used for mobile devices authorized to access the OT/ICS assets.	✓		
2-5-2	With reference to the ECC control 2-6-4, the cybersecurity requirements for mobile devices security in OT/ICS environment must be reviewed, and their implementation effectiveness is measured and evaluated periodically.	✓	✓	
2-6	Data and Information Protection			
Objective	To ensure the confidentiality, integrity, and availability of organization's data and information as per organizational policies and procedures, and related laws and regulations.			

Controls		Control level		
		L1	L2	L3
2-6-1	In addition to subcontrols in the ECC control 2-7-3, cybersecurity requirements for data and information protection in OT/ICS must include, at a minimum, the following: 2-6-1-1 Electronic and physical data (at rest and in transit) must be protected at a level consistent with its classification.	✓	✓	✓
	2-6-1-2 Data Leakage Prevention (DLP) mechanisms must be used to protect the classified data and information.	✓	✓	
	2-6-1-3 Secure wiping mechanisms for configuration details and stored data from OT/ICS assets prior to decommissioning must be implemented.	✓	✓	
	2-6-1-4 Transfer or usage of OT systems' data in any environment other than production environment must be limited, except after applying strict controls for protecting that data.	✓		
2-6-2	With reference to the ECC control 2-7-4, the cybersecurity requirements for data and information protection in OT/ICS environment must be reviewed, and their implementation effectiveness is measured and evaluated periodically.	✓	✓	
2-7	Cryptography			
Objective	To ensure the proper and efficient use of cryptography to protect information assets as per organizational policies and procedures, and related laws and regulations.			
Controls		Control level		
		L1	L2	L3
2-7-1	In addition to subcontrols in the ECC control 2-8-3, the organization must ensure that cryptographic technologies used in OT/ICS environment are aligned with the NCA National Cryptographic Standard (NCS1:2020).	✓	✓	✓
2-7-2	With reference to the ECC control 2-8-4, the cybersecurity requirements for cryptography in OT/ICS environment must be reviewed, and their implementation effectiveness is measured and evaluated periodically.	✓	✓	
2-8	Backup and Recovery Management			
Objective	To ensure the protection of organization's data and information, including information systems and software configurations from cyber risks as per organizational policies and procedures, and related laws and regulations.			

Controls		Control level		
		L1	L2	L3
2-8-1	In addition to subcontrols in the ECC control 2-9-3, cybersecurity requirements for backup and recovery management in OT/ICS must include, at a minimum, the following: 2-8-1-1 Backups for all OT/ICS assets must be covered and stored in centralized and offline locations.	✓	✓	✓
	2-8-1-2 OT/ICS assets' critical configuration files and engineering files must be included in the backup's scope.	✓	✓	✓
	2-8-1-3 Backups must be performed periodically as per the defined OT/ICS assets classification and their associated risks.	✓	✓	✓
	2-8-1-4 Access, storage, and transfer of backups and their mediums must be secured to ensure their protection against damage, change, or unauthorized access.	✓	✓	✓
2-8-2	With reference to the ECC control 2-9-4, the cybersecurity requirements for backup and recovery management in OT/ICS environment must be reviewed, and their implementation effectiveness is measured and evaluated periodically.	✓	✓	
2-9	Vulnerabilities Management			
Objective	To ensure timely detection and effective remediation of technical vulnerabilities to prevent or minimize the probability of exploiting these vulnerabilities to launch cyber-attacks against the organization.			
Controls		Control level		
		L1	L2	L3
2-9-1	In addition to subcontrols in the ECC control 2-10-3, cybersecurity requirements for vulnerability management in OT/ICS must cover, at a minimum, the following: 2-9-1-1 Scope and activities of vulnerability assessments must be defined for OT/ICS environment as part of organization's formal vulnerability management while ensuring limited or no impact on the production environment.	✓	✓	✓
	2-9-1-2 With reference to the ECC subcontrol 2-10-3-3, remediation of newly discovered critical vulnerabilities presenting significant risks to the OT/ICS environment must be performed in a timely manner.	✓		
	2-9-1-3 With reference to the ECC subcontrol 2-10-3-1, vulnerability assessment for OT/ICS systems must be conducted periodically.	3 Months	6 Months	12 Months

2-9-2	With reference to the ECC control 2-10-4, the cybersecurity requirements for vulnerability management in OT/ICS environment must be reviewed, and their implementation effectiveness is measured and evaluated periodically.	✓	✓	
2-10	Penetration Testing			
Objective	To assess and evaluate the efficiency of the organization's cybersecurity defense capabilities through simulated cyber-attacks to discover unknown weaknesses within the technical infrastructure that may lead to a cyber-breach.			
Controls		Control level		
		L1	L2	L3
2-10-1	In addition to the subcontrols in the ECC control 2-11-3, cybersecurity requirements for penetration testing in OT/ICS must cover, at a minimum, the following: 2-10-1-1 With reference to the ECC subcontrol 2-11-3-1, scope and activities of penetration testing must be defined to ensure the coverage of OT/ICS environment and networks connected to the operational network by qualified team.	✓		
	2-10-1-2 With reference to the ECC subcontrol 2-11-3-2, penetration testing must only be conducted with limited or no impact on the production environment, or on an identical separate environment.	✓		
	2-10-1-3 With reference to the ECC subcontrol 2-11-3-2, penetration testing for OT/ICS systems must be conducted periodically.	3 Months	6 Months	12 Months
	2-10-1-4 Alternative testing methods (such as passive testing mechanisms) must be defined and Implemented to collect relevant information when a potential impact to operational production environment may occur.	✓		
2-10-2	With reference to the ECC control 2-11-4, the cybersecurity requirements for penetration testing in OT/ICS environment must be reviewed, and their implementation effectiveness is measured and evaluated periodically.	✓		

2-11	Cybersecurity Event Logs and Monitoring Management			
Objective	To ensure timely collection, analysis, and monitoring of cybersecurity events for early detection of potential cyber-attacks in order to prevent or minimize the negative impacts on the organization's operations.			
Controls		Control level		
		L1	L2	L3
2-11-1	In addition to subcontrols in the ECC control <a href="#">2-12-3</a> , cybersecurity requirements for cybersecurity event logs and monitoring management in OT/ICS must include, at a minimum, the following: 2-11-1-1 Cybersecurity event logs and audit trails must be activated for all OT/ICS assets.	✓	✓	✓
	2-11-1-2 Failure attempts in accessing the organization's monitoring systems must be detected and logged.	✓	✓	✓
	2-11-1-3 Continuous, in-depth cybersecurity log review and monitoring, covering all logs and audit trails must be conducted.	✓		
	2-11-1-4 Monitoring, detecting, and analyzing User Behaviors Analytics (UBA) must be performed.	✓		
	2-11-1-5 Upload or download activities of OT/ICS assets including Safety Instrumented Systems (SIS) must be detected.	✓		
	2-11-1-6 All remote access sessions must be monitored.	✓	✓	
	2-11-1-7 Malicious events must be detected and analyzed.	✓	✓	✓
	2-11-1-8 Logging and monitoring of new alerts when new or unauthorized devices are connected to the OT/ICS networks must be performed.	✓	✓	✓
	2-11-1-9 OT/ICS Threat Intelligence must be used and incorporated to regularly tune and refresh alerts of Security Information and Event Management (SIEM) technologies.	✓		
	2-11-1-10 All access control points between the network security boundaries and external connections must be monitored.	✓	✓	✓
2-11-2	With reference to the ECC control <a href="#">2-12-4</a> , the cybersecurity requirements for cybersecurity event logs and monitoring management in OT/ICS environment must be reviewed, and their implementation effectiveness is measured and evaluated periodically.	✓	✓	



2-12	Cybersecurity Incident and Threat Management				
Objective	To ensure timely identification, detection, effective management, and handling of cybersecurity incidents and threats to prevent or minimize negative impacts on organization's OT/ICS operation.				
Controls	Control level				
	L1	L2	L3		
2-12-1	In addition to subcontrols in the ECC Control 2-13-3, cybersecurity requirements for cybersecurity incident and threat management in OT/ICS must include, at a minimum, the following: 2-12-1-1 OT/ICS cybersecurity incident response plans must be integrated and aligned with organizational plans and its procedures such as IT incident response plans, crisis management, and Business Continuity Plan (BCP).	✓	✓	✓	
	2-12-1-2 Formal incident response and root cause analysis for any detected cybersecurity incidents must be conducted.	✓	✓	✓	
	2-12-1-3 Sequence of incident response activities necessary to restore normal operations must be defined.	✓	✓	✓	
	2-12-1-4 Incident communications plan must be established.	✓	✓	✓	
	2-12-1-5 OT/ICS including Safety Instrumented Systems (SIS) recovery procedures must be included in the incident response, system recovery plans, and business continuity plans.	✓			
	2-12-1-6 Trainings and skillsets for the organization's personnel (including employees, contractors and subcontractors) to respond to OT/ICS cybersecurity incidents must be provided.	✓	✓	✓	
	2-12-1-7 Cybersecurity incident response capabilities, readiness, and plan must be periodically tested by performing cyber-attack simulations exercises.	✓	✓		
	2-12-1-8 Threat Intelligence information must be used to identify Tactics, Techniques, and Procedures (TTPs) of activity groups targeting OT/ICS systems.	✓			

2-12-2	With reference to the ECC control 2-13-4, the cybersecurity requirements for cybersecurity incident and threat management in OT/ICS environment must be reviewed, and their implementation effectiveness is measured and evaluated periodically.	✓	✓	
2-13	Physical Security			
Objective	To ensure the protection of OT/ICS assets from unauthorized physical access, loss, theft, and damage.			
2-13-1	In addition to subcontrols in the ECC Control 2-14-3, cybersecurity requirements for physical security in OT/ICS environment must include, at a minimum, the following: 2-13-1-1 List of personnel with authorized access to facilities and sensitive locations where OT/ICS assets reside must be maintained.	✓	✓	✓
	2-13-1-2 Real-time physical intrusion detection alarms and surveillance equipment, and proper mechanisms must be implemented to recognize potential intrusions and apply the approved response actions.	✓		
	2-13-1-3 Physical access points and perimeter to sensitive OT/ICS areas shall be protected and ensure continuous monitoring.	✓	✓	✓
	2-13-1-4 Safeguards, such as locks on cabinets containing control systems or sensitive assets related to OT/ICS, must be utilized to prevent unauthorized access to devices that could provide a mechanism to compromise the OT/ICS assets.	✓	✓	✓
	2-13-1-5 Strict limitation must be enforced on the physical access to all OT/ICS assets, including Safety Instrumented Systems (SIS).	✓	✓	
	2-13-1-6 Visitor access records to restricted locations where OT/ICS reside must be maintained.	✓	✓	✓
	2-13-1-7 Work being performed by contractor or vendor personnel must be monitored.	✓	✓	
	2-13-1-8 Trainings and skillsets for the organizational security guards must be provided in line with roles and responsibilities with respect to OT/ICS physical security.	✓	✓	✓
	2-13-1-9 Physical security capabilities and readiness must be periodically tested by performing simulation exercises (such as social engineering).	✓	✓	
2-13-2	With reference to the ECC control 2-14-4, the cybersecurity requirements for physical security in OT/ICS environment must be reviewed, and their implementation effectiveness is measured and evaluated periodically.	✓	✓	



## Cybersecurity Resilience

3-1		Cybersecurity Resilience Aspects of Business Continuity Management (BCM)		
Objective	To ensure the inclusion of the cybersecurity resiliency requirements within the organization's business continuity management and to remediate and minimize the impacts on OT/ICS environment from disasters caused by cybersecurity incidents.			
Controls		Control level		
		L1	L2	L3
3-1-1	In addition to subcontrols in the ECC control 3-1-3, cybersecurity requirements for cybersecurity resilience aspects of business continuity management in OT/ICS must include, at a minimum, the following: 3-1-1-1 Activities necessary to sustain minimum operations of the OT/ICS systems must be defined.	✓	✓	✓
	3-1-1-2 Redundant OT/ICS networks, connections, and devices must be implemented in accordance to the periodic cybersecurity risk assessment.	✓	✓	
	3-1-1-3 OT/ICS cybersecurity requirements must be incorporated into the Business Continuity Plan (BCP), Business Impact Analysis (BIA), Recovery Time Objectives (RTO), and Recovery Point Objectives (RPO).	✓	✓	✓
	3-1-1-4 OT/ICS cybersecurity requirements must be incorporated into the Disaster Recovery Plan (DRP) including cybersecurity-related disaster scenarios, system failure handling procedures, and operational continuity management procedures.	✓	✓	✓
	3-1-1-5 In the event of a system failure due to a cybersecurity incident, OT/ICS assets or systems must operate on an acceptable safe mode to achieve a continuous operation.	✓	✓	✓
	3-1-1-6 Periodic testing and simulation exercises (e.g. tabletop exercises "TTX") must be conducted to test the effectiveness of OT/ICS related DRP and BCP and complete incident root cause analysis.	✓	✓	
3-1-2	With reference to the ECC control 3-1-4, the cybersecurity requirements for cybersecurity resilience aspects of business continuity management in OT/ICS environment must be reviewed, and their implementation effectiveness is measured and evaluated periodically.	✓	✓	



### Third-Party Cybersecurity

4-1	Third-Party Cybersecurity			
Objective	To ensure the protection of organizational assets against the cybersecurity risks related to third-parties, including manufactures of OT/ICS-related hardware and software, vendors of OT/ICS products and suppliers of OT/ICS-related services as per organizational policies and procedures, and related laws and regulations.			
Controls				Control level
		L1	L2	L3
4-1-1	In addition to the ECC subcontrols within controls <a href="#">4-1-2</a> and <a href="#">4-1-3</a> , cybersecurity requirements for third-party cybersecurity in OT/ICS must include, at a minimum, the following: 4-1-1-1 Cybersecurity requirements are included during procurement lifecycle for OT/ICS products and services.	✓	✓	✓
	4-1-1-2 Cybersecurity requirements for third-party evaluation, selection, and information sharing must be defined.	✓	✓	
	4-1-1-3 Third-party contractors and vendors must use formal and documented Secure Development Life Cycle (SDLC) practices for systems and components designed or deployed in OT/ICS environment.	✓	✓	
	4-1-1-4 Periodic cybersecurity assessment and audits of third-party providers must be conducted to ensure the mitigation of any identified cyber threats.	✓		
4-1-2	With reference to the ECC control <a href="#">4-1-4</a> , the cybersecurity requirements for third-party cybersecurity in OT/ICS environment must be reviewed, and their implementation effectiveness is measured and evaluated periodically.	✓	✓	

## Appendices

### Appendix (A): Terms and Definitions

Table (3) below highlights some of the terms and their definitions which were used in this document.

Terminology	Definition
<b>Access Control</b>	Protection of system resources against unauthorized access; a process by which use of system resources is regulated according to cybersecurity policy and is permitted by only authorized entities (users, programs, processes, or other systems) according to that policy.
<b>Activity Group</b>	A collection of "similar" intrusions and malicious activity, behaviors or processes, capabilities, and infrastructure.
<b>Applications Whitelisting</b>	It is the security practice of specifying an index of approved software applications that are permitted to be present and active on the organization's end-users machines and servers. The goal of whitelisting is to protect the organization's end-users machines and servers from potentially harmful applications.
<b>Availability</b>	The management, operational, and technical controls (e.g., safeguards or countermeasures) employed by an organization in lieu of the recommended controls that provide equivalent or comparable protection for OT/ICS assets.
<b>Alternative Controls</b>	The management, operational, and technical controls (e.g., safeguards or countermeasures) employed by an organization in lieu of the recommended controls that provide equivalent or comparable protection for OT/ICS assets.
<b>Choke Point</b>	A choke point is a single point through which all incoming and outgoing network traffic is funneled.
<b>Communication Plan</b>	A section of an incident response plan that includes communications procedures for both internal and external stakeholders in the event of an incident.funneled.
<b>Confidentiality</b>	Maintaining authorized restrictions on access to and disclosure of information, including means of protecting information.
<b>Consequence</b>	Result of an incident, usually described in terms of health and safety effects, environmental impacts, loss of property, loss of information (for example, intellectual property), and/or business interruption costs that occur from a particular incident.
<b>Countermeasure</b>	Action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

Terminology	Definition
<b>Criticality</b>	A measure of the degree to which an organization depends on the OT/ICS for the success of a mission or of a business function.
<b>Critical Systems</b>	Any system or network whose failure, unauthorized change to its operation, unauthorized access to it, or to the data stored or processed by it; may result in negative impact on the organization's businesses and services' availability, or cause negative economic, financial, security or social impacts on the national level.
<b>Defense in Depth</b>	Provision of multiple cybersecurity protections, especially in layers, with the intent to delay if not prevent an attack.
<b>Demilitarized Zone</b>	Perimeter network segment that is logically between internal and external networks.
<b>Factory Acceptance Test</b>	A test of the OT/ICS equipment, conducted at the vendor facility where the equipment was constructed after the completion of assembly and configuration, performed to validate compliance with the functional specifications and proper operation of the equipment in a location where problems can be more easily identified and remediated.
<b>Industrial Control System</b>	A collective term used to describe different types of control systems and associated instrumentation, which includes the devices, systems, networks, and controls used to operate and/or automate industrial processes.
<b>Industrial Internet of Things</b>	The extension and use of the internet of things (IoT) in industrial sectors and applications.
<b>Information Technology</b>	The technology involving the development, maintenance, and use of computer systems, software, and networks for the processing and distribution of data; generally considered the business and administrative systems within an organization.
<b>Integrity</b>	Quality of a system reflecting the logical correctness and reliability of the OS, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data.

Terminology	Definition
<b>Jump Host</b>	A single, remote access point through which all ingress network traffic must pass between a higher-level zone and a lower level zone.
<b>Network Segmentation</b>	The act or practice of splitting a computer network into subnetworks, each being a network segment.
<b>Network Segregation</b>	The process to develop and enforce a ruleset for controlling the communications between specific hosts and services.
<b>Operational Technology</b>	The system of components, including network devices, computers, servers, cybersecurity devices, infrastructure equipment, and applications that support operations, maintenance, monitoring, and cybersecurity of the OT/ICS environment.
<b>Process Hazard Analysis</b>	A set of organized and systematic assessments of the potential hazards associated with an industrial process addressing known hazards with the process, previous incidents, engineering and administrative controls in place, consequences of the failure of those engineering and administrative controls, facility siting, human factors, and a qualitative evaluation of HSE effects.
<b>Impact</b>	A measure of the ultimate loss or harm associated with a consequence.
<b>RACI Matrix</b>	Responsible, Accountable, Consulted, Informed Matrix. Matrix that maps each player in a process, capability or function with the degree of involvement and responsibility undertaken in the process.
<b>Role-Based Access Control</b>	A method of restricting network access based on the roles of individual users within an enterprise. RBAC lets employees have access rights only to the information they need to do their jobs and prevent them from accessing information that does not pertain to them.
<b>Secure by Design</b>	A methodology to systems and software development and networks design that seeks to make systems, software and networks free from cybersecurity vulnerabilities/weaknesses and impervious to cyber-attack as much as possible through measures such as: continuous testing, authentication safeguards, and adherence to best programming and design practices.

Terminology	Definition
<b>Site Acceptance Test</b>	A test of the OT/ICS equipment conducted on-site at the organization's facility after completion of the installation and configuration of the equipment performed to validate compliance with the functional specifications, proper operation of the equipment in conjunction with other components not possible in the factory acceptance testing (FAT) such as instrumentation and associated process equipment furnished and installed by others.
<b>Source Code Review</b>	A process that is conducted manually/ automatically to identify security-related weaknesses (flaws) in set of commands and instructions written in one of programming languages.
<b>Tabletop Exercise</b>	A simulated exercise designed to test the detection and response capabilities of an organization's operational environment. The organization's response teams are guided through a fictional, but realistic OT/ICS focused cybersecurity event scenario in a discussion-based format. The goal of the exercise is to improve an organization's IRP, BCP, and DRP, as well as provide facilitated training to its response teams.
<b>Tactics, Techniques, and Procedures</b>	The behavior of a cyber-adversary. A tactic is the highest-level description of the behavior and represents the "why" of a technique (e.g. achieve credential access). Techniques represent "how" and adversary achieves a tactical goal by performing an action (e.g. dump credentials to achieve credential access). Procedures are the specific implementation the adversary uses for techniques (e.g. using PowerShell to inject into lsass.exe to dump credentials).
<b>User Behaviors Analytics</b>	Track, collect and analyze user data, and identify patterns of user activities in order to detect harmful or unusual behaviors.
<b>Zone</b>	Grouping of logical or physical assets that share common cybersecurity requirements.

Table 3: Terms and Definitions



## Appendices

### Appendix (B): List of the Abbreviations

Table (4) below highlights some of the terms and their definitions which were used in this document.

Abbreviations	Full term
BCM	Business Continuity Management.
BCP	Business Continuity Plan.
BIA	Business Impact Analysis.
CNI	Critical National Infrastructure.
DMZ	Demilitarized Zone.
DRP	Disaster Recovery Plan.
ECC	Essential Cybersecurity Controls.
EWS	Engineering Workstation.
FAT	Factory Acceptance Test.
HMI	Human-Machine Interface.
HSE	Health, Safety, and Environmental.
I/O	Input/output.
IRP	Incident Response Plan.
MDM	Mobile Devices Management.

Abbreviations	Full term
NCS	National Cryptographic Standards.
OT	Operational Technology.
OTCC	Operational Technology Cybersecurity Controls.
PHA	Process Hazard Analysis.
RACI	Responsible, Accountable, Consulted, and Informed.
RPO	Recovery Point Objective.
RTO	Recovery Time Objective.
SCyWF	Saudi Cybersecurity Workforce Framework.
SDLC	Software Development Life Cycle.
SIEM	Security Information and Event Management.
SIS	Safety Instrumented System.
TLP	Traffic Light Protocol.
TTP	Tactics, Techniques, and Procedures.
TTX	Tabletop Exercise.
VPN	Virtual Private Network.

Table 4: List of Abbreviations







الهيئة الوطنية للأمن السيبراني  
National Cybersecurity Authority

