الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Guide to Operational Technology Cybersecurity Controls (OTCC) Implementation

(GOTCC-1:2023)

TLP: white

Document Classification: Public

Disclaimer: This Guide has been developed by the National Cybersecurity Authority to enable organizations to implement the OTCC. The National Cybersecurity Authority disclaims responsibility for relying solely on this document and emphasizes the importance of considering the organization's specific requirements and environment. The National Cybersecurity Authority clarifies that this guide serves as an illustrative model and does not necessarily mean that this is the only method of implementing OTCC, as long as alternative methods align with the National Cybersecurity Authority. This document contains some illustrative deliverables related to the implementation of OTCC. The assessor or auditor has the right to request other evidences as deemed necessary to ensure that all OTCC are implemented.

In the Name of Allah,

The Most Gracious,

The Most Merciful

Traffic Light Protocol (TLP):

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

Red – Personal, Confidential and for 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

Introduction 6
Objectives 6
Scope of Work 6
OTCC Domains and Subdomains 7
Structure of the Guideline 7
OTCC Implementation Guidance 10

List of Figures

Figure 1: OTCC Main Domains and Subdomains 7
Figure 2: OTCC Structure 8

Introduction

The National Cybersecurity Authority (referred to in this document as "NCA") developed a guide for implementing the cybersecurity controls stipulated in the OTCC-1: 2022 (referred to in this document as "Controls"), to enable national organizations to implement the requirements to comply with the OTCC. This guide was developed based on the information and experiences that NCA collected and analyzed since the publication of the Controls, and was aligned with cybersecurity best practices to facilitate the implementation of the Controls across national organization.

Objectives

The main objective of this guide is to enable national organizations to fulfill compliance requirements for the OTCC implementation, strengthen their cybersecurity, and reduce cybersecurity risks that may arise from internal and external cyber threats.

Scope of Work

This guide's scope of work is the same as the OTCC-1:2022's: These controls are applicable to government organizations in the Kingdom of Saudi Arabia (including ministries, authorities, establishments, and others) and their companies and entities, as well as private sector organizations owning, operating, or hosting Critical National Infrastructures(CNIs), which are all referred to herein as "The Organization". The NCA strongly encourages all other organizations in the Kingdom to leverage this guide to implement best practices to improve and enhance their cybersecurity.

OTCC Domains and Subdomains

Figure 1 below show the main domain 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 Managment	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 Facilities Protection	2-4	Network Security Management
		2-5	Mobile Devices 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	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)		
4	Third-Party and Cloud Computing Cybersecurity	4-1	Third-Party Cybersecurity		

Figure 3: OTCC Main Domains and Subdomains

Guide Structure

Figure 2 below show the structure of OTCC

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

Figure 2: OTCC Structure

OTCC Implementation General Guidelines

General Guidelines
• Identify facilities and classify them according to the approved mechanism in the facility level identification tool issued by the NCA and review them periodically. • Identifying assets and operational systems within the facilities, and reviewing them periodically. • Identifying user accounts with sensitive privileges, who have the ability to access or manage the operational systems, and reviewing them periodically • Identify and document the Operational Technology Cybersecurity requirements, along with associated roles and responsibilities, and having them authorized by the authorizing official, reviewing them periodically. • Review the ECC guidelines and work on implementing the controls related to the OTCC. • Develop a plan to implement OTCC, and monitor it continuously

OTCC Implementation Guideline

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	
1-1-1	With reference to the ECC controls 1-3-1 and 1-3-2, the organization must document, approve, and implement a customized set of cybersecurity policies and procedures for OT/ICS systems or assets.
	Related cybersecurity tools: • Procedure for Development of Cybersecurity Documents Template • Cybersecurity Policy for Operational Technology Template **Controls implementation guidelines:** • Identify the OT/ICS cybersecurity requirements, and document them in the cybersecurity policies, standards, and procedures specified OT/ICS. So that they are approved by the authorized person in the organization based on the approved authority guide within the organization. • Ensure that policies and procedures are communicated through the approved communication channels according to the scope specified in the policy to internal and external personnel (employees and contractors). • Develop and monitor periodically an action plan to implement OT/ICS cybersecurity policies and procedures that cover all internal and external personnel (employees and contractors) to ensure that all requirements are fully and effectively implemented. • The Cybersecurity department shall ensure that cybersecurity controls are implemented, and that documented and approved policies and procedures are adhered to.
	Expected Deliverables: • OT/ICS cybersecurity policies, standards, and procedures are all documented and approved by the authorized personnel within the organization or their delegate . • Confirmation that the organization is publishing policies, standards, and procedures specific to the OT/ICS for employees and relevant parties.
1-1-2	With reference to the ECC control 1-3-3, the cybersecurity OT/ICS policies and procedures must be supported by cybersecurity requirements such as vendor recommendations, implementation guidelines, and configuration management guidelines.
	Related cybersecurity tools:

	• Operational Technology/Industrial Control Systems (OT/ICS) Security Standard Template • Cybersecurity Policy for Operational Technology Template **Controls implementation guidelines:** • Identify, document, and adopt technical standards to cover the assets related to OT/ICS within the organization (e.g., vendor recommendations, implementation guidelines, and configuration management guidelines, etc...) • Disseminate technical standards to relevant departments within the organization (e.g., the department responsible for operational systems in the facility) and ensuring their periodic implementation on assets related to OT/ICS.
	Expected Deliverables: • Documents of cybersecurity standards specific to OT/ICS adopted within the organization. • Evidence confirming the implementation of cybersecurity policies and procedures specific to OT/ICS within the organization.
1-1-3	With reference to the ECC control 1-3-4, 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.
	Related cybersecurity tools: • Cybersecurity Policy for Operational Technology Template **Controls implementation guidelines:** • Review the OT/ICS cybersecurity policies, procedures and standards in the organization periodically based on defined frequency In the policy document (e.g., conduct the periodical review every year). • Review and update the OT/ICS cybersecurity policies, procedures and standards in the case of changes in related laws and regulations (e.g., when new legislative cybersecurity framework that applies to the organization is issued). • Review and update the OT/ICS cybersecurity policies, procedures and standards when changes occur that effect the security and safety of OT/ICS (e.g., changes in the level or nature of risks or in operational processes and procedures). • Document the review and changes to the OT/ICS cybersecurity policies, procedures and standards in the organization and obtaining approval from the head of the organization or his/her delegate.
	Expected Deliverables: • A certified document that specifies the review schedule. • Approved document of OT/ICS policies, procedures and standards, which show that they have been reviewed periodically based on the specified time frame for the review. • Policy, procedure, and standard document that outlines the review, update, documentation of changes, and approval by the authorized personnel.

	• Official approval and endorsement by the authorized personnel of the updated policies, procedures, and standards.

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		
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.
	Related cybersecurity tools: • Template for Cybersecurity Roles and Responsibilities **Controls implementation guidelines:** • Identify and document cybersecurity roles and responsibilities related to OT/ICS in a (RACI) matrix, ensuring that all parties involved in implementing cybersecurity controls within the organization are aware of their responsibilities in implementing cybersecurity programs and requirements, while considering avoiding conflicts of interest. • Ensuring that the organizational structure, roles, and responsibilities within the organization are endorsed by the executive management, through the approval and endorsement of the authorized personnel. • Working to include the following roles and responsibilities (including but not limited to): ○ Roles and Responsibilities related to the head of the cybersecurity function. ○ Roles and Responsibilities related to the cybersecurity function (e.g., developing and updating cybersecurity policies and standards, conducting cybersecurity risk assessments, ensuring compliance with cybersecurity policies and legislations, monitoring cybersecurity events, vulnerability scanning, implementing cybersecurity awareness programs, etc.). ○ Roles and Responsibilities related to cybersecurity for other departments within the organization (e.g., the operation department, human resources department, industrial security department, etc.). ○ Roles and Responsibilities related to cybersecurity for all employees, contractors, and subcontractors.	
	Expected Deliverables: • Organizational Structure Document • The document containing the cybersecurity roles and responsibilities in a (RACI) matrix related to OT/ICS that is approved by the organization (hard or soft approved copies).	

	• Proof of disseminating cybersecurity roles and responsibilities document related to the organization.	
	1-2-1-2	Cybersecurity roles and responsibilities related to OT/ICS assets must be assigned to the cybersecurity function in the organization.
	Related cybersecurity tools: • Template for Cybersecurity Roles and Responsibilities **Controls implementation guidelines:** • Assign clear ownership and accountability for OT/ICS cybersecurity related roles and responsibilities to the cybersecurity function, while ensuring there is no conflict of interest.	
	Expected Deliverables: • Proof showing assigning clear ownership and accountability for OT/ICS cybersecurity related roles and responsibilities to the cybersecurity function, while ensuring there is no conflict of interest.	

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		
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.
	Related cybersecurity tools: • Template for Cybersecurity Operational Technology Policy • Template for Cybersecurity Risk Management Procedure • Template for Cybersecurity Risk Register **Controls implementation guidelines:** • Develop and implement a dedicated OT/ICS cybersecurity risk management methodology and extend the organization's risk management and safety risk management methodologies with that. • Review and verify that the prepared OT/ICS cybersecurity risk management methodology is a part of and in line with the general organization's risk management and safety risk management methodologies. • Develop a periodic review plan and prepare summary reports.	
	Expected Deliverables: • Approved OT/ICS cybersecurity risk management methodology. • A proof that OT/ICS cybersecurity risk management methodology is part of the general organization's risk management and safety risk management methodologies.	

	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.
	Related cybersecurity tools: • Template for Cybersecurity Industrial Control Systems Policy • Template for Cybersecurity Risk Management Procedure • Template for Cybersecurity Risk Register **Controls implementation guidelines:** • Conduct cybersecurity risk assessment for OT/ICS assets periodically (based on a defined frequency). • Conduct cybersecurity risk assessment before signing contracts and agreements with third-party organizations related to OT/ICS. • Conduct cybersecurity risk assessment when there are changes in related regulatory requirements.	
	Expected Deliverables: • Cybersecurity risk assessment for OT/ICS assets reports. • OT/ICS risk register. • A proof that OT/ICS risk assessment is conducted periodically and includes risk assessment associated with the signing of contracts and agreements with OT/ICS related third-party organizations and/or upon changes in related regulatory requirements.	
	1-3-1-3	Risk register for OT/ICS cybersecurity risks must be included as part of the organization's risk register.
	Related cybersecurity tools: • Template for Cybersecurity Operational Technology Policy • Template for Cybersecurity Risk Management Procedure • Template for Cybersecurity Risk Register **Controls implementation guidelines:** • Develop a risk register for the (OT/ICS) assets. • Include the (OT/ICS) risk register in the organization's risk register.	
	Expected Deliverables: • OT/ICS risk register. • A proof that OT/ICS risk register is 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.
	Related cybersecurity tools: • Template for Cybersecurity Operational Technology Policy	

- Template for Cybersecurity Risk Management Procedure
- Template for Cybersecurity Risk Register

Controls implementation guidelines:

- Document and approve the methodology used for the appropriate level assignment to facilities which include (OT/ICS).
- Ensure that the appropriate level assignment process is conducted in line with the approved methodology.

Expected Deliverables:

- Approved document containing OT/ICS facilities level assignment methodology.
- A proof that a proper level assignment process is conducted in line with the 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.

Related cybersecurity tools:

- Template for Cybersecurity Operational Technology Policy
- Template for Cybersecurity Risk Management Procedure
- Template for Cybersecurity Risk Register

Controls implementation guidelines:

- Update the Process Hazard Analysis procedures and include cybersecurity risks within the study.
- Ensure that the qualitative analysis of the OT/ICS cybersecurity risks are included in the Process Hazard Analysis (PHA) study report.

Expected Deliverables:

- A proof that the Process Hazard Analysis procedures are updated to include cybersecurity risks within the study.
- Latest report of the Process Hazard Analysis study.

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.

Related cybersecurity tools:

- Template for Cybersecurity Operational Technology Policy
- Template for Cybersecurity Risk Management Procedure
- Template for Cybersecurity Risk Register

Controls implementation guidelines:

- In case cybersecurity requirements cannot be implemented within the OT/ICS environment, the following shall be implemented:
  - Document the specific justifications for not applying those requirements; this include an official letter from the vendors in case they don't recommend applying such requirement due to technical or operational reasons showcasing the details and technical justifications.
  - Conduct cybersecurity risk assessment to identify the risks from not applying such control, and include the alternative controls following the risk acceptance process.

	○ Obtain approval from cybersecurity function and the authorizing official.	
	Expected Deliverables: • The document containing the specific justifications for not applying the selected requirements; this include an official letter from the vendors in case they don't recommend applying such requirement due to technical or operational reasons showcasing the details and technical justifications. • The cybersecurity risk assessment report containing the alternative controls, while following the risk acceptance process. • The approval from 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.
	Related cybersecurity tools: • Template for Cybersecurity Operational Technology Policy • Template for Cybersecurity Risk Management Procedure • Template for Cybersecurity Risk Register **Controls implementation guidelines:** • In the event of risk acceptance: ○ Clarifying and documenting residual risks, and obtaining approval from the authorizing official ○ Define and document alternative cybersecurity controls, then obtain approval by the respective cybersecurity function and the Authorizing Official. ○ Alternative cybersecurity controls must be implemented effectively for a defined period of time. ○ Continuously reassess the risk and the effectiveness of the alternative cybersecurity controls.	
	Expected Deliverables: • Cybersecurity risk assessment report showcasing the documentation of alternative cybersecurity controls. • Approval of the respective cybersecurity function and the authorizing official. • A proof that alternative cybersecurity controls are implemented for a defined period of time. • A proof that the risk and the effectiveness of the alternative cybersecurity controls are continuously reassessed.	

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		
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.
	Related Cybersecurity Tools: • Template for Cybersecurity requirements checklist on IT and change management projects • Template for Cybersecurity Operational Technology Policy **Controls implementation guidelines:** • Develop cybersecurity requirements and include them into the OT/ICS project's lifecycle (initiation, planning, execution, closing). • Approve the updated OT/ICS project's lifecycle. • Verify and ensure that all OT/ICS projects are in line with the defined and approved OT/ICS project's lifecycle requirements.	
	Expected Deliverables: • Document outlining the project management methodology for OT/ICS, detailing cybersecurity requirements throughout the lifecycle of projects related to OT/ICS • Evidence confirming that the project management methodology of OT/ICS, which outlines cybersecurity requirements throughout the lifecycle of projects related to OT/ICS, is up-to date and approved by the authorizing official or his/her delegate. • Evidence confirming that all projects related to OT/ICS are compliant with and adhere to the cybersecurity requirements approved in the lifecycle of projects related to OT/ICS	
	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).
	Related cybersecurity tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Checklist for Cybersecurity Requirements in Software Development **Controls implementation guidelines:** • Develop, document and include cybersecurity requirements within Factory Acceptance Testing "FAT", Site Acceptance Testing "SAT", Commissioning Testing, Change Testing, Integration Testing, and Source Code Review.	

- Verify and ensure that all Factory Acceptance Testings "FAT", Site Acceptance Testings "SAT", Commissioning Testings, Change Testings, Integration Testing, and Source Code Review are conducted in line with the defined OT/ICS cybersecurity requirements.

Expected Deliverables:

- A proof that Factory Acceptance Testing "FAT", Site Acceptance Testing "SAT", Commissioning Testing, Change Testing, Integration Testing, and Source Code Testing are in line with OT/ICS cybersecurity requirements.
- Sample of the latest forms used related to Factory Acceptance Testing "FAT", Site Acceptance Testing "SAT", Commissioning Testing, Change Testing, Integration Testing, and Source Code Testing showcasing the inclusion of cybersecurity requirements.

1-4-1-3	Secure-by-design principles must be included as part of security architectural designs for OT/ICS environments.

Related cybersecurity tools:

- Template for Cybersecurity Operational Technology Policy
- Template for OT/ICS Security Standard
- Checklist for Cybersecurity Requirements in Software Development

Controls implementation guidelines:

- Define and include secure-by-design principles in security architectural designs for OT/ICS environments.
- Implement secure-by-design principles for OT/ICS environments.
- Verify and ensure that all OT/ICS environments are designed using the secure-by-design principles.

Expected Deliverables:

- Documented requirements for security architectural designs for OT/ICS environments showcasing the secure-by-design principles.
- A proof that all security architectures for OT/ICS environments are designed based on secure-by-design principles.

1-4-1-4	System development environments including testing environment and integration platforms must be protected.

Related cybersecurity tools:

- Template for Cybersecurity Operational Technology Policy
- Template for OT/ICS Security Standard
- Checklist for Cybersecurity Requirements in Software Development

Controls implementation guidelines:

- Identify if there is a system development environments including testing environment and integration platforms.
- Define and document a procedure containing requirements related to the protection of the identified environments.
- Approve the procedure by the systems owner.

	• Verify and ensure that the identified environments are protected in line with defined procedure.
	Expected Deliverables: • List of identified system development environments. • The approved procedure by systems owner. • A proof that all identified environments are protected in line with defined procedure.
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.
	Related cybersecurity tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Key Performance Indicator Report **Controls implementation guidelines:** • Regularly review cybersecurity requirements within OT/ICS project management according to a documented and approved review plan based on a specific time frame (e.g., conducting annual periodic reviews). • Develop key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically (based on defined frequency).
	Expected Deliverables: • Evidence confirming the periodic review of cybersecurity requirements within the organization's OT/ICS project management. • A proof that shows the key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically (based on defined frequency).

1-5	**Cybersecurity in Change Management**
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	
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.
	Related cybersecurity tools: • Template for Cybersecurity Operational Technology Policy

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

- Template for OT/ICS Security Standard

Controls implementation guidelines:

- Define, document and approve cybersecurity requirements within the organization's OT/ICS change management.

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

Expected Deliverables:

- Defined and approved cybersecurity requirements within the organization's OT/ICS change management.

</td></tr>
<tr><td>1-5-2</td><td>Cybersecurity requirements within the organization’s OT/ICS change management lifecycle must be implemented.</td></tr>
<tr><td></td><td>

Related cybersecurity tools:

- Template for Cybersecurity Operational Technology Policy
- Template for OT/ICS Security Standard

Controls implementation guidelines:

- Implement the documented and approved cybersecurity requirements within the organization’s OT/ICS change management.
- Verify and ensure that every change in the OT/ICS area is conducted in line with the defined cybersecurity requirements.

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

Expected Deliverables:

- A proof that the defined cybersecurity requirements within the organization’s OT/ICS change management are implemented.

</td></tr>
<tr><td>1-5-3</td><td>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.</td></tr>
<tr><td></td><td>

Related Cybersecurity Tools:

- Template for Cybersecurity Operational Technology Policy
- Template for OT/ICS Security Standard
- Template for Cybersecurity requirements checklist on IT and change management projects

Controls implementation guidelines:

- Develop and approve a procedure containing cybersecurity requirements in the change management lifecycle.
- Implement the approved procedure for any change within the OT/ICS environments.

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

Expected Deliverables:

- A documented and approved procedure containing cybersecurity requirements in the change management lifecycle.
- A proof that the defined procedure is implemented for any change within the OT/ICS environments.

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

	1-5-3-2	Changes are validated in a separate environment prior to implementing the changes on the production environment.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard **Controls implementation guidelines:** • Prepare a dedicated and separated environment to validate changes before implementation (e.g. lab environment or test-bed). • Verify and ensure that all changes are validated within the dedicated and separated environment.	
	Expected Deliverables: • Site visit to the dedicated and separated environment. • A proof that all changes are validated before implementing on the production environment by documenting the validation results.	
	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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard **Controls implementation guidelines:** • Prepare a checklist containing set of cybersecurity requirements related to OT/ICS to verify their efficiency when replaced with similar devices, for example: configuration of group policy, patches updates, and anti-virus version and configurations. • Verify all new devices against the defined checklist.	
	Expected Deliverables: • The documented checklist containing set of cybersecurity requirements related to OT/ICS to verify their efficiency when replaced with similar devices. • A proof that all new devices replaced within the OT/ICS environments were validated using the defined checklist.	
	1-5-3-4	Restricted processes for exceptional changes must be implemented.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard **Controls implementation guidelines:** • Define a procedure for approving emergency changes related to cybersecurity within OT/ICS environments.	

<table>
<tr><td></td><td>
Ensure that the defined procedure is implemented.
Expected Deliverables:
Documented procedure for approving emergency changes related to cybersecurity within OT/ICS environments.
A proof that the defined procedure is implemented.
<table>
<tr><td>1-5-3-5</td><td>Automated configuration and asset change detection mechanisms must be implemented.</td></tr>
</table>
Related Cybersecurity Tools:
Template for Cybersecurity Operational Technology Policy
Template for OT/ICS Security Standard
Controls implementation guidelines:
Implement an automated configuration and asset change detection solution.
Ensure that the solution is configured properly and cover all OT/ICS assets.
Expected Deliverables:
Site visit to check the automated configuration and asset change detection solution.
A proof that the solution is configured properly and cover all OT/ICS assets.
</td></tr>
<tr><td>1-5-4</td><td>
Cybersecurity requirements within the organization's OT/ICS change management requirements must be reviewed, and their implementation effectiveness is measured and evaluated periodically.
Related Cybersecurity Tools:
Template for Cybersecurity Operational Technology Policy
Template for OT/ICS Security Standard
Template for Key Performance Indicator Report
Controls implementation guidelines:
Review the cybersecurity requirements within the organization's OT/ICS change management requirements based on a documented and approved review plan and on a defined frequency (e.g., conduct a review annually).
Develop key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically (e.g., conduct a periodical review every year).
Expected Deliverables:
Evidence confirming the periodic review of cybersecurity requirements from change management related to OT/ICS.
A proof that shows the key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically (based on defined frequency).
</td></tr>
</table>

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	
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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cybersecurity Auditing Procedure • Template for Cybersecurity Audit Plan Record **Controls implementation guidelines:** • Review the implementation of (OTCC-1:2022) controls at least annually. • Ensure that the results are documented and shared with relevant functions within the organization.
	Expected Deliverables: • The reports for the review of the implementation of (OTCC-1:2022) controls. • A proof that the results have been shared with relevant functions within the organization.
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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cybersecurity Auditing Procedure • Cybersecurity Audit Report Template **Controls implementation guidelines:** • Review the implementation of (OTCC-1:2022) controls at least once every three years by independent parties of the Cybersecurity Organization such as internal audit, or by third parties. • Ensure that the results are documented and shared with relevant functions within the organization and to follow up on the observed notes until they are addressed.
	Expected Deliverables: • The reports for the review of the implementation of (OTCC-1:2022) controls conducted by independent parties of the Cybersecurity Organization such as internal audit, or by third parties. • A proof that the results have been shared with relevant functions within the organization and to follow up on the observed notes until they are addressed.

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	
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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cybersecurity Human Resources Policy **Controls implementation guidelines:** • Identify list of individuals who has access or can utilize the OT/ICS assets (including employees, contractors and subcontractors). • Ensure that screenings or vetting is conducted for the identified list.
	Expected Deliverables: • The identified list of individuals of who has access or can utilize the OT/ICS assets (including employees, contractors and subcontractors). • A proof that the screenings or vetting is conducted for the identified list.
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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cybersecurity Human Resources Policy • Template for Key Performance Indicator Report **Controls implementation guidelines:** • Regularly review the cybersecurity requirements for OT/ICS relate to human resources according to a documented and approved review plan based on a specific timeframe (e.g., conducting annual reviews). • Develop key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically (e.g., conducting annual reviews).

	Expected Deliverables: • Evidence confirming the periodic review of cybersecurity requirements for OT/ICS related to human resources. • A proof that shows the key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically (based on defined frequency).

1-8	Cybersecurity Awareness and Training Program	
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		
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.	
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cybersecurity Awareness Program **Controls implementation guidelines:** • Include awareness topics about a secure and safe interaction with the OT/ICS assets or systems as part of the cybersecurity awareness program. • Ensure that the awareness topics related to the secure and safe interaction with the OT/ICS assets or systems are implemented.	
	Expected Deliverables: • The approved cybersecurity awareness program showcasing the topics related to the secure and safe interaction with the OT/ICS assets or systems. • A proof that the awareness topics related to the secure and safe interaction with the OT/ICS assets or systems are implemented.	
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).
	Related Cybersecurity Tools:	

		• Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cybersecurity Awareness Program **Controls implementation guidelines:** • Identify a list with all personnel names with access to the OT/ICS. • Prepare and document customized training, qualifications, knowledge, and professional skillsets for all identified personnel. • Conduct customized training, qualifications, knowledge, and professional skillsets for all identified personnel.
		Expected Deliverables: • Documented and approved customized training, qualifications, knowledge, and professional skillsets for OT/ICS personnel. • A proof that all personnel with access to the OT/ICS assets completed prepared trainings, qualifications, and professional skillsets.
	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.
		Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard **Controls implementation guidelines:** • Employees, who manage the OT/ICS systems shall participate in OT/ICS authorized and/or specialized organizations and groups, including but not limited to (CySec conference, Dragos Industrial Security Conference).
		Expected Deliverables: • A proof that employees, who manage the OT/ICS systems participated in OT/ICS authorized and/or specialized organizations and groups, including but not limited to (CySec conference, Dragos Industrial Security Conference).

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		
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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Asset Management Policy • Template for Asset Management Standard **Controls implementation guidelines:** • Develop, document and approve the OT/ICS assets inventory in electronic format (e.g. Excel sheet is accepted as a minimum). • Develop a periodic review plan (based on a defined frequency). • Review and update OT/ICS asset inventory periodically (based on a defined frequency). The asset inventory must show the name of the reviewer and the date of the review.	
	Expected Deliverables: • An OT/ICS assets inventory in electronic format showing all OT/ICS assets are inventoried. • A proof that the OT/ICS asset inventory are reviewed periodically (based on a defined frequency).	
	2-1-1-2	Automated solution to collect asset inventory information must be utilized.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Asset Management Policy • Template for Asset Management Standard **Controls implementation guidelines:** • Deploy an automated solution to collect OT/ICS asset inventory information (e.g. dedicated OT/ICS asset scanners). • Verify and ensure that implemented solution does not impact the process and operational continuity.	

	Expected Deliverables: • A periodically generated OT/ICS assets inventory report (based on a defined frequency). • A proof of the provision of OT/ICS asset's automation solutions. • A proof that the OT/ICS assets inventory solution is implemented and does not impact the process.	
	2-1-1-3	OT/ICS asset inventory must be stored securely.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Asset Management Policy • Template for Asset Management Standard **Controls implementation guidelines:** • Ensure compliance with identity and access management procedures for automation systems and technologies. • Ensure that both the access to automated solution and the OT/ICS Asset inventory in electronic format are protected by password and only authorized personnel can access the data.	
	Expected Deliverables: • A Proof showing the compliance with identity and access management procedures for automation systems and technologies. • A Proof showing the OT/ICS asset inventory is protected by password.	
	2-1-1-4	Asset owners for all OT/ICS assets must be identified and involved throughout the relevant asset inventory management lifecycle.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Asset Management Policy • Template for Asset Management Standard **Controls implementation guidelines:** • Identify and document all asset owners for all OT/ICS assets. Prepare a formalized register of OT/ICS assets and their owners. • Verify and ensure that the asset owners and custodian are involved throughout the relevant asset inventory management lifecycle).	
	Expected Deliverables: • A proof that shows the identified asset owners for all OT/ICS assets in asset register/asset inventory. • A proof that highlights the involvement of asset owners throughout the OT/ICS asset inventory management lifecycle.	
	2-1-1-5	Criticality rating for all assets must be assigned, documented, and approved by asset owners.

	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Asset Management Policy • Template for Asset Management Standard Including Classification Guidelines **Controls implementation guidelines:** • Define principles and rules for the mechanism of classifying assets criticality ratings. • Define and document the criticality ranting for all OT/ICS assets based on the defined rules and principles. • Verify and ensure that criticality rating is approved by the relevant asset owner.
	Expected Deliverables: • A proof that shows the approved criticality rating for all assets by asset owners. • A documented proof that shows the assigned criticality rating for all assets in asset register/asset inventory.
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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Asset Management Policy • Template for Key Performance Indicator Report **Controls implementation guidelines:** • Review the cybersecurity requirements for managing OT/ICS assets periodically based on a documented and approved review plan and on a defined frequency (e.g., conduct a review annually). • Develop key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically based on a defined frequency (e.g., conduct an annual review).
	Expected Deliverables: • A proof of conducting periodical reviews for cybersecurity requirements related to OT/ICS asset management. • A proof that shows the key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically (based on a defined frequency).

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		
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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Identity and Access Management Policy • Template for Identity and Access Management Standard **Controls implementation guidelines:** • Develop an identity and access management process, which include its lifecycle (creating new user, renewing existing user, and removing existing user) for OT/ICS. • Verify and ensure that developed OT/ICS identity and access management lifecycle is separated and independent from the Information Technology (IT).	
	Expected Deliverables: • Documented identity and access management lifecycle process for OT/ICS. • A site visit to check the (Active Directory Domain) for OT/ICS separation and independence from Information Technology (IT) (Active Directory Domain).	
	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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Identity and Access Management Policy • Template for Identity and Access Management Standard **Controls implementation guidelines:** • Define a service account management procedure in coordination with the vendor for OT/ICS services, applications, systems, and devices that are separated and disconnected from interactive users account logins, where they are managed securely. • Ensure that all listed accounts are managed in line with defined procedure.	
	Expected Deliverables:	

	• A service accounts for OT/ICS systems list. • A service account management procedure. • Site visit to check all service accounts that they are managed in line with defined cybersecurity requirements and procedure.
2-2-1-3	Default credentials for all OT/ICS assets must be changed, disabled, or removed.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Identity and Access Management Policy • Template for Identity and Access Management Standard **Controls implementation guidelines:** • Ensure the default credentials for all OT/ICS assets have been changed, disabled, or removed in coordination with the vendor.
	Expected Deliverables: • A proof from the vendor showing that all OT/ICS default credentials have been changed, disabled, or removed. • Site visit to check the OT/ICS accounts and ensure the default credentials disabled, change, or removed
2-2-1-4	Sessions must be managed securely, including session authenticity, session lockout, and session timeout termination.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Identity and Access Management Policy • Template for Identity and Access Management Standard **Controls implementation guidelines:** • Define sessions management procedures in coordination with vendor to manage the sessions securely. This includes session authenticity, session lockout, and session timeout termination for windows servers and windows desktop. • Ensure the implementation of the defined procedures for sessions management. This includes session authenticity, session lockout, and session timeout termination for windows servers and windows desktop.
	Expected Deliverables: • A documented sessions management procedures. • Site visit to check the sessions policy including session authenticity, session lockout, and session timeout termination for windows servers and windows desktop.

	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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Identity and Access Management Policy • Template for Identity and Access Management Standard **Controls implementation guidelines:** • Ensure that accounts related to engineers and operators don't have the ability to uninstall programs. • Define a specific user account for each individual (System Admin or Engineers). For example: (The individual must have a specific user name and password when he/she wants to use the engineering workstation). This includes setting the correct privileges for each user.	
	Expected Deliverables: • Site visit to check the privileges of both engineers and operators. • Site visit to ensure the administrator accounts are created for individuals.	
	2-2-1-6	Dual approval and explicit privilege escalation mechanisms for sensitive actions within the OT/ICS environment must be employed.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Identity and Access Management Policy • Template for Identity and Access Management Standard **Controls implementation guidelines:** • Define and formally document sensitive procedures within the OT/ICS environment. • Implement dual approval and explicit privilege escalation mechanisms for documented actions.	
	Expected Deliverables: • A documented sensitive procedure within the OT/ICS environment. • A proof that dual approval and explicit privilege escalation mechanisms for sensitive actions within the OT/ICS environment are used/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.
	Related Cybersecurity Tools:	

- Template for Cybersecurity Operational Technology Policy
- Template for OT/ICS Security Standard
- Template for Identity and Access Management Policy
- Template for Identity and Access Management Standard

Controls implementation guidelines:

- Define, document and approve cybersecurity requirements and rules regarding the remote access to the OT/ICS networks.
- Prepare the risk assessment and risk monitoring procedure for remote access to the OT/ICS networks.
- Implement the solution with trusted multi-factor authenticated and encrypted channel for OT/ICS remote access (e.g. secure remote access tool).
- Monitor and record remote access sessions while its time duration and granted user's privilege must be in accordance with the cybersecurity risk assessment.

Expected Deliverables:

- A documented cybersecurity requirements and rules regarding the remote access to the OT/ICS networks.
- Risk assessment procedure.
- Risk assessment reports.
- A proof that the OT/ICS remote access solution with trusted multi-factor authenticated and encrypted channel is implemented.
- Monitoring and recording reports regarding the remote sessions.

2-2-1-8	Secure and complex password standards must be implemented.

Related Cybersecurity Tools:

- Template for Cybersecurity Operational Technology Policy
- Template for OT/ICS Security Standard
- Template for Identity and Access Management Policy
- Template for Identity and Access Management Standards, encompassing password management

Controls implementation guidelines:

- Define, document and approve secure and complex password standards.
- Implement approved password standards on OT/ICS.

Expected Deliverables:

- Document on password management standard
- Site visit to ensure that the passwords standards are implemented within local or group policy.

2-2-1-9	Secure mechanisms to store OT/ICS assets' passwords must be used.

Related Cybersecurity Tools:

- Template for Cybersecurity Operational Technology Policy

- Template for OT/ICS Security Standard
- Template for Identity and Access Management Policy
- Template for Identity and Access Management Standard

Controls implementation guidelines:

- Define and document OT/ICS assets' passwords storing procedure.
- Implement the secure mechanisms to store OT/ICS assets' passwords (e.g. secure password manager).
- Verify and ensure that all OT/ICS assets' passwords are stored in line with documented procedures and by secure mechanisms.
- Ensure emergency account are stored in line with documented procedures and by secure mechanisms.

Expected Deliverables:

- Documented OT/ICS assets' passwords storing procedures.
- Site visit to check the OT/ICS assets' passwords and emergency account are stored in line with approved procedures by secure mechanisms.

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.

Related Cybersecurity Tools:

- Template for Cybersecurity Operational Technology Policy
- Template for OT/ICS Security Standard
- Template for Identity and Access Management Policy
- Template for Identity and Access Management Standard

Controls implementation guidelines:

- Develop an approved procedure document and an action plan for periodic review of users' identities and access rights in case of cybersecurity incidents, personnel roles changes, or whenever there is a change in OT/ICS system architecture.
- Verify and ensure the implementation of the periodic review plan for user identities and access rights, especially when responding to cybersecurity incidents, personnel role changes, or any changes in the architecture structure of OT/ICS.

Expected Deliverables:

- Procedures and action plan for periodic review of users' identities and access rights.
- Proof that showcase the implementation of the periodic review plan for user identities and access rights, especially when responding to cybersecurity incidents, personnel role changes, or any changes in the architecture structure of OT/ICS.

2-2-1-11	Access shall be immediately revoked when no longer needed.

Related Cybersecurity Tools:

- Template for Cybersecurity Operational Technology Policy

	• Template for OT/ICS Security Standard • Template for Identity and Access Management Policy • Template for Identity and Access Management Standard **Controls implementation guidelines:** • Revoke access permissions for all user upon completion. • Verify and ensure that every access that is no longer needed is revoked.
	Expected Deliverables: • Document the requirements of the control in the OT/ICS identity and access management policy. • A proof that every access that is no longer needed is immediately revoked.
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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Identity and Access Management Policy • Template for Identity and Access Management Standard • Template for Key Performance Indicator Report **Controls implementation guidelines:** • Review the cybersecurity requirements for identity and access management within the OT/ICS environment periodically based on a documented and approved review plan and on a defined frequency (e.g., conduct a review annually). • Develop key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically (based on defined frequency).
	Expected Deliverables: • Proof that showcase the implementation of the periodic review for cybersecurity requirements related to identity and access management within the environment of OT/ICS. • A proof that shows the key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically (based on a defined frequency).

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	

<table>
<tr><td rowspan="6">2-3-1</td><td colspan="2">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:</td></tr>
<tr><td>2-3-1-1</td><td>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.</td></tr>
<tr><td colspan="2">Related Cybersecurity Tools:
Template for Cybersecurity Operational Technology Policy
Template for OT/ICS Security Standard
Template for Malware Protection Standards
Template for Server Security Standard
Template for Advanced Persistent Threat (APT) Protection Standard
Controls implementation guidelines:
Implement advanced protection mechanisms (solution) to block and protect from malware, Advanced Persistent Threats (APT), malicious files, and activities.
Implement the newest version of solutions, updates or signatures and periodically review the mechanisms.
Ensure that the solution is managed to block and protect from malware. This includes the periodic updates (based on a defined frequency), and enabling the schedule scan, in addition to saving the logs for at least 3 months.</td></tr>
<tr><td colspan="2">Expected Deliverables:
Site visit to check the following:
The implemented advanced protection mechanisms (solution).
The coverage of solution (Must cover all OT/ICS assets).
The solution, signatures, and its database version.
The schedule scanning.
The logs of scanning for all endpoints.</td></tr>
<tr><td>2-3-1-2</td><td>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.</td></tr>
<tr><td colspan="2">Related Cybersecurity Tools:
Template for Cybersecurity Operational Technology Policy
Template for OT/ICS Security Standard
Template for Secure Configuration and Hardening Standard
Controls implementation guidelines:
Develop a checklist to review and assess the security configurations' and hardening of OT/ICS systems.
The checklist must be aligned with vendor implementation guidance or recommendations (Vendor Security Baselines).</td></tr>
<tr><td colspan="2">Expected Deliverables:</td></tr>
</table>

	• A documented periodic security configurations' review and hardening procedure. • A proof that security configurations' review and hardening are periodically conducted in alignment with vendor implementation guidance or recommendations.
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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Patch and Update Management Policy • Template for Patch and Update Management Standard **Controls implementation guidelines:** • Obtain a confirmation of the latest approved patches from the vendor in order to align with the applied security patches. • Define, document, and approve the periodic security patches and upgrades implementation procedure in line with the gathered guidance or recommendations with respect to cybersecurity and the organization's formal change management mechanisms. • Implement and verify the approved periodic security patches and updates by the vendor. • Ensure that periodic security patches and updates comply with the change management procedure followed in the organization.
	Expected Deliverables: • A document of the periodic security patches and updates implementation procedure. • Site visit to check the patches and updates implementation. • The confirmation of the latest approved patches and updates from the vendor. • The change request related to the implementation of updates and security patches.
2-3-1-4	Principles of least privilege and least functionality must be applied.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard **Controls implementation guidelines:** • Define roles and responsibilities within the organization and document least privileges and least functionalities for all defined roles. • Implement principles of least privilege and least functionality (e.g. by Privileged Access Management tool). • Verify and ensure that all OT/ICS are embraced by the least privilege and least functionality principles.
	Expected Deliverables:

	• A documented least privileges and least functionalities for all roles defined within the organization. • Site visit to check the implemented least privileges and least functionalities.	
	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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard **Controls implementation guidelines:** • Ensure that Safety Instrumented Systems (SIS) controllers are configured in appropriate modes at all times. • Define a procedure in case there is a need to change the Safety Instrumented Systems (SIS) controllers to improper modes. • Ensure that changes to improper modes occurs only in exceptional circumstances with a specific period of time.	
	Expected Deliverables: • Site visit to check the Safety Instrumented Systems (SIS) controllers that they are in appropriate modes. • A documented list of non-exceptional cases in case of the need to change the control units of Safety Instrumented Systems (SIS) to improper modes.	
	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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard **Controls implementation guidelines:** • Ensure that the application whitelisting techniques or other similar techniques are utilized to limit the applications that are allowed to run in OT/ICS environment.	
	Expected Deliverables: • Site visit to check the application whitelisting techniques or other similar techniques that are implemented.	
	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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard **Controls implementation guidelines:** • Verify and ensure that all Engineering Workstation (EWS) and Human-Machine Interface (HMI) for management and maintenance purposes are dedicated and segmented.	

	• Verify and ensure that all Engineering Workstation (EWS) and Human-Machine Interface (HMI) for management and maintenance purposes are hardened in line with approved requirements and principles.
	Expected Deliverables: • Site visit to check all OT/ICS assets are managed through dedicated, segmented and hardened Engineering Workstations (EWS) and Human-Machine Interfaces (HMI).
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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Storage Media Security Policy **Controls implementation guidelines:** • Develop an isolated and secure environment for external storage media scanning. • Identify, document, and implement the scanning procedure. • Verify and ensure that all external storage media are scanned and analyzed against malware and APT.
	Expected Deliverables: • A documented external storage media scanning procedure. • Proof that shows all external storage media are scanned and analyzed against malware and APT.
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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard **Controls implementation guidelines:** • Restrict usage of external storage media in the production environment to avoid unauthorized access and unexpected influence on the process. • Develop and implement secure mechanisms and procedure for data transfer in the production environment (e.g. dedicated file servers, USBs, and hard disks used exclusively for the facility).
	Expected Deliverables: • A procedure document for data transfer in the production environment. • Site visit to check the usage of external storage media in the production environment is restricted.
2-3-1-10	Systems' logs and critical files must be protected from unauthorized access, tampering, illegitimate modification and/or deletion.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy

	• Template for OT/ICS Security Standard **Controls implementation guidelines:** • Ensure that all system and security logs are enabled. • Ensure systems' logs and critical files are protected from unauthorized access and tampering by enabling session lockout and session timeout on the workstation as well as creating individual users with set of privileges.	
	Expected Deliverables: • Site visit to check the following: ○ System and security logs. ○ Session management. ○ List of accounts.	
	2-3-1-11	Unauthorized applications, scripts, tasks, and changes must be detected and analyzed.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard **Controls implementation guidelines:** • Ensure that the logs of unauthorized applications, scripts, tasks, and changes are detected and forwarded to the SIEM solution or log collector, then sent to the Security Operation Center (SOC) to be analyzed.	
	Expected Deliverables: • A proof that the logs of unauthorized applications, scripts, tasks, and changes are detected. • OT/ICS use-cases list by the Security Operation Center (SOC).	
	2-3-1-12	New communications sessions and commands execution must be detected and analyzed.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard **Controls implementation guidelines:** • Implement techniques and tools to detect executed commands and new communication sessions (e.g. network traffic monitoring tools or intrusion detection system). • Ensure that the logs of new communication sessions and commands execution are detected and forwarded to the SIEM solution, then sent to the Security Operation Center (SOC) to be analyzed.	
	Expected Deliverables: • A proof that the logs of new communication sessions and commands execution are detected. • OT/ICS use-cases list by Security Operation Center (SOC).	
	2-3-1-13	Direct communications between the OT/ICS environment and external hosts must be detected and analyzed.

	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard **Controls implementation guidelines:** • Implement network traffic analysis tool between OT/ICS and external hosts (e.g. network traffic monitoring tools). • Ensure that the logs of direct communications between the OT/ICS environment and external hosts are detected and forwarded to the SIEM solution, then sent to the Security Operation Center (SOC) to be analyzed.
	Expected Deliverables: • A proof that the logs of new communications sessions and commands execution are detected. • OT/ICS use-cases list by Security Operation Center (SOC).
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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Key Performance Indicator Report **Controls implementation guidelines:** • Review the cybersecurity requirements for system and processing facilities protection in OT/ICS environment periodically based on a documented and approved review plan and on a defined frequency (e.g., conduct a review annually). • Develop key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically based on a defined frequency (e.g., conduct an annual review).
	Expected Deliverables: • A proof that shows the periodic review of cybersecurity requirements to protect systems and processing facilities related to OT/ICS. • A proof that shows the key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically based on a defined frequency.

2-4	Network Security Management	
Objective	To ensure the protection of the organization's OT/ICS networks from cyber risks.	
Controls		
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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Data Diode Standard • Template for Network Security Policy • Template for Network Security Standard **Controls implementation guidelines:** • Implement logical or physical OT/ICS segmentation from other networks (e.g., VLANs, next-generation firewalls, Data diode). • Verify and ensure that assets in the OT/ICS environment are not reachable from other environments or networks.	
	Expected Deliverables: • Network diagrams confirming the segmentation. • Site visit to check the logical or physical segmentation of OT/ICS networks from other 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".
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Network Security Policy • Template for Network Security Standard **Controls implementation guidelines:** • Ensure that the diagrams show the high level architecture including the zones within the OT/ICS environment, and the connection between the IT corporate network and the OT/ICS network. • Implement logical or physical OT/ICS segmentation between OT/ICS zones using e.g. VLANs and next-generation firewalls.	
	Expected Deliverables: • Network diagrams illustrating the segmentation.	

	• Site visit to check that all OT/ICS zones are segmented logically or physically from other environments or networks and that the traffic directs to "Choke Points".
2-4-1-3	Safety Instrumented Systems (SIS) must be segmented logically or physically from other OT/ICS networks.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Network Security Policy • Template for Network Security Standard **Controls implementation guidelines:** • Ensure Safety Instrumented Systems (SIS) are stand-alone and segmented logically or physically from other OT/ICS networks. • Verify and ensure that the network diagram clearly shows the Safety Instrumented Systems (SIS) segmentation.
	Expected Deliverables: • Network diagrams illustrating the segmentation. • Site visit to check that all Safety Instrumented Systems (SIS) are segmented logically or physically.
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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Network Security Policy • Template for Network Security Standard **Controls implementation guidelines:** • Restrict wireless technologies usage (e.g., Wi-Fi, Bluetooth, Cellular, Satellite, etc.). • Define and document the business justifications and requirements for wireless technologies usage. • Define, document, and implement wireless technologies usage requirements and principles. • Verify and ensure that all deployed wireless technologies are in line with documented requirements and principles.
	Expected Deliverables: • The business justifications and requirements for wireless technologies usage. • A document that demonstrates wireless technologies usage requirements and principles. • Site visit to ensure that wireless technologies usage are restricted and in line with documented requirements and principles.

	2-4-1-5	Wireless technologies must be segmented logically or physically from other OT/ICS networks.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Network Security Policy • Template for Network Security Standard **Controls implementation guidelines:** • Identify the list of the wireless technologies used. • Implement logical or physical segmentation between wireless technologies and other OT/ICS networks (e.g. VLANs, next-generation firewalls). • Verify and ensure that wireless technologies do not interact with other environments or networks related to OT/ICS.	
	Expected Deliverables: • List of the wireless technologies used. • Network diagrams illustrating the segmentation. • Site visit to check that all wireless technologies are 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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Network Security Policy • Template for Network Security Standard **Controls implementation guidelines:** • Managing firewall rules to restrict network communications, services, and connection points between different zones and limiting them to the minimum necessary, to meet operational, maintenance, and safety requirements.	
	Expected Deliverables: • Site visit to check that network communications, services, and connection points between different zones are limited to the minimum while meeting 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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard	

	• Data Diode Standard • Template for Network Security Policy • Template for Network Security Standard **Controls implementation guidelines:** • Avoid direct access to authentication services by e.g. disabling services on external-facing hosts. • Verify and ensure that direct exposure of common remote authentication and access management services on all external-facing hosts is prevented.
	Expected Deliverables: • Network diagrams illustrating the segregation and segmentation clearly of OT/ICS environment from other environments.
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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Network Security Policy • Template for Network Security Standard **Controls implementation guidelines:** • Conduct risk assessment to ensure that the risks are monitored and controlled. • Ensure that the obsolete systems are only used for authorized business-critical services with applying compensating controls such as (delete unwanted services, restrict the access to these systems, manage the account to certain list of users).
	Expected Deliverables: • Risk assessment. • Site visit to check that the obsolete systems are only used for authorized business-critical services with applying compensating controls.
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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Data Diode Standard • Template for Network Security Policy • Template for Network Security Standard **Controls implementation guidelines:** • Prevent direct communications between corporate zone and OT/ICS zones.

	• In case there is a need to send data to the corporate zone, direct all the required connections through dedicated, secured, and hardened jump host/solution in the DMZ zone.	
	Expected Deliverables: • Network diagrams confirming that the DMZ zone is utilized. • Site visit to check that all the required connections between corporate zone and OT/ICS zones are going through dedicated, secured, and hardened jump host/solution in the DMZ zone.	
	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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Network Security Policy • Template for Network Security Standard **Controls implementation guidelines:** • Ensure that the remote access point in the DMZ zone is not being connected to the OT/ICS networks unless needed. • Define a procedure in case there is a need to connect to the OT/ICS networks from the DMZ zone through remote access point, the procedure must include at least these requirements: ○ The session is multi-factor authenticated. ○ The session is recorded. ○ The established session has a defined period of time.	
	Expected Deliverables: • Site visit to check that remote access point in the DMZ is not connected to the OT/ICS networks without need. • Approved remote sessions procedure. • A proof that in case remote sessions are needed, they are 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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Data Diode Standard • Template for Network Security Policy • Template for Network Security Standard	

	• Template for Proxy Protection Standard **Controls implementation guidelines:** • Implement proxy solution between the corporate and OT/ICS zones for all machine-to-machine traffic. • Verify and ensure that all machine-to-machine traffic between the corporate and OT/ICS zones is going through the proxy.
	Expected Deliverables: • Site visit to ensure that all machine-to-machine traffic between the corporate and OT/ICS zones is going through the proxy.
	2-4-1-12 — Dedicated gateways must be used to segment OT/ICS networks from corporate zone.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Data Diode Standard • Template for Network Security Policy • Template for Network Security Standard **Controls implementation guidelines:** • Implement dedicated gateway to segment OT/ICS networks from corporate zone.
	Expected Deliverables: • Site visit and network diagram showing that dedicated gateway to segment OT/ICS networks from corporate zone are implemented.
	2-4-1-13 — Dedicated DMZ zone must be used to reside any system that needs services provided by corporate zone.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Data Diode Standard • Template for Network Security Policy • Template for Network Security Standard **Controls implementation guidelines:** • Define and implement a dedicated DMZ zone based on the requirements related to cybersecurity. • Include all systems that provide services between the OT/ICS zone and corporate zone within a dedicated DMZ zone.
	Expected Deliverables: • List of all systems that provide services between the OT/ICS zone and corporate zone. • Site visit to check that the dedicated DMZ zone is utilized, and that is when any of the systems that provide services between the OT/ICS zone and corporate zone is in use.

	2-4-1-14	Strict limitation on enabling/usage of industrial protocols and ports to the minimum to meet operational, maintenance, and safety requirements.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Data Diode Standard • Template for Network Security Policy • Template for Network Security Standard **Controls implementation guidelines:** • Verify and ensure that there is strict limitation on enabling/usage of industrial protocols and ports to meet operational, maintenance, and safety requirements.	
	Expected Deliverables: • Site visit to ensure that there is strict limitation on enabling/usage of industrial protocols and ports 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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Network Security Policy • Template for Network Security Standard • Template for Patch and Update Management Standard **Controls implementation guidelines:** • Ensure all periodic update packages and security patches for assets in the production environment are approved by the vendor • Conduct a test in a testing environment before applying periodic updates and patches for assets in the production environment.	
	Expected Deliverables: • A certification of periodic patches and upgrades from the vendor. • Implemented dedicated and separated test environment. • A proof that all periodic patches and upgrades for production assets are tested in a testing environment.	
	2-4-1-16	Details related to network architecture and topology, zones, network data flows, connectivity, and interdependencies must be documented, updated, and maintained.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Network Security Policy	

	• Template for Network Security Standard **Controls implementation guidelines:** • Document all details related to network architecture and topology, zones, network data flows, connectivity, and interdependencies. • Ensure that network diagrams and documentation is periodically updated.
	Expected Deliverables: • The latest and updated network diagram.
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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Network Security Policy • Template for Key Performance Indicator Report **Controls implementation guidelines:** • Review the cybersecurity requirements for network security management periodically based on a documented and approved review plan and on a defined frequency (e.g., conduct a review annually). • Develop key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically based on a defined frequency (e.g., conduct an annual review).
	Expected Deliverables: • A proof that shows the periodic review of cybersecurity requirements to manage OT/ICS network security. • A proof that shows the key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically (based on defined frequency).

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		
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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Mobile Devices Security Standard **Controls implementation guidelines:** • Restrict usage of mobile devices for OT/ICS to avoid unauthorized access and unexpected influence on the process. • Define and document exceptional cases where usage of mobile devices is required. • Conduct a cybersecurity risk assessment to identify and manage risks in line with the organization's mechanisms. • Define, document, and implement cybersecurity requirements specified for mobile devices usage. • Ensure that all mobile devices used are implementing and in line with the approved documented requirements.	
	Expected Deliverables: • Report of Cybersecurity risk assessment when using mobile devices. • Document for Cybersecurity requirements when using mobile devices. • Site visit to check that usage of mobile devices for OT/ICS is restricted and limited only to defined cases.	
	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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Mobile Devices Security Standard • Template for Security Configuration and Hardening Standard • Template for Advanced Persistent Threat (APT) Protection Standard **Controls implementation guidelines:** • Define and document a hardening and update procedure when using mobile devices dedicated for work purposes. • Verify and ensure that all mobile devices are used only for their intended purposes (e.g. by the mobile devices management tools). • Verify and ensure that all mobile devices are hardened and updated with the latest security patches and scanned against malware and APT.	
	Expected Deliverables:	

	• A documented hardening and update procedure and that is for when using mobile devices dedicated for work purposes. • Site visit to check that all mobile devices are used only for their intended purposes. • Reports illustrating installed security patches for mobile devices • Reports for mobile devices scanning.	
	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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Mobile Devices Security Standard **Controls implementation guidelines:** • Define and formally document a limited and approved list of mobile devices which can be connected to OT/ICS. • Verify and ensure that only listed mobile devices can be connected to OT/ICS environment.	
	Expected Deliverables: • A documented and approved list of mobile devices which can be connected to OT/ICS. • Site visit to check that only listed mobile devices can be connected to the OT/ICS environment.	
	2-5-1-4	Centralized management of mobile devices must be deployed.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Mobile Devices Security Standard **Controls implementation guidelines:** • Deploy a centralized mobile devices management solution. • Verify and ensure that all identified mobile devices are managed by a centralized solution.	
	Expected Deliverables: • A proof that ensures the deployment of a centralized mobile devices management solution. • A proof that all identified mobile devices are managed by a centralized solution.	
	2-5-1-5	Encryptions mechanisms must be used for mobile devices authorized to access the OT/ICS assets.

	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Encryption Standard • Template for Mobile Devices Security Standard **Controls implementation guidelines:** • Define, document, and approve encryption mechanisms on mobile devices authorized to access the OT/ICS assets. The approved mechanisms should be compliant with the organization's regulations. • Verify and ensure that all mobile devices authorized to access the OT/ICS assets have implemented approved encryption mechanisms.
	Expected Deliverables: • A proof that all mobile devices authorized to access the OT/ICS assets have implemented approved encryption mechanisms.
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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Mobile Devices Security Standard • Template for Key Performance Indicator Report s **Controls implementation guidelines:** • Review the cybersecurity requirements for mobile devices security in the OT/ICS environment periodically based on a documented and approved review plan and on a defined frequency (e.g., conduct a review annually). • Develop key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically based on a defined frequency (e.g., conduct an annual review).
	Expected Deliverables: • A proof that shows the periodic review of cybersecurity requirements to secure the mobile devices in the OT/ICS environment. • A proof that shows the key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically (based on defined frequency).

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		
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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Data Cybersecurity Policy • Template for Data Cybersecurity Standard **Controls implementation guidelines:** • Identify and classify electronic and physical data in OT/ICS environment. • Ensure that the physical data (at rest and in transit) are protected by restricting the access to any classified or critical physical data, such as network diagrams, P&ID diagrams, and engineering documents. • Ensure that the electronic data (at rest and in transit) are protected by implementing security controls including but not limited to: (enable session timeout and lockout in engineering workstation, configure the removable media settings).	
	Expected Deliverables: • Site visit to check that electronic and physical data (at rest and in transit) are protected in line with the data classification.	
	2-6-1-2	Data Leakage Prevention (DLP) mechanisms must be used to protect the classified data and information.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Data Loss Prevention Standard • Template for Data Cybersecurity Policy • Template for Data Cybersecurity Standard **Controls implementation guidelines:** • Implement Data Leakage Prevention (DLP) mechanisms in the OT/ICS environment (e.g. data transfer monitoring or data access management tools). • Verify and ensure that data and information are protected by Data Leakage Prevention (DLP) mechanisms.	
	Expected Deliverables:	

	• Site visit to check that classified data and information are protected by Data Leakage Prevention (DLP) mechanisms.	
	2-6-1-3	Secure wiping mechanisms for configuration details and stored data from OT/ICS assets prior to decommissioning must be implemented.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Data Cybersecurity Policy • Template for Data Cybersecurity Standard **Controls implementation guidelines:** • Define and formally document secure wiping procedure for OT/ICS assets. • Verify and ensure that all OT/ICS assets before decommissioning are securely wiped.	
	Expected Deliverables: • A documented secure wiping procedures. • A proof that all OT/ICS assets are securely wiped before decommissioning.	
	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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Data Cybersecurity Policy • Template for Data Cybersecurity Standard **Controls implementation guidelines:** • Limit and verify transfer or usage of OT systems' data in any environment other than the production environment. • Ensure that the transfer or usage of OT systems' data in any environment other than production environment is limited, except after applying strict controls including but not limited to; (scanning the USBs and Hard Disks against Malware and APT, configure the removable media settings to allow a certain list of known USBs, and using secure file server).	
	Expected Deliverables: • Site visit to check that the transfer or usage of OT systems' data in any environment other than production is limited, apart from environments that apply 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.	
	Related Cybersecurity Tools:	

	• Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Data Cybersecurity Policy • Template for Key Performance Indicator Report **Controls implementation guidelines:** • Review the cybersecurity requirements for data and information protection periodically based on a documented and approved review plan and on a defined frequency (e.g., conduct a review annually). • Develop key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically based on a defined frequency (e.g., conduct reviews annually).
	Expected Deliverables: • A proof that shows the periodic review of cybersecurity requirements for data and information protection in the OT/ICS environment. • A proof that shows the key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically based on a defined frequency (e.g., conduct reviews annually).

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	
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).
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cryptography Policy • Template for Cryptography Standard • Template for Key Management Standard **Controls implementation guidelines:** • Identify and document all cryptographic technologies used in OT/ICS environment. • Verify and ensure that cryptographic technologies used in OT/ICS environment are aligned with the NCA National Cryptographic Standard (NCS-1:2020).
	Expected Deliverables: • A documented cryptographic technologies used in OT/ICS environment list.

	• Site visit to check that all cryptographic technologies used in OT/ICS environment are aligned with the NCA National Cryptographic Standard (NCS-1:2020).
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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cryptography Policy • Template for Key Performance Indicator Report **Controls implementation guidelines:** • Review the cybersecurity requirements for cryptography in the OT/ICS environment periodically based on a documented and approved review plan and on a defined frequency (e.g., conduct a review annually). • Develop key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically based on a defined frequency (e.g., conduct a review annually).
	Expected Deliverables: • A proof that shows the periodic review of cybersecurity requirements for cryptography in the OT/ICS environment. • A proof that shows the key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically (based on defined frequency).

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		
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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Backup Policy • Template for Backup Standard **Controls implementation guidelines:**	

	• Verify and ensure that backups for all OT/ICS assets are covered and stored in a centralized and offline locations.	
	Expected Deliverables: • A documented OT/ICS backup plan including its requirements and principles. • A backup scope list of OT/ICS. • Site visit to check that backups for all OT/ICS assets are covered and stored in a 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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Backup Policy • Template for Backup Standard **Controls implementation guidelines:** • Verify and ensure that all OT/ICS assets' critical configuration files and engineering files are included in the backup's scope.	
	Expected Deliverables: • A documented list of OT/ICS assets' critical configuration files and engineering files. • Site visit to check that all OT/ICS assets' critical configuration files and engineering files are 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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Backup Management Policy • Template for Cybersecurity Backup Management Standard **Controls implementation guidelines:** • Verify and ensure that all backups are performed periodically (based on a defined frequency).	
	Expected Deliverables: • A proof that shows all backups are performed periodically as per the defined frequency.	
	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.
	Related Cybersecurity Tools:	

	• Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Backup Policy • Template for Backup Standard **Controls implementation guidelines:** • Define and implement security mechanisms on backup mediums to ensure that the access, storage, and transfer of backups are protected. • Verify and ensure that documented requirements and principles embrace protection against damage, change, or unauthorized access.
	Expected Deliverables: • Site visit to check implemented security mechanisms on backup mediums to ensure that the access, storage, and transfer of backups are protected • Site visit to check that documented requirements and principles embrace 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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Backup Management Policy • Template for Key Performance Indicator Report **Controls implementation guidelines:** • Review the cybersecurity requirements for backup management for OT/ICS periodically based on a documented and approved review plan and on a defined frequency (e.g., conduct a review annually). • Develop key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically (based on defined frequency).
	Expected Deliverables: • A proof that shows the periodic review of cybersecurity requirements for backup and recovery management in the OT/ICS environment. • A proof that shows the key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically (based on a defined frequency).

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		
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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Vulnerability Management Policy • Template for Vulnerability Management Standard • Template for Cybersecurity Vulnerability Management Processes and Procedures, including a template for managing discovered vulnerabilities **Controls implementation guidelines:** • Define, document, and approve vulnerability assessment scope and activities for OT/ICS environment ensuring limited or no impact on the production environment. • Include OT/ICS vulnerability assessment as part of the organization's formal vulnerability management process. • Verify and ensure that all OT/ICS assets are covered by the approved vulnerability assessment process.	
	Expected Deliverables: • A documented OT/ICS vulnerability assessment scope and activities. • A proof that OT/ICS vulnerability assessment is part of the organization's formal vulnerability management.	
	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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Vulnerability Management Policy • Template for Vulnerability Management Standard • Template for Cybersecurity Vulnerability Management Processes and Procedures, including a template for managing discovered vulnerabilities • Template for Vulnerability Register	

	Controls implementation guidelines: • Develop a procedure for the remediation of newly discovered critical vulnerabilities presenting significant risks in a timely manner. • Ensure that the vulnerabilities management procedures are implemented.	
	Expected Deliverables: • Approved vulnerability remediation plan. • A vulnerability remediation report. • A proof that all newly discovered critical vulnerabilities that pose significant risks to the OT/ICS environment are remediated 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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Vulnerability Management Policy • Template for Vulnerability Management Standard • Template for Cybersecurity Vulnerability Management Processes and Procedures, including a template for managing discovered vulnerabilities • Template for Vulnerability Register **Controls implementation guidelines:** • Verify and ensure that vulnerability assessment is conducted periodically in accordance to the facility level stated in (OTCC-1:2022).	
	Expected Deliverables: • Periodically prepared vulnerability assessment reports. • A Proof that vulnerability assessment for OT/ICS systems is conducted periodically in accordance to the facility level stated in (OTCC-1:2022).	
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.	
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Vulnerability Management Policy • Template for Key Performance Indicator Report **Controls implementation guidelines:** • Review the cybersecurity requirements for vulnerability management specific to OT/ICS periodically based on a documented and approved review plan and on a defined frequency (e.g., conduct a review annually).	

	• Develop key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically based on a defined frequency (e.g., conduct a review annually).
	Expected Deliverables: • A proof that shows the periodic review of cybersecurity requirements for vulnerability management in the OT/ICS environment. • A proof that shows the key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically (based on a defined frequency).

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		
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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Penetration Testing Policy • Template for Penetration Testing Standard **Controls implementation guidelines:** • Define the scope of penetration testing activities. • Ensure that the penetration testing activities are conducted by a qualified team.	
	Expected Deliverables: • A proof that penetration testing is conducted for the OT/ICS environment and networks connected to the operational network and that it is conducted by a 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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard	

	• Template for Penetration Testing Policy • Template for Penetration Testing Standard **Controls implementation guidelines:** • Conduct penetration testing with limited or no impact on the production environment, or perform the testing in a separate but identical environment (e.g., testing or training environments).	
	Expected Deliverables: • A proof that penetration testing is conducted with limited or no impact on the production environment, or that it's performed in a separate but identical environment (e.g., testing or training environments).	
	2-10-1-3	With reference to the ECC subcontrol 2-11-3-2, penetration testing for OT/ICS systems must be conducted periodically.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Penetration Testing Policy • Template for Penetration Testing Standard **Controls implementation guidelines:** • Ensure that the penetration testing for OT/ICS systems are conducted periodically in accordance to the facility level stated in (OTCC-1:2022).	
	Expected Deliverables: • A proof that penetration testing for OT/ICS systems is conducted periodically in accordance to the facility level stated in (OTCC-1:2022).	
	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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Penetration Testing Policy • Template for Penetration Testing Standard **Controls implementation guidelines:** • List OT/ICS systems or assets requiring alternative testing methods. • Define, document, and implement alternative testing methods (such as passive testing mechanisms) and that is when a potential impact on the operational production environment may occur. • Implement a proper alternative testing methods (such as Passive Testing) for a specified OT/ICS system or asset in line with the approved procedures. • Verify and ensure that the alternative tests allow for gathering information about assets related to OT/ICS.	

	Expected Deliverables: • Periodically prepared alternative testing methods reports.
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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Penetration Testing Policy • Template for Key Performance Indicator Report **Controls implementation guidelines:** • Review the cybersecurity requirements for penetration testing on OT/ICS periodically based on a documented and approved review plan and on a defined frequency (e.g., conduct a review annually). • Develop key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically based on a defined frequency (e.g., conduct a review annually).
	Expected Deliverables: • A proof that shows the periodic review of cybersecurity requirements for penetration testing on OT/ICS. • A proof that shows the key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically (based on a defined frequency).

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		
2-11-1	In addition to subcontrols in the ECC control 2-12-3, 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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cybersecurity Event Logs and Monitoring Management Policy • Template for Cybersecurity Event Logs and Monitoring Management Standard **Controls implementation guidelines:**	

	• Activate cybersecurity event logs for all assets in the OT/ICS environment (e.g., operators' devices, engineering devices, servers, and network devices).	
	Expected Deliverables: • Cybersecurity event logs and audit trails received by the monitoring system. • Proof that all OT/ICS assets have event logs and audit trails feature activated (e.g., operators' devices, engineering devices, servers, and network devices).	
	2-11-1-2	Failure attempts in accessing the organization's monitoring systems must be detected and logged.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cybersecurity Event Logs and Monitoring Management Policy • Template for Cybersecurity Event Logs and Monitoring Management Standard **Controls implementation guidelines:** • Implement mechanisms to detect and log failure attempts in accessing the organization's monitoring systems (e.g. alerting system in case of unauthorized access). • Ensure that event logs are enabled and forwarded to a SIEM or event log collector, then analyze these events through the Security Operation Center (SOC).	
	Expected Deliverables: • A proof that shows the implementation of mechanisms to detect and log failure attempts in accessing the organization's monitoring systems. • OT/ICS use-cases list by Security Operation Center (SOC).	
	2-11-1-3	Continuous, in-depth cybersecurity log review and monitoring, covering all logs and audit trails must be conducted.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cybersecurity Event Logs and Monitoring Management Policy • Template for Cybersecurity Event Logs and Monitoring Management Standard **Controls implementation guidelines:** • Ensure that the continuous, in-depth cybersecurity log review and monitoring, covering all logs and audit trails are conducted through SOC capabilities. • Ensure that event logs are enabled and forwarded to a SIEM or event log collector, then analyze these events through the Security Operation Center (SOC).	
	Expected Deliverables: • Site visit to the Security Operation Center (SOC).	

	• OT/ICS use-cases list by Security Operation Center (SOC).
2-11-1-4	Monitoring, detecting, and analyzing User Behaviors Analytics (UBA) must be performed.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cybersecurity Event Logs and Monitoring Management Policy • Template for Cybersecurity Event Logs and Monitoring Management Standard **Controls implementation guidelines:** • Define and implement monitoring, detection, and analysis of User Behaviors Analytics mechanisms. • Verify and ensure that all users are covered by monitoring, detection, and analyses of User Behaviors Analytics mechanisms. • Ensure that event logs are enabled and forwarded to a SIEM or event log collector, then analyze these events through the Security Operation Center (SOC).
	Expected Deliverables: • A proof that monitoring, detection, and analysis of User Behaviors Analytics are performed.
2-11-1-5	Upload or download activities of OT/ICS assets including Safety Instrumented Systems (SIS) must be detected.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cybersecurity Event Logs and Monitoring Management Policy • Template for Cybersecurity Event Logs and Monitoring Management Standard **Controls implementation guidelines:** • Identify and list all OT/ICS assets including Safety Instrumented Systems (SIS). • Define and implement detection mechanisms for upload or download activities on the listed OT/ICS assets including Safety Instrumented Systems (SIS). • Verify and ensure that all upload or download activities on the OT/ICS including Safety Instrumented Systems (SIS) assets are detected.
	Expected Deliverables: • Site visit to check that all upload or download activities on the OT/ICS including Safety Instrumented Systems (SIS) assets are detected.
2-11-1-6	All remote access sessions must be monitored.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard

		• Template for Cybersecurity Event Logs and Monitoring Management Policy • Template for Cybersecurity Event Logs and Monitoring Management Standard **Controls implementation guidelines:** • Ensure that all remote access sessions are monitored. • Ensure that event logs are enabled and forwarded to a SIEM or event log collector, then analyze these events through the Security Operation Center (SOC).
		Expected Deliverables: • A proof that all remote access sessions are monitored. • OT/ICS use-cases list by Security Operation Center (SOC).
	2-11-1-7	Malicious events must be detected and analyzed.
		Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cybersecurity Event Logs and Monitoring Management Policy • Template for Cybersecurity Event Logs and Monitoring Management Standard **Controls implementation guidelines:** • Ensure that the anti-virus scan schedule is enabled and performed periodically. • Ensure that the malicious events are detected and analyzed through SOC capabilities. • Ensure that event logs are enabled and forwarded to a SIEM or event log collector, then analyze these events through the Security Operation Center (SOC).
		Expected Deliverables: • A proof confirming the detection and analysis of malicious events.
	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.
		Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cybersecurity Event Logs and Monitoring Management Policy • Template for Cybersecurity Event Logs and Monitoring Management Standard **Controls implementation guidelines:** • Ensure that the logging and monitoring of new alerts when new or unauthorized devices are connected to the OT/ICS networks are performed through SOC capabilities. • Ensure that event logs are enabled and forwarded to a SIEM or event log collector, then analyze these events through the Security Operation Center (SOC).
		Expected Deliverables: • A proof that shows logging and monitoring mechanisms of new or unauthorized OT/ICS device alerts.

	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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cybersecurity Event Logs and Monitoring Management Policy • Template for Cybersecurity Event Logs and Monitoring Management Standard **Controls implementation guidelines:** • Verify and ensure that the OT/ICS Threat Intelligence is used and incorporated to regularly tune and refresh alerts of Security Information and Event Management (SIEM) technologies.	
	Expected Deliverables: • A proof that the OT/ICS Threat Intelligence is used and incorporated to regularly tune and refresh alerts of SIEM technologies.	
	2-11-1-10	All access control points between the network security boundaries and external connections must be monitored.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cybersecurity Event Logs and Monitoring Management Policy • Template for Cybersecurity Event Logs and Monitoring Management Standard **Controls implementation guidelines:** • Ensure that the access control points between the network security boundaries and external connections are monitored. • Ensure that event logs are enabled and forwarded to a SIEM or event log collector, then analyze these events through the Security Operation Center (SOC).	
	Expected Deliverables: • A proof that all access control points between the network security boundaries and external connections are monitored.	
2-11-2	With reference to the ECC control 2-12-4, 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.	
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cybersecurity Event Logs and Monitoring Management Policy • Template for Key Performance Indicator Report **Controls implementation guidelines:**	

	• Review the cybersecurity requirements for cybersecurity event logs and monitoring management specified to the OT/ICS periodically based on a documented and approved review plan and on a defined frequency (e.g., conduct a review annually). • Develop key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically based on a defined frequency (e.g., conduct a review annually).
	Expected Deliverables: • A proof that shows the periodic review of cybersecurity requirements for OT/ICS event logs and monitoring management. • A proof that shows the key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically (based on a defined frequency).

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		
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).
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cybersecurity Incident and Threat Management Policy • Template for Cybersecurity Incident and Threat Management Standard • Guideline for Cybersecurity Incident Response • Templates for Cybersecurity Incident Response Detailed Plan **Controls implementation guidelines:** • Define, document, and approve OT/ICS cybersecurity incident response plans. Approved plans should be formally documented (e.g. as a procedure) based on existing and globally available standards. • Include approved OT/ICS cybersecurity incident response plans into the general organizational plans and its procedures. • Verify and ensure that OT/ICS cybersecurity incident response plans are integrated and aligned with other organizational plans and procedures.	

	Expected Deliverables: • Documented OT/ICS cybersecurity incident response plans. • A proof that shows the approved OT/ICS cybersecurity incident response plans are integrated and aligned with organizational plans and its procedures.	
	2-12-1-2	Formal incident response and root cause analysis for any detected cybersecurity incidents must be conducted.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cybersecurity Incident and Threat Management Policy • Template for Cybersecurity Incident and Threat Management Standard • Guideline for Cybersecurity Incident Response • Templates for Cybersecurity Incident Response Detailed Plan **Controls implementation guidelines:** • Define and formally document a root cause analysis procedure and methodologies in case of any detected cybersecurity incidents. • Implement developed OT/ICS cybersecurity incident response plans and handle the incidents according to the stages specified in the plan. • Conduct defined incident analysis and root cause analysis in case of cybersecurity incident detection.	
	Expected Deliverables: • A documented root cause analysis procedure and methodologies. • Prepared incident response and root cause analysis reports. • A proof that the incident response and root cause analysis is conducted for all detected cybersecurity incidents.	
	2-12-1-3	Sequence of incident response activities necessary to restore normal operations must be defined.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cybersecurity Incident and Threat Management Policy • Template for Cybersecurity Incident and Threat Management Standard • Guideline for Cybersecurity Incident Response • Templates for Cybersecurity Incident Response Detailed Plan **Controls implementation guidelines:** • Define, document, and approve the sequence of incident response activities necessary to restore normal operations, and approved activities should be formally documented (e.g. as an activity plan or procedure).	

- Define and formally document operations restoration action plan. Containing a detailed step-by-step description and a manual.
- Verify and ensure that in case of an operations breach the restoration plan is performed.

Expected Deliverables:

- A documented and approved sequence of incident response activities necessary to restore normal operations.
- A documented restoration action plan when encountering a cybersecurity incident.
- A proof that ensures the restoration of normal operations when encountering a cybersecurity incident.

2-12-1-4	Incident communications plan must be established.

Related Cybersecurity Tools:

- Template for Cybersecurity Operational Technology Policy
- Template for OT/ICS Security Standard
- Template for Cybersecurity Incident and Threat Management Policy
- Template for Cybersecurity Incident and Threat Management Standard
- Guideline for Cybersecurity Incident Response
- Templates for Cybersecurity Incident Response Detailed Plan

Controls implementation guidelines:

- Define and formally document an incident communications plan in case of incidents.
- Verify and ensure that the incident communications plan is implemented if an incident occurred.

Expected Deliverables:

- A documented incident communication plan.
- A proof that the incident communications plan is implemented in case of incidents.

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.

Related Cybersecurity Tools:

- Template for Cybersecurity Operational Technology Policy
- Template for OT/ICS Security Standard
- Template for Cybersecurity Incident and Threat Management Policy
- Template for Cybersecurity Incident and Threat Management Standard
- Guideline for Cybersecurity Incident Response
- Templates for Cybersecurity Incident Response Detailed Plan

Controls implementation guidelines:

- Ensure the OT/ICS critical assets including Safety Instrumented Systems (SIS) recovery procedures are included in the incident response, system recovery, and business continuity plans.

Expected Deliverables:

	• Documented recovery procedures for OT/ICS environment. • Documented incident response plans for OT/ICS environment. • Documented business continuity plans for OT/ICS environment.
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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cybersecurity Incident and Threat Management Policy • Template for Cybersecurity Incident and Threat Management Standard **Controls implementation guidelines:** • Train personnel within the organization in the required skills and courses (including employees and contractors) to respond to cybersecurity incidents related to OT/ICS.
	Expected Deliverables: • A documented list of the organization's personnel embraced by the OT/ICS cybersecurity incidents response training program. • A proof confirming the provision of all personnel within the organization with the required skills and courses (including employees and contractors) to respond to cybersecurity incidents related to OT/ICS.
2-12-1-7	Cybersecurity incident response capabilities, readiness, and plan must be periodically tested by performing cyber-attack simulations exercises.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cybersecurity Incident and Threat Management Policy • Template for Cybersecurity Incident and Threat Management Standard **Controls implementation guidelines:** • Ensure the cybersecurity incident response capabilities, readiness, and plan are periodically tested by performing cyber-attack simulations exercises (such as drills, tabletop exercises).
	Expected Deliverables: • A documented list of cyber-attack simulations exercises (such as cybersecurity drills and tabletop exercises). • A proof that cybersecurity incident response capabilities, readiness, and plan are periodically tested.
2-12-1-8	Threat Intelligence information must be used to identify Tactics, Techniques, and Procedures (TTPs) of activity groups targeting OT/ICS systems.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard

	• Template for Cybersecurity Incident and Threat Management Policy • Template for Cybersecurity Incident and Threat Management Standard **Controls implementation guidelines:** • Gather and document Threat Intelligence information and use it to identify Tactics, Techniques, and Procedures (TTPs) of activity groups targeting OT/ICS systems. • Verify and ensure Threat Intelligence is up-to-date.
	Expected Deliverables: • A documented Threat Intelligence report. • A proof that shows the Threat Intelligence information is 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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cybersecurity Incident and Threat Management Policy • Template for Key Performance Indicator Report **Controls implementation guidelines:** • Review the cybersecurity requirements for cybersecurity incident and threat management within the OT/ICS environment periodically based on a documented and approved review plan and on a defined frequency (e.g., conduct a review annually). • Develop key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically based on a defined frequency (e.g., conduct a review annually).
	Expected Deliverables: • A proof that shows the periodic review of cybersecurity requirements for incident and threat management within the OT/ICS environment. • A proof that shows the key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically (based on a defined frequency).

2-13	Physical Security
Objective	To ensure the protection of OT/ICS assets from unauthorized physical access, loss, theft, and damage.

<table>
<tr><td rowspan="8">2-13-1</td><td colspan="2">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:</td></tr>
<tr><td>2-13-1-1</td><td>List of personnel with authorized access to facilities and sensitive locations where OT/ICS assets reside must be maintained.</td></tr>
<tr><td colspan="2">Related Cybersecurity Tools:
Template for Cybersecurity Operational Technology Policy
Template for OT/ICS Security Standard
Template for Physical Security Policy
Template for Physical Security Standard
Controls implementation guidelines:
Identify and list personnel with authorized access to facilities and sensitive locations where OT/ICS assets reside.
Maintain and update the performed list continuously, and manage it according to the mechanism and procedures established within the organization.</td></tr>
<tr><td colspan="2">Expected Deliverables:
A documented list of personnel with authorized access to facilities and sensitive locations where OT/ICS assets reside.
A proof that the list is periodically maintained and updated.</td></tr>
<tr><td>2-13-1-2</td><td>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.</td></tr>
<tr><td colspan="2">Related Cybersecurity Tools:
Template for Cybersecurity Operational Technology Policy
Template for OT/ICS Security Standard
Template for Physical Security Policy
Template for Physical Security Standard
Controls implementation guidelines:
Ensure that the real-time physical intrusion detection alarms and surveillance equipment, and proper mechanisms are implemented.</td></tr>
<tr><td colspan="2">Expected Deliverables:
Site visit to check that the real-time physical intrusion detection alarms and surveillance equipment, and proper mechanisms are implemented.</td></tr>
<tr><td>2-13-1-3</td><td>Physical access points and perimeter to sensitive OT/ICS areas shall be protected and ensure continuous monitoring.</td></tr>
<tr><td colspan="2">Related Cybersecurity Tools:
Template for Cybersecurity Operational Technology Policy
Template for OT/ICS Security Standard
Template for Physical Security Policy</td></tr>
</table>

		• Template for Physical Security Standard **Controls implementation guidelines:** • Identify and list physical access points and perimeter to sensitive OT/ICS areas. • Implement protection and monitoring mechanisms (e.g. access control system) to avoid unauthorized physical access to sensitive OT/ICS areas. Implemented mechanisms should be formally documented (as an implementation plan or procedure). • Verify and ensure that all listed access points and perimeters are continuously monitored.
		Expected Deliverables: • A documented list of physical access points and perimeter to sensitive OT/ICS areas. • Site visit to check that all listed access points and perimeters are continuously monitored.
	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.
		Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Physical Security Policy • Template for Physical Security Standard **Controls implementation guidelines:** • Verify and ensure the use of appropriate protection measures, such as locking all cabinets containing control systems. • Verify and ensure that all OT/ICS assets are protected from unauthorized physical access in line with the organization's approved mechanisms.
		Expected Deliverables: • Site visit to check the protection measures of the following sites: ○ Physical access to industrial facilities. ○ Cabinets containing control systems. ○ Control room center (CCR).
	2-13-1-5	Strict limitation must be enforced on the physical access to all OT/ICS assets, including Safety Instrumented Systems (SIS).
		Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Physical Security Policy • Template for Physical Security Standard **Controls implementation guidelines:**

- Verify and ensure that strict physical access limitation to all OT/ICS assets, including Safety Instrumented Systems (SIS) is enforced.

Expected Deliverables:

- Site visit to check that the strict physical access limitation to all OT/ICS assets, including Safety Instrumented Systems (SIS) is enforced.

2-13-1-6	Visitor access records to restricted locations where OT/ICS reside must be maintained.

Related Cybersecurity Tools:

- Template for Cybersecurity Operational Technology Policy
- Template for OT/ICS Security Standard
- Template for Physical Security Policy
- Template for Physical Security Standard

Controls implementation guidelines:

- Ensure to maintain visitor access records to restricted locations where OT/ ICS reside.
- Ensure that the visitors must record their entries once they access the restricted locations where OT/ ICS reside.

Expected Deliverables:

- Documented visitor access logs to restricted area where OT/ ICS reside.
- Site visit to check that the visitor access records to restricted locations where OT/ ICS reside is maintained.

2-13-1-7	Work being performed by contractor or vendor personnel must be monitored.

Related Cybersecurity Tools:

- Template for Cybersecurity Operational Technology Policy
- Template for OT/ICS Security Standard
- Template for Physical Security Policy
- Template for Physical Security Standard

Controls implementation guidelines:

- Define the requirements for monitoring work that is being performed by the contractor or vendor personnel. All requirements should be formally documented and aligned with related documents such as (work permits).
- Define and prepare contractor or vendor personnel's works register.
- Verify and ensure that all work being performed by contractor or vendor personnel is monitored.

Expected Deliverables:

- Requirements document for monitoring work that is being performed by the contractor or vendor personnel.

	• A proof that shows all work being performed by contractor, service providers, or vendor personnel is 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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Physical Security Policy • Template for Physical Security Standard **Controls implementation guidelines:** • Ensure that training and skillsets for industrial security personnel including (facilities and plants) are provided in line with their roles and responsibilities with respect to OT/ICS physical security.	
	Expected Deliverables: • A documented list of the organizational security guards' names embraced by the OT/ICS physical security training program. • A proof confirming that training and skillsets for industrial security personnel including (facilities and plants) are provided, and are in line with their 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).
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Physical Security Policy • Template for Physical Security Standard **Controls implementation guidelines:** • Ensure the physical security capabilities and readiness are periodically tested (based on a defined frequency) by performing simulation exercises (such as social engineering).	
	Expected Deliverables: • A documented list of cyber-attack simulations (cybersecurity drills and tabletop exercises). • A proof that physical security capabilities and readiness are 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.	
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy	

	• Template for OT/ICS Security Standard • Template for Physical Security Policy • Template for Key Performance Indicator Report **Controls implementation guidelines:** • Review the cybersecurity requirements for physical security management within the OT/ICS environment periodically based on a documented and approved review plan and on a defined frequency (e.g., conduct a review annually). • Develop key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically based on a defined frequency (e.g., conduct a review annually).
	Expected Deliverables: • A proof that shows the periodic review of cybersecurity requirements for physical security management within the OT/ICS environment. • A proof that shows the key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically (based on a defined frequency).

3 (Cybersecurity Resilience)

3-1	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	
Objective	To ensure the inclusion of the cybersecurity resiliency requirements within the organization's business continuity management and to remediate and minimize the impacts on OT/ICS environment from disasters caused by cybersecurity incidents.	
Controls		
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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cybersecurity Business Continuity Policy **Controls implementation guidelines:** • Define a list of sensitive operation technologies and activities necessary to sustain minimum operations of the OT/ICS systems in coordination with the industrial facility personnel.	

	• Verify and ensure that all activities identified are sufficient to maintain the minimum operation of sensitive operation technologies.
	Expected Deliverables: • A documented list of sensitive operation technologies of the OT/ICS systems at the facility. • A documented list of essential activities to maintain the minimum operation of sensitive operation technologies. • A proof that all activities identified are sufficient to maintain the minimum operation of sensitive operation technologies.
3-1-1-2	Redundant OT/ICS networks, connections, and devices must be implemented in accordance to the periodic cybersecurity risk assessment.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cybersecurity Business Continuity Policy **Controls implementation guidelines:** • Perform the periodic cybersecurity risk assessment in line with the defined periodical OT/ICS risk assessment plan. • Based on the risk assessment, identify and document areas and systems where redundancy is necessary. • Implement redundant networks, connections, and sensitive devices for OT/ICS assets in line with risk assessment results.
	Expected Deliverables: • A periodic risk assessment report. • A documented list of areas and systems where redundancy is necessary. • Site visit to check that redundant networks, connections, and sensitive devices for OT/ICS assets are implemented in line with risk assessment results.
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).
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cybersecurity Business Continuity Policy **Controls implementation guidelines:** • Define and document OT/ICS cybersecurity requirements related to the Business Continuity Plan (BCP), Business Impact Analysis (BIA), Recovery Time Objectives (RTO), and Recovery Point Objectives (RPO).

- Include documented requirements in the Business Continuity Plan (BCP), Business Impact Analysis (BIA), Recovery Time Objectives (RTO), and Recovery Point Objectives (RPO).
- Verify and ensure that documented OT/ICS cybersecurity requirements are integrated and aligned with general organizational requirements.

Expected Deliverables:

- Documented OT/ICS cybersecurity requirements.
- A proof that documented OT/ICS cybersecurity requirements are 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.

Related Cybersecurity Tools:

- Template for Cybersecurity Operational Technology Policy
- Template for OT/ICS Security Standard
- Template for Cybersecurity Business Continuity Policy

Controls implementation guidelines:

- Define and document OT/ICS cybersecurity requirements related to the Disaster Recovery Plan (DRP).
- Ensure the OT/ICS cybersecurity requirements are incorporated into the Disaster Recovery Plan (DRP) including:
  - Cybersecurity related disaster scenarios.
  - System failure handling procedures.
  - Operational technology management procedures.

Expected Deliverables:

- Documented OT/ICS cybersecurity requirements.
- A proof that the documented OT/ICS cybersecurity requirements are 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.

Related Cybersecurity Tools:

- Template for Cybersecurity Operational Technology Policy
- Template for OT/ICS Security Standard
- Template for Cybersecurity Business Continuity Policy

Controls implementation guidelines:

- Develop and implement system failure handling procedures.

	• Verify and ensure that all OT/ICS assets or systems have defined the acceptable safe mode and the action plan to achieve a continuous operation.	
	Expected Deliverables: • A documented system failure handling procedures. • A proof that shows all OT/ICS assets or systems have defined the acceptable safe mode and the action plan 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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cybersecurity Business Continuity Policy **Controls implementation guidelines:** • Conduct a periodic testing and simulation exercises (e.g. tabletop exercises "TTX") to test the effectiveness of OT/ICS related DRP and BCP and complete incident root cause analysis. • Document the reports specified for testing and simulation exercises results.	
	Expected Deliverables: • A documented OT/ICS related DRP and BCP effectiveness testing plan. • A periodically prepared testing and simulation exercises reports. • A proof that OT/ICS related to DRP and BCP effectiveness and complete incident root cause analysis is periodically tested.	
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.	
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Cybersecurity Business Continuity Policy • Template for Key Performance Indicator Report **Controls implementation guidelines:** • Review the cybersecurity requirements for cybersecurity resilience aspects of business continuity management in the OT/ICS environment periodically based on a documented and approved review plan and on a defined frequency (e.g., conduct a review annually). • Develop key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically based on a defined frequency (e.g., conduct a review annually).	

	Expected Deliverables: • A proof that shows the periodic review of cybersecurity requirements for cybersecurity resilience aspects of business continuity management for the OT/ICS environment. • A proof that shows the key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically (based on a defined frequency).

4 (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		
4-1-1	In addition to the ECC subcontrols within controls 4-1-2 and 4-1-3, 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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Third-Party Cybersecurity Policy **Controls implementation guidelines:** • Define, document, and approve OT/ICS products and services cybersecurity requirements to be included within the procurement lifecycle (Defining the Requirements, Vendor Selection, Negotiation and Contracting, Service Delivery and Performance Monitoring, and Renewal/Contract Closure). • Ensure that the cybersecurity requirements are included in the procurement lifecycle for OT/ICS products and services.	
	Expected Deliverables: • A documented OT/ICS products and services cybersecurity requirements during the procurement lifecycle. • A proof that all new procurements of OT/ICS products and services are conducted in line with defined requirements.	
	4-1-1-2	Cybersecurity requirements for third-party evaluation, selection, and information sharing must be defined.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Third-Party Cybersecurity Policy **Controls implementation guidelines:** • Define, document, and approve cybersecurity requirements for third-party evaluation, selection, and information sharing. • Ensure that all defined cybersecurity requirements are included within the qualification requirements.	

	Expected Deliverables: • Documented cybersecurity requirements for third-party evaluation, selection, and information sharing. • A qualification requirements document that include all defined cybersecurity requirements. • A proof that the evaluation, selection, and information sharing of all third-parties are conducted based on the defined requirements.	
	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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Third-Party Cybersecurity Policy **Controls implementation guidelines:** • Obtain a certification from third-party contractors and vendors that use formal and documented practices for the Secure Development Life Cycle (SDLC) of systems and assets designed or deployed in the OT/ICS environment.	
	Expected Deliverables: • A certification from approved third-party contractors and vendors that they are using Secure Development Life Cycle (SDLC) practices for systems and assets 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.
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Third-Party Cybersecurity Policy **Controls implementation guidelines:** • Conduct periodic cybersecurity assessment and audits of third-party providers to ensure control over any identified cyber risks.	
	Expected Deliverables: • Cybersecurity assessments and audits of OT/ICS third-party providers' reports.	
4-1-2	With reference to the ECC control 4-1-4, the cybersecurity requirements for third-party cybersecurity in OT/ICS environment must be reviewed, and their implementation effectiveness is measured and evaluated periodically.	
	Related Cybersecurity Tools: • Template for Cybersecurity Operational Technology Policy • Template for OT/ICS Security Standard • Template for Third-Party Cybersecurity Policy • Template for Key Performance Indicator Report	

	Controls implementation guidelines: • Review the cybersecurity requirements for third-party cybersecurity for the OT/ICS environment periodically based on a documented and approved review plan and on a defined frequency (e.g., conduct a review annually). • Develop key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically based on a defined frequency (e.g., conduct a review annually).
	Expected Deliverables: • A proof that shows the periodic review of cybersecurity requirements for third-party cybersecurity for the OT/ICS environment. • A proof that shows the key performance indicators (KPIs) for each control within the related policy or procedure to ensure the implementation effectiveness is measured and evaluated periodically (based on a defined frequency).

الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority