NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Saudi Arabia - Operational Technology Cybersecurity Controls (OTCC - 1: 2022)
Focal Document URL: https://nca.gov.sa/otcc_en.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-otcc-1-2022.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
1	Cybersecurity Governance	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
1-1	Cybersecurity Policies and Procedures	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
1-1-1	Cybersecurity Policies and Procedures	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.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
1-1-2	Cybersecurity Policies and Procedures	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.	Functional	Intersects With	Secure Practices Alignment Justification	GOV-01.4	Mechanisms exist to align the organization's Security, Compliance & Resilience Program (SCRP) with one or more industry-recognized frameworks that: (1) Support external scrutiny; and	8	
1-1-2	Cybersecurity Policies and Procedures	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.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8	
1-1-3	Cybersecurity Policies and Procedures	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.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
1-2	Cybersecurity Roles and Responsibilities	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
1-2-1	Cybersecurity Roles and Responsibilities	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:	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
1-2-1-1	Cybersecurity Roles and Responsibilities	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.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	5	
1-2-1-2	Cybersecurity Roles and Responsibilities	Cybersecurity roles and responsibilities related to OT/ ICS assets must be assigned to the cybersecurity function in the organization.	Functional	Intersects With	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5	
1-2-1-2	Cybersecurity Roles and Responsibilities	Cybersecurity roles and responsibilities related to OT/ ICS assets must be assigned to the cybersecurity function in the organization.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
1-3	Cybersecurity Risk Management	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
1-3-1	Cybersecurity Risk Management	In addition to the ECC subdomain 1-5, cybersecurity requirements for cybersecurity risk management in OT/ICS must include, at a minimum, the following:	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	10	
1-3-1-1	Cybersecurity Risk Management	OT/ICS cybersecurity risk management methodology must be included as part of the organization's risk management and safety risk management methodologies.	Functional	Intersects With	Risk Assessment Methodology	RSK-04.2	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	5	
1-3-1-2	Cybersecurity Risk Management	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.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
1-3-1-3	Cybersecurity Risk Management	Risk register for OT/ICS cybersecurity risks must be included as part of the organization's risk register.	Functional	Intersects With	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
1-3-1-4	Cybersecurity Risk Management	Appropriate level assignment to facilities which include (OT/ICS) must be conducted based on approved methodology.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
1-3-1-5	Cybersecurity Risk Management	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.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
1-3-1-6	Cybersecurity Risk Management	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.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
1-3-1-6	Cybersecurity Risk Management	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.	Functional	Intersects With	Risk Treatment Options	RSK-06.3	Mechanisms exist to select appropriate risk treatment options, based on applicable risk assessment findings, including: (1) Mitigating the risk to an acceptable level; (2) Avoiding the risk (e.g., terminating the project); (3) Transferring the risk to a third party (e.g., insurance, service provider, etc.); or (4) Accepting the risk.	5	
1-3-1-6	Cybersecurity Risk Management	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.	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-06.4	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	5	
1-3-1-7	Cybersecurity Risk Management	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.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: (1) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner); (8) Resources required to conduct remediation actions; (9) Planned remedial actions to the deficiency(ies); (10) Proposed remediation timeline; and (11) Disposition statement (e.g., closeout summary).	5	
1-3-1-7	Cybersecurity Risk Management	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.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
1-4	Cybersecurity in Industrial Control System Project Management	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
1-4-1	Cybersecurity in Industrial Control System Project Management	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:	Functional	Subset Of	Embedded Technology Security Program	EMB-01	Mechanisms exist to facilitate the implementation of embedded technology controls.	10	
1-4-1-1	Cybersecurity in Industrial Control System Project Management	Cybersecurity requirements must be part of OT/ICS project's lifecycle.	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience controls as part of Technology Assets, Applications and/or Services (TAAS) project development to determine whether controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting requirements.	5	
1-4-1-1	Cybersecurity in Industrial Control System Project Management	Cybersecurity requirements must be part of OT/ICS project's lifecycle.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by: (1) Defining technical security, compliance and resilience requirements; and (2) Performing a criticality analysis at predefined decision points in the Secure Development Life Cycle (SDLC).	5	
1-4-1-1	Cybersecurity in Industrial Control System Project Management	Cybersecurity requirements must be part of OT/ICS project's lifecycle.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Saudi Arabia - Operational Technology Cybersecurity Controls (OTCC - 1: 2022)
Focal Document URL: https://nca.gov.sa/otcc_en.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-otcc-1-2022.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
1-4-1-2	Cybersecurity in Industrial Control System Project Management	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).	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	
1-4-1-2	Cybersecurity in Industrial Control System Project Management	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).	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; (11) Artificial Intelligence and Autonomous Technologies (AAT); and/or (12) Other Technology Assets, Applications and/or Services (TAAS) that require specialized expertise to determine conformity with security, compliance and/or resilience requirements.	5	
1-4-1-2	Cybersecurity in Industrial Control System Project Management	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).	Functional	Intersects With	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical security, compliance and resilience controls.	5	
1-4-1-2	Cybersecurity in Industrial Control System Project Management	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).	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5	
1-4-1-3	Cybersecurity in Industrial Control System Project Management	Secure-by-design principles must be included as part of security architectural designs for OT/ICS environments.	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience controls as part of Technology Assets, Applications and/or Services (TAAS) project development to determine whether controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting requirements.	5	
1-4-1-3	Cybersecurity in Industrial Control System Project Management	Secure-by-design principles must be included as part of security architectural designs for OT/ICS environments.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	5	
1-4-1-4	Cybersecurity in Industrial Control System Project Management	System development environments including testing environment and integration platforms must be protected.	Functional	Intersects With	Secure Development Environments	TDA-07	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	5	
1-4-2	Cybersecurity in Industrial Control System Project Management	Cybersecurity requirements within the organization's OT/ICS project management must be reviewed, and their implementation effectiveness is measured and evaluated periodically.	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
1-4-2	Cybersecurity in Industrial Control System Project Management	Cybersecurity requirements within the organization's OT/ICS project management must be reviewed, and their implementation effectiveness is measured and evaluated periodically.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5	
1-4-2	Cybersecurity in Industrial Control System Project Management	Cybersecurity requirements within the organization's OT/ICS project management must be reviewed, and their implementation effectiveness is measured and evaluated periodically.	Functional	Intersects With	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	5	
1-4-2	Cybersecurity in Industrial Control System Project Management	Cybersecurity requirements within the organization's OT/ICS project management must be reviewed, and their implementation effectiveness is measured and evaluated periodically.	Functional	Intersects With	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	5	
1-4-2	Cybersecurity in Industrial Control System Project Management	Cybersecurity requirements within the organization's OT/ICS project management must be reviewed, and their implementation effectiveness is measured and evaluated periodically.	Functional	Intersects With	Prioritization To Address Evolving Risks & Threats	PRM-02.1	Mechanisms exist to integrate foundational cybersecurity practices with advanced technologies to maintain situation awareness of and minimize the organization's exposure to evolving risks and threats.	5	
1-4-2	Cybersecurity in Industrial Control System Project Management	Cybersecurity requirements within the organization's OT/ICS project management must be reviewed, and their implementation effectiveness is measured and evaluated periodically.	Functional	Intersects With	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	3	
1-5	Cybersecurity in Change Management	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
1-5-1	Cybersecurity in Change Management	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.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
1-5-2	Cybersecurity in Change Management	Cybersecurity requirements within the organization's OT/ICS change management lifecycle must be implemented.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
1-5-3	Cybersecurity in Change Management	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:	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
1-5-3-1	Cybersecurity in Change Management	Cybersecurity requirements are part of the change management lifecycle.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
1-5-3-2	Cybersecurity in Change Management	Changes are validated in a separate environment prior to implementing the changes on the production environment.	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	5	
1-5-3-3	Cybersecurity in Change Management	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.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
1-5-3-3	Cybersecurity in Change Management	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.	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; (11) Artificial Intelligence and Autonomous Technologies (AAT); and/or (12) Other Technology Assets, Applications and/or Services (TAAS) that require specialized expertise to determine conformity with security, compliance and/or resilience requirements.	5	
1-5-3-3	Cybersecurity in Change Management	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.	Functional	Intersects With	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical security, compliance and resilience controls.	5	
1-5-3-3	Cybersecurity in Change Management	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.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5	
1-5-3-4	Cybersecurity in Change Management	Restricted processes for exceptional changes must be implemented.	Functional	Subset Of	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	10	
1-5-3-4	Cybersecurity in Change Management	Restricted processes for exceptional changes must be implemented.	Functional	Intersects With	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	5	
1-5-3-5	Cybersecurity in Change Management	Automated configuration and asset change detection mechanisms must be implemented.	Functional	Intersects With	Automated Access Enforcement / Auditing	CHG-04.1	Mechanisms exist to perform after-the-fact reviews of configuration change logs to discover any unauthorized changes.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Saudi Arabia - Operational Technology Cybersecurity Controls (OTCC - 1: 2022)
Focal Document URL: https://nca.gov.sa/otcc_en.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-otcc-1-2022.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
1-5-4	Cybersecurity in Change Management	Cybersecurity requirements within the organization's OT/ICS change management requirements must be reviewed, and their implementation effectiveness is measured and evaluated periodically.	Functional	Intersects With	Security, Compliance & Resilience Representative for Asset Lifecycle Changes	CHG-02.3	Mechanisms exist to include a cybersecurity and/or data protection representative in the configuration change control review process.	5	
1-5-4	Cybersecurity in Change Management	Cybersecurity requirements within the organization's OT/ICS change management requirements must be reviewed, and their implementation effectiveness is measured and evaluated periodically.	Functional	Intersects With	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	5	
1-5-4	Cybersecurity in Change Management	Cybersecurity requirements within the organization's OT/ICS change management requirements must be reviewed, and their implementation effectiveness is measured and evaluated periodically.	Functional	Intersects With	Control Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.	5	
1-5-4	Cybersecurity in Change Management	Cybersecurity requirements within the organization's OT/ICS change management requirements must be reviewed, and their implementation effectiveness is measured and evaluated periodically.	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
1-6	Periodical Cybersecurity Review and Audit	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
1-6-1	Periodical Cybersecurity Review and Audit	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.	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
1-6-2	Periodical Cybersecurity Review and Audit	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.	Functional	Intersects With	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate security, compliance and resilience at planned intervals or when the Technology Asset, Application and/or Service (TAAS) undergoes significant changes.	5	
1-7	Cybersecurity in Human Resources	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
1-7-1	Cybersecurity in Human Resources	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.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
1-7-1	Cybersecurity in Human Resources	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.	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	
1-7-1	Cybersecurity in Human Resources	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.	Functional	Intersects With	Third-Party Personnel	HRS-10	Mechanisms exist to govern third-party personnel by reviewing and monitoring third-party security, compliance and/or resilience roles and responsibilities.	5	
1-7-2	Cybersecurity in Human Resources	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.	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
1-7-2	Cybersecurity in Human Resources	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.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5	
1-7-2	Cybersecurity in Human Resources	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.	Functional	Intersects With	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
1-8	Cybersecurity in Human Resources	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
1-8-1	Cybersecurity in Human Resources	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.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
1-8-2	Cybersecurity in Human Resources	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:	Functional	Subset Of	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	10	
1-8-2-1	Cybersecurity in Human Resources	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).	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
1-8-2-1	Cybersecurity in Human Resources	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).	Functional	Intersects With	Continuing Professional Education (CPE) - Security, Compliance & Resilience Personnel	SAT-03.7	Mechanisms exist to ensure security, compliance and resilience personnel receive Continuing Professional Education (CPE) training to maintain currency and proficiency with industry-recognized secure practices that are pertinent to their assigned roles and responsibilities.	5	
1-8-2-2	Cybersecurity in Human Resources	Participation in OT/ICS authorized and/or specialized organizations and groups must be encouraged to stay up-to-date on common cybersecurity practices.	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	
2	Cybersecurity Defense	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
2-1	Asset Management	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-1-1	Asset Management	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:	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
2-1-1-1	Asset Management	OT/ICS assets inventory must be developed in electronic format for all OT/ICS assets, and reviewed periodically.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	
2-1-1-2	Asset Management	Automated solution to collect asset inventory information must be utilized.	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	5	
2-1-1-3	Asset Management	OT/ICS asset inventory must be stored securely.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive and/or regulated data wherever it is processed and/or stored.	5	
2-1-1-4	Asset Management	Asset owners for all OT/ICS assets must be identified and involved throughout the relevant asset inventory management lifecycle.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
2-1-1-5	Asset Management	Criticality rating for all assets must be assigned, documented, and approved by asset owners.	Functional	Intersects With	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	5	
2-1-2	Asset Management	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.	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
2-1-2	Asset Management	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.	Functional	Intersects With	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5	
2-2	Identity and Access Management	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Saudi Arabia - Operational Technology Cybersecurity Controls (OTCC - 1: 2022)
Focal Document URL: https://nca.gov.sa/otcc_en.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-otcc-1-2022.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2-2-1	Identity and Access Management	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:	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
2-2-1-1	Identity and Access Management	Identity and access management lifecycle for OT/ICS is separated and independent from Information Technology (IT) including centrally managed identity and access management solutions.	Functional	Subset Of	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	10	
2-2-1-2	Identity and Access Management	Service accounts must be managed securely for OT/ICS services, applications, systems, and devices that are separated and disconnected from interactive users account logins.	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
2-2-1-3	Identity and Access Management	Default credentials for all OT/ICS assets must be changed, disabled, or removed.	Functional	Intersects With	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5	
2-2-1-4	Identity and Access Management	Sessions must be managed securely, including session authenticity, session lockout, and session timeout termination.	Functional	Intersects With	Session Management	AAT-30.2	Mechanisms exist to control AI agent sessions by: (1) Embedding session IDs into the requests to the AI model; (2) Implementing capabilities to correlate sessions; and (3) Terminating sessions after a defined time period.	5	
2-2-1-5	Identity and Access Management	Automatic disabling/removing of service accounts, programs, or accounts related to (OT/ICS) assets must be prevented, except for monitoring systems.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	8	
2-2-1-6	Identity and Access Management	Dual approval and explicit privilege escalation mechanisms for sensitive actions within the OT/ICS environment must be employed.	Functional	Intersects With	Dual Approval For High-Impact Environments	CHG-08	Mechanisms exist to require dual approval for any changes that might result in a serious incident that could adversely impact: (1) Business processes; and/or (2) Technology Assets, Applications, Services and/or Data (TAASD).	5	
2-2-1-7	Identity and Access Management	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.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
2-2-1-7	Identity and Access Management	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.	Functional	Intersects With	Automated Monitoring & Control	NET-14.1	Automated mechanisms exist to monitor and control remote access sessions.	5	
2-2-1-7	Identity and Access Management	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.	Functional	Intersects With	Protection of Confidentiality / Integrity Using Encryption	NET-14.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of remote access sessions (e.g., VPN).	5	
2-2-1-8	Identity and Access Management	Secure and complex password standards must be implemented.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
2-2-1-8	Identity and Access Management	Secure and complex password standards must be implemented.	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
2-2-1-9	Identity and Access Management	Secure mechanisms to store OT/ICS assets' passwords must be used.	Functional	Intersects With	Password Managers	IAC-10.11	Mechanisms exist to protect and store passwords via a password manager tool.	5	
2-2-1-10	Identity and Access Management	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.	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	8	
2-2-1-10	Identity and Access Management	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.	Functional	Intersects With	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	8	
2-2-1-11	Identity and Access Management	Access shall be immediately revoked when no longer needed.	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	8	
2-2-1-11	Identity and Access Management	Access shall be immediately revoked when no longer needed.	Functional	Intersects With	Change of Roles & Duties	IAC-07.1	Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.	8	
2-2-1-11	Identity and Access Management	Access shall be immediately revoked when no longer needed.	Functional	Intersects With	Termination of Employment	IAC-07.2	Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.	8	
2-2-2	Identity and Access Management	With reference to the ECC control 2-2-4, the cybersecurity requirements for identity and access management in OT/ICS env ronment must be reviewed, and its implementation effectiveness is measured and evaluated periodically	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
2-2-2	Identity and Access Management	With reference to the ECC control 2-2-4, the cybersecurity requirements for identity and access management in OT/ICS env ronment must be reviewed, and its implementation effectiveness is measured and evaluated periodically	Functional	Intersects With	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	5	
2-3	System and Processing Facilities Protection	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-3-1	System and Processing Facilities Protection	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:	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
2-3-1-1	System and Processing Facilities Protection	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.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	8	
2-3-1-1	System and Processing Facilities Protection	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.	Functional	Intersects With	Extended Detection & Response (XDR)	END-06.8	Mechanisms exist to implement Extended Detection & Response (XDR) technologies to correlate data and respond to threats across multiple security layers, including: (1) Endpoints; (2) On-premises networks; (3) Cloud-based networks; (4) Electronic communications; (5) Applications; and (6) Services.	3	
2-3-1-2	System and Processing Facilities Protection	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.	Functional	Intersects With	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	5	
2-3-1-3	System and Processing Facilities Protection	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.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
2-3-1-4	System and Processing Facilities Protection	Principles of least privilege and least functionality must be applied.	Functional	Equal	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	10	
2-3-1-5	System and Processing Facilities Protection	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.	Functional	No Relationship	N/A	N/A	N/A	0	
2-3-1-6	System and Processing Facilities Protection	Application whitelisting techniques or other similar techniques must be deployed to limit the applications that are allowed to run in OT/ICS environment.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	
2-3-1-7	System and Processing Facilities Protection	OT/ICS assets must be managed through dedicated, segmented and hardened Engineering Workstation (EWS) and Human-Machine Interface (HMI) for management purposes and maintenance.	Functional	Intersects With	Dedicated Administrative Machines	IAC-20.4	Mechanisms exist to restrict executing administrative tasks or tasks requiring elevated access to a dedicated machine.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Saudi Arabia - Operational Technology Cybersecurity Controls (OTCC - 1: 2022)
Focal Document URL: https://nca.gov.sa/otcc_en.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-otcc-1-2022.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2-3-1-8	System and Processing Facilities Protection	External storage media is scanned and analyzed against malware and APT. The scan must be executed in an isolated and secure environment.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	3	
2-3-1-9	System and Processing Facilities Protection	Usage of external storage media in the production environment must be restricted unless secure mechanisms for data transfer are developed and properly implemented.	Functional	Intersects With	Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	5	
2-3-1-10	System and Processing Facilities Protection	Systems' logs and critical files must be protected from unauthorized access, tampering, illegitimate modification and/or deletion.	Functional	Intersects With	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	5	
2-3-1-11	System and Processing Facilities Protection	Unauthorized applications, scripts, tasks, and changes must be detected and analyzed.	Functional	Intersects With	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	5	
2-3-1-11	System and Processing Facilities Protection	Unauthorized applications, scripts, tasks, and changes must be detected and analyzed.	Functional	Intersects With	Respond To Unauthorized Changes	CFG-02.8	Mechanisms exist to respond to unauthorized changes to configuration settings as security incidents.	5	
2-3-1-12	System and Processing Facilities Protection	New communications sessions and commands execution must be detected and analyzed.	Functional	Intersects With	Extended Detection & Response (XDR)	END-06.8	Mechanisms exist to implement Extended Detection & Response (XDR) technologies to correlate data and respond to threats across multiple security layers, including: (1) Endpoints; (2) On-premises networks; (3) Cloud-based networks; (4) Electronic communications; (5) Applications; and (6) Services.	5	
2-3-1-12	System and Processing Facilities Protection	New communications sessions and commands execution must be detected and analyzed.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	
2-3-1-12	System and Processing Facilities Protection	New communications sessions and commands execution must be detected and analyzed.	Functional	Intersects With	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-08	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	5	
2-3-1-13	System and Processing Facilities Protection	Direct communications between the OT/ICS environment and external hosts must be detected and analyzed.	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
2-3-1-13	System and Processing Facilities Protection	Direct communications between the OT/ICS environment and external hosts must be detected and analyzed.	Functional	Intersects With	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-08	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	5	
2-3-2	System and Processing Facilities Protection	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.	Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5	
2-3-2	System and Processing Facilities Protection	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.	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
2-4	Networks Security Management	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-4-1	Networks Security Management	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:	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
2-4-1-1	Networks Security Management	OT/ICS environment must be segmented logically or physically from other environments or networks.	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	5	
2-4-1-1	Networks Security Management	OT/ICS environment must be segmented logically or physically from other environments or networks.	Functional	Intersects With	Separate Subnets To Isolate Functions	NET-06.9	Mechanisms exist to implement physically or logically separate subnetworks to isolate organization-defined Technology Assets, Applications, Services and/or Data (TAASD).	5	
2-4-1-2	Networks Security Management	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".	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	5	
2-4-1-2	Networks Security Management	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".	Functional	Intersects With	Sensitive / Regulated Data Enclave (Secure Zone)	NET-06.3	Mechanisms exist to implement segmentation controls to restrict inbound and outbound connectivity for sensitive and/or regulated data enclaves (secure zones).	5	
2-4-1-3	Networks Security Management	Safety Instrumented Systems (SIS) must be segmented logically or physically from other OT/ICS networks.	Functional	Intersects With	Sensitive / Regulated Data Enclave (Secure Zone)	NET-06.3	Mechanisms exist to implement segmentation controls to restrict inbound and outbound connectivity for sensitive and/or regulated data enclaves (secure zones).	5	
2-4-1-4	Networks Security Management	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.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
2-4-1-4	Networks Security Management	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.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
2-4-1-5	Networks Security Management	Wireless technologies must be segmented logically or physically from other OT/ICS networks.	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	5	
2-4-1-5	Networks Security Management	Wireless technologies must be segmented logically or physically from other OT/ICS networks.	Functional	Intersects With	Separate Subnets To Isolate Functions	NET-06.9	Mechanisms exist to implement physically or logically separate subnetworks to isolate organization-defined Technology Assets, Applications, Services and/or Data (TAASD).	5	
2-4-1-6	Networks Security Management	Network communications, services, and connection points between different zones must be limited to the minimum to meet operational, maintenance, and safety requirements.	Functional	Intersects With	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	5	
2-4-1-6	Networks Security Management	Network communications, services, and connection points between different zones must be limited to the minimum to meet operational, maintenance, and safety requirements.	Functional	Intersects With	Separate Subnets To Isolate Functions	NET-06.9	Mechanisms exist to implement physically or logically separate subnetworks to isolate organization-defined Technology Assets, Applications, Services and/or Data (TAASD).	5	
2-4-1-7	Networks Security Management	Direct exposure of common remote authentication and access management services on external-facing hosts must be prevented.	Functional	Intersects With	Direct Internet Access Restrictions	NET-06.5	Mechanisms exist to prohibit, or strictly-control, Internet access from sensitive and/or regulated data enclaves (secure zones).	5	
2-4-1-7	Networks Security Management	Direct exposure of common remote authentication and access management services on external-facing hosts must be prevented.	Functional	Intersects With	Managed Access Control Points	NET-14.3	Mechanisms exist to route all remote accesses through managed network access control points (e.g., VPN concentrator).	5	
2-4-1-8	Networks Security Management	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.	Functional	Intersects With	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	5	
2-4-1-9	Networks Security Management	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.	Functional	Intersects With	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	5	
2-4-1-9	Networks Security Management	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.	Functional	Intersects With	Separate Subnets To Isolate Functions	NET-06.9	Mechanisms exist to implement physically or logically separate subnetworks to isolate organization-defined Technology Assets, Applications, Services and/or Data (TAASD).	5	
2-4-1-10	Networks Security Management	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	Functional	Intersects With	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	5	
2-4-1-10	Networks Security Management	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	Functional	Intersects With	Separate Subnets To Isolate Functions	NET-06.9	Mechanisms exist to implement physically or logically separate subnetworks to isolate organization-defined Technology Assets, Applications, Services and/or Data (TAASD).	5	
2-4-1-10	Networks Security Management	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	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
2-4-1-11	Networks Security Management	Proxies must be employed between the corporate and OT/ICS zones for all machine-to-machine traffic.	Functional	Intersects With	Route Internal Traffic to Proxy Servers	NET-18.1	Mechanisms exist to route internal communications traffic to external networks through organization-approved proxy servers at managed interfaces.	5	
2-4-1-12	Networks Security Management	Dedicated gateways must be used to segment OT/ICS networks from corporate zone.	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
2-4-1-12	Networks Security Management	Dedicated gateways must be used to segment OT/ICS networks from corporate zone.	Functional	Intersects With	Separate Subnets To Isolate Functions	NET-06.9	Mechanisms exist to implement physically or logically separate subnetworks to isolate organization-defined Technology Assets, Applications, Services and/or Data (TAASD).	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Saudi Arabia - Operational Technology Cybersecurity Controls (OTCC - 1: 2022)
Focal Document URL: https://nca.gov.sa/otcc_en.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-otcc-1-2022.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2-4-1-13	Networks Security Management	Dedicated DMZ zone must be used to reside any system that needs services provided by corporate zone.	Functional	Intersects With	Separate Subnets To Isolate Functions	NET-06.9	Mechanisms exist to implement physically or logically separate subnetworks to isolate organization-defined Technology Assets, Applications, Services and/or Data (TAASD).	5	
2-4-1-13	Networks Security Management	Dedicated DMZ zone must be used to reside any system that needs services provided by corporate zone.	Functional	Intersects With	Use of Demilitarized Zones (DMZ)	WEB-02	Mechanisms exist to utilize a Demilitarized Zone (DMZ) to restrict inbound traffic to authorized Technology Assets, Applications and/or Services (TAAS) on certain services, protocols and ports.	5	
2-4-1-14	Networks Security Management	Strict limitation on enabling/usage of industrial protocols and ports to the minimum to meet operational, maintenance, and safety requirements.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	
2-4-1-15	Networks Security Management	Periodic patches and upgrades for production assets must be certified by respective vendor and tested in a separate environment prior to implementation.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
2-4-1-15	Networks Security Management	Periodic patches and upgrades for production assets must be certified by respective vendor and tested in a separate environment prior to implementation.	Functional	Intersects With	Software Patch Integrity	VPM-05.8	Mechanisms exist to ensure software and/or firmware patches are: (1) Obtained from trusted sources; and (2) Checked for integrity.	5	
2-4-1-16	Networks Security Management	Details related to network architecture and topology, zones, network data flows, connectivity, and interdependencies must be documented, updated, and maintained.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive and/or regulated data flows.	5	
2-4-2	Networks Security Management	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.	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
2-4-2	Networks Security Management	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.	Functional	Intersects With	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	5	
2-5	Mobile Devices Security	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-5-1	Mobile Devices Security	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:	Functional	Subset Of	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10	
2-5-1-1	Mobile Devices Security	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.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
2-5-1-1	Mobile Devices Security	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.	Functional	Intersects With	Organization-Owned Mobile Devices	MDM-07	Mechanisms exist to prohibit the installation of non-approved applications or approved applications not obtained through the organization-approved application store.	5	
2-5-1-2	Mobile Devices Security	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	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
2-5-1-3	Mobile Devices Security	Limited and approved list of mobile devices must be defined while ensuring that only these mobile devices can be connected to OT/ICS environment.	Functional	Intersects With	Access Control For Mobile Devices	MDM-02	Mechanisms exist to enforce access control requirements for the connection of mobile devices to organizational Technology Assets, Applications and/or Services (TAAS).	5	
2-5-1-3	Mobile Devices Security	Limited and approved list of mobile devices must be defined while ensuring that only these mobile devices can be connected to OT/ICS environment.	Functional	Intersects With	Personally-Owned Mobile Devices	MDM-06	Mechanisms exist to restrict the connection of personally-owned, mobile devices to organizational Technology Assets, Applications and/or Services (TAAS).	5	
2-5-1-3	Mobile Devices Security	Limited and approved list of mobile devices must be defined while ensuring that only these mobile devices can be connected to OT/ICS environment.	Functional	Intersects With	Organization-Owned Mobile Devices	MDM-07	Mechanisms exist to prohibit the installation of non-approved applications or approved applications not obtained through the organization-approved application store.	5	
2-5-1-4	Mobile Devices Security	Centralized management of mobile devices must be deployed.	Functional	Intersects With	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	5	
2-5-1-5	Mobile Devices Security	Encryptions mechanisms must be used for mobile devices authorized to access the OT/ICS assets.	Functional	Intersects With	Full Device & Container-Based Encryption	MDM-03	Cryptographic mechanisms exist to protect the confidentiality and integrity of information on mobile devices through full-device or container encryption.	5	
2-5-2	Mobile Devices Security	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.	Functional	Intersects With	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	5	
2-5-2	Mobile Devices Security	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.	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
2-6	Data and Information Protection	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-6-1	Data and Information Protection	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:	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
2-6-1	Data and Information Protection	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:	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
2-6-1-1	Data and Information Protection	Electronic and physical data (at rest and in transit) must be protected at a level consistent with its classification.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	8	
2-6-1-1	Data and Information Protection	Electronic and physical data (at rest and in transit) must be protected at a level consistent with its classification.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	8	
2-6-1-2	Data and Information Protection	Data Leakage Prevention (DLP) mechanisms must be used to protect the classified data and information.	Functional	Intersects With	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5	
2-6-1-3	Data and Information Protection	Secure wiping mechanisms for configuration details and stored data from OT/ICS assets prior to decommissioning must be implemented.	Functional	Intersects With	Remote Purging	MDM-05	Mechanisms exist to remotely purge selected information from mobile devices.	5	
2-6-1-4	Data and Information Protection	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.	Functional	Intersects With	Ad-Hoc Transfers	DCH-17	Mechanisms exist to secure ad-hoc exchanges of large digital files with internal or external parties.	3	
2-6-2	Data and Information Protection	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.	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
2-6-2	Data and Information Protection	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.	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
2-7	Cryptography	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-7-1	Cryptography	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).	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
2-7-2	Cryptography	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.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
2-7-2	Cryptography	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.	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Saudi Arabia - Operational Technology Cybersecurity Controls (OTCC - 1: 2022)
Focal Document URL: https://nca.gov.sa/otcc_en.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-otcc-1-2022.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2-8	Backup and Recovery Management	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-8-1	Backup and Recovery Management	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:	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
2-8-1-1	Backup and Recovery Management	Backups for all OT/ICS assets must be covered and stored in centralized and offline locations.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
2-8-1-1	Backup and Recovery Management	Backups for all OT/ICS assets must be covered and stored in centralized and offline locations.	Functional	Intersects With	Transfer to Alternate Storage Site	BCD-11.6	Mechanisms exist to transfer backup data to the alternate storage site at a rate that is capable of meeting both Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	3	
2-8-1-2	Backup and Recovery Management	OT/ICS assets' critical configuration files and engineering files must be included in the backup's scope.	Functional	Intersects With	Separate Storage for Critical Information	BCD-11.2	Mechanisms exist to store backup copies of critical software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the system being backed up.	5	
2-8-1-3	Backup and Recovery Management	Backups must be performed periodically as per the defined OT/ICS assets classification and their associated risks.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
2-8-1-4	Backup and Recovery Management	Access, storage, and transfer of backups and their mediums must be secured to ensure their protection against damage, change, or unauthorized access.	Functional	Intersects With	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	3	
2-8-2	Backup and Recovery Management	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.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
2-8-2	Backup and Recovery Management	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.	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
2-9	Vulnerabilities Management	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-9-1	Vulnerabilities Management	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:	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
2-9-1-1	Vulnerabilities Management	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.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	
2-9-1-2	Vulnerabilities Management	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.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
2-9-1-3	Vulnerabilities Management	With reference to the ECC subcontrol 2-10-3-1, vulnerability assessment for OT/ICS systems must be conducted periodically.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
2-9-2	Vulnerabilities Management	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.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
2-9-2	Vulnerabilities Management	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.	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
2-10	Penetration Testing	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-10-1	Penetration Testing	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:	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
2-10-1-1	Penetration Testing	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.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	
2-10-1-2	Penetration Testing	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.	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5	
2-10-1-3	Penetration Testing	With reference to the ECC subcontrol 2-11-3-2, penetration testing for OT/ICS systems must be conducted periodically	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5	
2-10-1-4	Penetration Testing	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.	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; (11) Artificial Intelligence and Autonomous Technologies (AAT); and/or (12) Other Technology Assets, Applications and/or Services (TAAS) that require specialized expertise to determine conformity with security, compliance and/or resilience requirements.	5	
2-10-2	Penetration Testing	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	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
2-10-2	Penetration Testing	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	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
2-11	Cybersecurity Event Logs and Monitoring Management	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-11-1	Cybersecurity Event Logs and Monitoring Management	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:	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
2-11-1-1	Cybersecurity Event Logs and Monitoring Management	Cybersecurity event logs and audit trails must be activated for all OT/ICS assets.	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	5	
2-11-1-2	Cybersecurity Event Logs and Monitoring Management	Failure attempts in accessing the organization's monitoring systems must be detected and logged.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	
2-11-1-3	Cybersecurity Event Logs and Monitoring Management	Continuous, in-depth cybersecurity log review and monitoring, covering all logs and audit trails must be conducted.	Functional	Intersects With	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	5	
2-11-1-4	Cybersecurity Event Logs and Monitoring Management	Monitoring, detecting, and analyzing User Behaviors Analytics (UBA) must be performed.	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Saudi Arabia - Operational Technology Cybersecurity Controls (OTCC - 1: 2022)
Focal Document URL: https://nca.gov.sa/otcc_en.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-otcc-1-2022.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2-11-1-5	Cybersecurity Event Logs and Monitoring Management	Upload or download activities of OT/ICS assets including Safety Instrumented Systems (SIS) must be detected.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
2-11-1-6	Cybersecurity Event Logs and Monitoring Management	All remote access sessions must be monitored.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
2-11-1-7	Cybersecurity Event Logs and Monitoring Management	Malicious events must be detected and analyzed.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
2-11-1-8	Cybersecurity Event Logs and Monitoring Management	Logging and monitoring of new alerts when new or unauthorized devices are connected to the OT/ICS networks must be performed.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
2-11-1-9	Cybersecurity Event Logs and Monitoring Management	OT/ICS Threat Intelligence must be used and incorporated to regularly tune and refresh alerts of Security Information and Event Management (SIEM) technologies.	Functional	Intersects With	Analyze and Prioritize Monitoring Requirements	MON-01.16	Mechanisms exist to assess the organization's needs for monitoring and prioritize the monitoring of Technology Assets, Applications and/or Services (TAAS), based on TAAS criticality and the sensitivity of the data it stores, transmits and processes.	5	
2-11-1-9	Cybersecurity Event Logs and Monitoring Management	OT/ICS Threat Intelligence must be used and incorporated to regularly tune and refresh alerts of Security Information and Event Management (SIEM) technologies.	Functional	Intersects With	Audit Level Adjustments	MON-02.6	Mechanisms exist to adjust the level of audit review, analysis and reporting based on evolving threat information from law enforcement, industry associations or other credible sources of threat intelligence.	5	
2-11-1-10	Cybersecurity Event Logs and Monitoring Management	All access control points between the network security boundaries and external connections must be monitored.	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	
2-11-2	Cybersecurity Event Logs and Monitoring Management	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.	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	
2-11-2	Cybersecurity Event Logs and Monitoring Management	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.	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
2-12	Cybersecurity Incident and Threat Management	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-12-1	Cybersecurity Incident and Threat Management	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:	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
2-12-1-1	Cybersecurity Incident and Threat Management	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).	Functional	Intersects With	Coordinate with Related Plans	BCD-01.1	Mechanisms exist to coordinate contingency plan development with internal and external elements responsible for related plans.	5	
2-12-1-1	Cybersecurity Incident and Threat Management	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).	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
2-12-1-2	Cybersecurity Incident and Threat Management	Formal incident response and root cause analysis for any detected cybersecurity incidents must be conducted.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5	
2-12-1-3	Cybersecurity Incident and Threat Management	Sequence of incident response activities necessary to restore normal operations must be defined.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
2-12-1-3	Cybersecurity Incident and Threat Management	Sequence of incident response activities necessary to restore normal operations must be defined.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
2-12-1-4	Cybersecurity Incident and Threat Management	Incident communications plan must be established.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
2-12-1-4	Cybersecurity Incident and Threat Management	Incident communications plan must be established.	Functional	Intersects With	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	5	
2-12-1-5	Cybersecurity Incident and Threat Management	OT/ICS including Safety Instrumented Systems (SIS) recovery procedures must be included in the incident response, system recovery plans, and business continuity plans.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
2-12-1-6	Cybersecurity Incident and Threat Management	Trainings and skillsets for the organization's personnel (including employees, contractors and subcontractors) to respond to OT/ICS cybersecurity incidents must be provided.	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	5	
2-12-1-7	Cybersecurity Incident and Threat Management	Cybersecurity incident response capabilities, readiness, and plan must be periodically tested by performing cyber-attack simulations exercises.	Functional	Intersects With	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5	
2-12-1-8	Cybersecurity Incident and Threat Management	Threat Intelligence information must be used to identify Tactics, Techniques, and Procedures (TTPs) of activity groups targeting OT/ICS systems.	Functional	Subset Of	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	10	
2-12-1-8	Cybersecurity Incident and Threat Management	Threat Intelligence information must be used to identify Tactics, Techniques, and Procedures (TTPs) of activity groups targeting OT/ICS systems.	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
2-12-2	Cybersecurity Incident and Threat Management	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.	Functional	Intersects With	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	5	
2-12-2	Cybersecurity Incident and Threat Management	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.	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
2-13	Physical Security	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
2-13-1	Physical Security	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:	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
2-13-1-1	Physical Security	List of personnel with authorized access to facilities and sensitive locations where OT/ICS assets reside must be maintained.	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	5	
2-13-1-2	Physical Security	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.	Functional	Intersects With	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	5	
2-13-1-2	Physical Security	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.	Functional	Intersects With	Intrusion Alarms / Surveillance Equipment	PES-05.1	Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.	5	
2-13-1-3	Physical Security	Physical access points and perimeter to sensitive OT/ICS areas shall be protected and ensure continuous monitoring.	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
2-13-1-4	Physical Security	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.	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Saudi Arabia - Operational Technology Cybersecurity Controls (OTCC - 1: 2022)
Focal Document URL: https://nca.gov.sa/otcc_en.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-otcc-1-2022.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2-13-1-5	Physical Security	Strict limitation must be enforced on the physical access to all OT/ICS assets, including Safety Instrumented Systems (SIS).	Functional	Intersects With	Access To Critical Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical systems or sensitive and/or regulated data, in addition to the physical access controls for the facility.	5	
2-13-1-6	Physical Security	Visitor access records to restricted locations where OT/ ICS reside must be maintained.	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	
2-13-1-7	Physical Security	Work being performed by contractor or vendor personnel must be monitored.	Functional	Intersects With	Monitoring Physical Access To Critical Systems	PES-05.2	Facility security mechanisms exist to monitor physical access to critical systems or sensitive and/or regulated data, in addition to the physical access monitoring of the facility.	5	
2-13-1-8	Physical Security	Trainings and skillsets for the organizational security guards must be provided in line with roles and responsibilities with respect to OT/ICS physical security.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
2-13-1-8	Physical Security	Trainings and skillsets for the organizational security guards must be provided in line with roles and responsibilities with respect to OT/ICS physical security.	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	
2-13-1-9	Physical Security	Physical security capabilities and readiness must be periodically tested by performing simulation exercises (such as social engineering).	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
2-13-2	Physical Security	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.	Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5	
2-13-2	Physical Security	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.	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
3	Cybersecurity Resilience	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
3-1	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
3-1-1	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	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:	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
3-1-1	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	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:	Functional	Intersects With	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	5	
3-1-1-1	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	Activities necessary to sustain minimum operations of the OT/ICS systems must be defined.	Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-01.4	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
3-1-1-1	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	Activities necessary to sustain minimum operations of the OT/ICS systems must be defined.	Functional	Intersects With	Achieving Resilience Requirements	SEA-01.2	Mechanisms exist to achieve resilience requirements in normal and adverse situations.	5	
3-1-1-2	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	Redundant OT/ICS networks, connections, and devices must be implemented in accordance to the periodic cybersecurity risk assessment.	Functional	Intersects With	Redundant Secondary System	BCD-11.7	Mechanisms exist to maintain a failover capability, which is not collocated with the primary Technology Asset, Application and/or Service (TAAS), which can be activated with little-to-no loss of information or disruption to operations.	3	
3-1-1-3	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	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).	Functional	Intersects With	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-01.7	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	8	
3-1-1-4	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	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.	Functional	Intersects With	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-01.7	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	8	
3-1-1-5	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	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.	Functional	Intersects With	Continue Essential Mission & Business Functions	BCD-02.2	Mechanisms exist to continue essential missions and business functions with little or no loss of operational continuity and sustain that continuity until full system restoration at primary processing and/or storage sites.	5	
3-1-1-5	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	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.	Functional	Intersects With	Resume Essential Missions & Business Functions	BCD-02.3	Mechanisms exist to resume essential missions and business functions within an organization-defined time period of contingency plan activation.	5	
3-1-1-6	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	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.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	
3-1-2	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	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.	Functional	Intersects With	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	5	
3-1-2	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	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.	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
4	Third-Party Cybersecurity	N/A	Functional	No Relationship	N/A	N/A	N/A	0	
4-1	Third-Party Cybersecurity	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	
4-1-1	Third-Party Cybersecurity	In addition to the ECC subcontrols within controls 4-1-2 and 4-13, cybersecurity requirements for third-party cybersecurity in OT/ ICS must include, at a minimum, the following:	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
4-1-1-1	Third-Party Cybersecurity	Cybersecurity requirements are included during procurement lifecycle for OT/ICS products and services.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
4-1-1-2	Third-Party Cybersecurity	Cybersecurity requirements for third-party evaluation, selection, and information sharing must be defined.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	
4-1-1-3	Third-Party Cybersecurity	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.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
4-1-1-4	Third-Party Cybersecurity	Periodic cybersecurity assessment and audits of third-party providers must be conducted to ensure the mitigation of any identified cyber threats.	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5	
4-1-2	Third-Party Cybersecurity	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.	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Saudi Arabia - Operational Technology Cybersecurity Controls (OTCC - 1: 2022)
Focal Document URL: https://nca.gov.sa/otcc_en.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-sau-otcc-1-2022.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
4-1-2	Third-Party Cybersecurity	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.	Functional	Intersects With	Control Conformity Monitoring	CPL-03	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	