ISA99 Committee on the Security of Industrial Automation and Control Systems (IACS)

Comments on NIST CSF 2.0

Date: November 30, 2023
To: National Institute of Standards and Technology, US Dept of Commerce
RE: Comments on NIST CSF 2.0

Thank you for the opportunity to submit comments on the NIST Cybersecurity Framework version 2.0, dated August 8, 2023.

The International Society of Automation (ISA) is an ANSI-accredited standards development organization. The ISA99 Standards and Practices Committee is responsible for developing the ISA/IEC 62443 series of standards for the Security of Industrial Automation and Control Systems (IACS). The development of the ISA/IEC 62443 series of standards is a collaborative effort between the ISA99 Standards and Practices Committee and the IEC TC65 WG10 Committee. This work complements the work of other standards organizations working in cybersecurity such as the ISO 27000 family of standards for Information Technology[1].

The comments and opinions that follow are those of a working group within the ISA99 Committee that was responsible for reviewing the NIST Cybersecurity Framework v2.0. These comments and opinions have not been reviewed and approved by the full ISA99 Committee.

Johan B. Nye
Eric Cosman
ISA99 Co-Chairs

[1] https://www.iso.org/standard/iso-iec-27000-family

ISA99 Committee on the Security of Industrial Automation and Control Systems (IACS) Comments on NIST CSF 2.0

1 Introduction

An Industrial Automation and Control System (IACS) is a system designed to monitor and control physical entities such as machinery, industrial processes, and manufacturing processes. Similar terms include Operational Technology, Industrial Control Systems, SCADA Systems, and Safety Instrumented Systems. While the term IACS includes the term *Industrial*, these systems are used in most of the Critical Infrastructure Sectors identified by the US Cybersecurity & Infrastructure Security Agency (CISA).

The fundamental difference between Information Systems and Industrial Automation and Control Systems is that failure or compromise of the latter may result in *physical consequences*. Physical consequences can include but are not limited to: the loss of the health and safety of persons, damage to the environment, damage to equipment, loss of production, and loss of product quality and integrity. This fundamental difference affects most aspects of cybersecurity such as the risk assessment process, the rigor of management of change processes, and incident management may also require emergency response.

The NATO Energy Security Centre of Excellence has produced a *Guide for Protecting Industrial Automation and Control Systems Against Cyber Incidents in Critical Energy Infrastructure*[2] which provides background and guidance on securing IACS with a focus on NATO pipeline systems.

The comments submitted are from the point of view of a user of an IACS (asset owner, service provider or product supplier) that wishes to implement a security program based on NIST CSF 2.0.

2 General Comments

2.1 Change in scope from Critical Infrastructure

There is a concern that the change in scope of the CSF from a focus on critical infrastructure organizations to a focus on all organizations may weaken the CSF for use with Industrial Automation and Control Systems. While the scope states that it includes Operations Technology, the reader of CSF 2.0 is left with the overwhelming impression that CSF 2.0 is focused on Information Technology, since there are very few references to physical consequences or the protection of health, safety, and the environment.

2.2 Health, Safety, and the Environment (HSE)

There is a lack of emphasis in CSF 2.0 on the protection of health, safety, and the environment. For example, the term Information is used 49 times in the Core Framework document, while the term safety is used 2 times, and the term physical is used 7 times. While the scope of the CSF includes Operational Technology, after reading the document, the IACS practitioner may be left with the impression that this document does not sufficiently address the requirements for an IACS security program.

[2] https://www.enseccoe.org/data/public/uploads/2022/01/d1_guide-for-protecting-industrial-automation-and-control-systems-against-cyber-incidents.pdf

2.3 Ease of Use

NIST CSF 2.0 Functions, Categories, and Subcategories have embedded the change list from CSF 1.1 to CSF 2.0 within the Framework. While this may be advantageous for the existing user of CSF 1.1, it is confusing to a new user of CSF 2.0. For example, when the CSF 1.1 dropped or moved Categories and Subcategories are removed from the list, there are gaps in sequences. Recommend publishing a clean version of CSF 2.0 (without gaps) and a separate change list from CSF 1.1 to 2.0 for existing users.

2.4 Terminology

NIST CSF 1.1 included a glossary of terms, but this appears to be missing in NIST CSF 2.0. A reference to the NIST Glossary could be provided, however, the NIST Glossary is heavily oriented towards information systems, and the definitions there typically do not include physical consequences.

It is recommended that, at a minimum, the following terms are defined by reference or in the document: essential function, industrial automation and control system, information technology, operations technology, safety instrumented system, security control/measure.

The term “operations” is used throughout the document. This term could refer to IT operations or OT operations or both. Clarify the definition of this term or use IT operations and OT operations consistently throughout the document. Our comments assume that “operations” could apply to “operations technology”.

3 Core Framework document

3.1 Scope (lines 138-143)

The Framework’s scope as described in lines 138-143 is too wide to act as a guide for many industrial and manufacturing operations. Besides contradicting an earlier statement made on lines 98-99 that this “voluntary Framework is not a one-size-fits-all approach to managing cybersecurity risks” there are many important caveats that need to be considered in operations of critical infrastructure that will make it difficult for operators of critical infrastructure to apply.

It is recommended that an important distinction be made in the Framework’s recommendations that clearly differentiate and accommodate the cybersecurity concerns found in IT and OT operating environments. A recommended cybersecurity practice in one domain may not apply well in others. For example for a power utility the process used to patch and update software in the utilities’ billing department may not apply well to the utilities’ control room that is monitoring and controlling the operations of a regional power grid. Different patching policies may need to be applied in real-time systems that require suspending operations for testing and applying the patch first to avoid catastrophic failure. ISA/IEC 62443-2-3 offers guidance on employing patching policies in IACS environments. ISA/IEC 62443-3-3 provides guidance in determining and protecting high risk communication conduits and security zones to protect the confidentiality, integrity, availability, and safety of critical IACS automation, control and safety systems.

3.2 Primary audience (lines 150-157)

The Framework's primary audience as stated in line 150 is for "those responsible for developing and leading a cybersecurity program". While this statement is appropriate, it should be recognized that responsibility for cybersecurity may reside in multiple roles in an organization. For example, a Chief Information Security Officer (CISO) may have responsibility for Information Technology Systems, and a Plant/Facility Manager may have responsibility for Operations Technology Systems. The CSF should make it clear that multiple roles within the organization may have responsibility for developing and leading cybersecurity programs.

3.3 Rename Identify Function

The Identify Function is often confused with the Protect Function: Identity Management, Authentication and Access Control Category (PR.AA). Since the Categories in Identify are Asset Management, Risk Assessment, and Improvement a better choice could be "Prepare" or "Manage".

3.4 Response Function

The Response Function is currently focused on responding to incidents where information is compromised and does not include incidents with physical consequences which may require emergency response.

Incident Command System for Industrial Control Systems (ICS4ICS)[3] is designed to improve Industrial Control System cybersecurity incident management capabilities. ICS4ICS leverages the Incident Command System, as outlined by FEMA, for response structure, roles, and interoperability. It should be used as a basis for cybersecurity incident management where physical consequences are possible.

3.5 Recovery Function

The Recovery Function is currently focused on recovering from incidents where information is compromised and does not include incidents with physical consequences which may require recovery of manufacturing or production equipment.

3.6 Integrating Cybersecurity Framework with a Health/Safety/Environment Framework

Section 4 includes recommendations for integrating the Cybersecurity Framework with the Privacy Framework and Risk Management Framework. However, a discussion of the integration of the Cybersecurity Framework with a Health/Safety/Environment Framework is missing from CSF 2.0. While the Enterprise Risk Management Framework includes "safety" in its scope, there are only two references to the term safety in NIST IR 8286. This is not sufficient for an Operations Technology implementation of CSF 2.0.

[3] https://www.ics4ics.org

IEC 63069 *Framework for functional safety and security*, and ISA-TR84.00.09 *Cybersecurity related to the Functional Safety Lifecycle* provide guidance on the integration of cybersecurity and safety lifecycles. The ISA84 Standards Committee is currently working on a second edition of ISA-TR84.00.09.

3.7 Essential Functions concept

The ISA/IEC 62443 series of standards includes a concept called *Essential Functions*, which is a *function or capability that is required to maintain health, safety, the environment, and availability for the equipment under control. Essential functions include, but are not limited to, the safety instrumented function (SIF), the control function, and the ability of the operator to view and manipulate the equipment under control. The loss of essential functions is commonly termed loss of protection, loss of control, and loss of view respectively. In some industries, additional functions such as history may be considered essential.*

This concept allows the IACS practitioner to identify those functions that are essential to protecting health, safety, the environment, and the means of production and prioritizing the security protections for those functions. There is also guidance that security measures such as access control can not prevent an essential function from operating. This concept is not present in CSF 2.0.

3.8 Zone and Conduit Partitioning concept

Included in the risk assessment process described in ISA/IEC 62443-3-2 is the concept of partitioning the IACS into Security Zones and Conduits (communications between Zones). The concept is similar to network segmentation but takes it further by incorporating it into the risk assessment process and defining criteria when assets should be grouped into separate Zones. For example, IT Systems and OT Systems are required to be in separate Zones, and Safety Zones are required to be separated from all other types of Zones. This concept is not sufficiently covered in CSF 2.0.

4 Implementation Examples document

Detailed comments on the Implementation Examples document can be found in Annex A. Annex A includes Informative References to ISA/IEC 62443 documents, an assessment of applicability of a Function/Category/Subcategory to OT Systems, and recommended changes to Functions, Categories, Subcategories, or Implementation Examples.

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Organizational Context (GV.OC)**: The circumstances - mission, stakeholder expectations, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood (formerly ID.BE)	**GV.OC-01**: The organizational mission is understood and informs cybersecurity risk management (formerly ID.BE-02, ID.BE-03)	**Ex1**: Share the organization's mission (e.g., through vision and mission statements, marketing, and service strategies) to provide a basis for identifying risks that may impede that mission		Applies as is	
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Organizational Context (GV.OC)**: The circumstances - mission, stakeholder expectations, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood (formerly ID.BE)	**GV.OC-02**: Internal and external stakeholders are determined, and their needs and expectations regarding cybersecurity risk management are understood	**Ex1**: Identify relevant internal stakeholders and their cybersecurity-related expectations (e.g., performance and risk expectations of officers, directors, and advisors; cultural expectations of employees) **Ex2**: Identify relevant external stakeholders and their cybersecurity-related expectations (e.g., privacy expectations of customers, business expectations of partnerships, compliance expectations of regulators, ethics expectations of society)		Applies as is	

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Organizational Context (GV.OC)**: The circumstances - mission, stakeholder expectations, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood (formerly ID.BE)	**GV.OC-03**: Legal, regulatory, and contractual requirements regarding cybersecurity - including privacy and civil liberties obligations - are understood and managed (formerly ID.GV-03)	**Ex1**: Determine a process to track and manage legal and regulatory requirements regarding protection of individuals' information (e.g., Health Insurance Portability and Accountability Act, California Consumer Privacy Act, General Data Protection Regulation) **Ex2**: Determine a process to track and manage contractual requirements for cybersecurity management of supplier, customer, and partner information **Ex3**: Align the organization's cybersecurity strategy with legal, regulatory, and contractual requirements		Applies as is	
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Organizational Context (GV.OC)**: The circumstances - mission, stakeholder expectations, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood (formerly ID.BE)	**GV.OC-04**: Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are determined and communicated (formerly ID.BE-04, ID.BE-05)	**Ex1**: Establish criteria for determining the criticality of capabilities and services as viewed by internal and external stakeholders **Ex2**: Determine (e.g., from a business impact analysis) assets and business operations that are vital to achieving mission objectives and the potential impact of a loss (or partial loss) of such operations **Ex3**: Establish and communicate resilience objectives (e.g., recovery time objectives) for delivering critical capabilities and services in various operating states (e.g., under attack, during recovery, normal operation)	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-4-1	Applies but needs change	Add Ex4: Determine critical and essential functions for cyber-physical systems and the potential impact of loss of these functions

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Organizational Context (GV.OC)**: The circumstances - mission, stakeholder expectations, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood (formerly ID.BE)	**GV.OC-05**: Outcomes, capabilities, and services that the organization depends on are determined and communicated (formerly ID.BE-01, ID.BE-04)	**Ex1**: Create an inventory of the organization's dependencies on external resources (e.g., facilities, cloud-based hosting providers) and their relationships to organizational assets and business functions **Ex2**: Identify and document external dependencies that are potential points of failure for the organization's critical capabilities and services	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-4-1	Applies as is	
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Risk Management Strategy (GV.RM)**: The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions (formerly ID.RM)	**GV.RM-01**: Risk management objectives are established and agreed to by organizational stakeholders (formerly ID.RM-01)	**Ex1**: Update near-term and long-term cybersecurity risk management objectives as part of annual strategic planning and when major changes occur **Ex2**: Establish measurable objectives for cybersecurity risk management (e.g., manage the quality of user training, ensure adequate risk protection for industrial control systems) **Ex3**: Senior leaders agree about cybersecurity objectives and use them for measuring and managing risk and performance	ISA-62443-2-1 ISA-62443-3-2	Applies as is	
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Risk Management Strategy (GV.RM)**: The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions (formerly ID.RM)	**GV.RM-02**: Risk appetite and risk tolerance statements are determined, communicated, and maintained (formerly ID.RM-02, ID.RM-03)	**Ex1**: Determine and communicate risk appetite statements that convey expectations about the appropriate level of risk for the organization **Ex2**: Translate risk appetite statements into specific, measurable, and broadly understandable risk tolerance statements **Ex3**: Refine organizational objectives and risk appetite	ISA-62443-2-1 ISA-62443-3-2	Applies as is	

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
			periodically based on known risk exposure and residual risk			
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Risk Management Strategy (GV.RM)**: The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions (formerly ID.RM)	**GV.RM-03**: Enterprise risk management processes include cybersecurity risk management activities and outcomes (formerly ID.GV-04)	**Ex1**: Aggregate and manage cybersecurity risks alongside other enterprise risks (e.g., compliance, financial, regulatory) **Ex2**: Include cybersecurity risk managers in enterprise risk management planning **Ex3**: Establish criteria for escalating cybersecurity risks within enterprise risk management	ISA-62443-2-1 ISA-62443-3-2	Applies but needs change	Add Ex4: Aggregate and manage cybersecurity risks for cyber-physical systems (e.g. safety, health, environmental protection, equipment protection, product integrity) Add Ex5: Integrate safety and cybersecurity risk management processes for cyber-physical critical and essential functions
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Risk Management Strategy (GV.RM)**: The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions (formerly ID.RM)	**GV.RM-04**: Strategic direction that describes appropriate risk response options is established and communicated	**Ex1**: Specify criteria for accepting and avoiding cybersecurity risk for various classifications of data **Ex2**: Determine whether to purchase cybersecurity insurance **Ex3**: Document conditions under which shared responsibility models are acceptable (e.g., outsourcing certain cybersecurity functions, having a third party perform financial transactions on behalf of the organization, using public cloud-based services)	ISA-62443-2-1 ISA-62443-3-2	Applies but needs change	Add Ex4: Specify criteria for accepting and avoiding cybersecurity cyber-physical risk

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Risk Management Strategy (GV.RM)**: The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions (formerly ID.RM)	**GV.RM-05**: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	**Ex1**: Determine how to update senior executives, directors, and management on the organization's cybersecurity posture at agreed-upon intervals **Ex2**: Identify how all departments across the organization - such as management, internal auditors, legal, acquisition, physical security, and HR - will communicate with each other about cybersecurity risks **Ex3**: Identify how third parties will communicate with the organization about cybersecurity risks		Applies but needs change	Not only senior executives need to be updated. The term "operations personnel "used in GV SC 09 , should be added to Ex2 for completeness.
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Risk Management Strategy (GV.RM)**: The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions (formerly ID.RM)	**GV.RM-06**: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	**Ex1**: Establish criteria for using a quantitative approach to cybersecurity risk analysis, and specify probability and exposure formulas **Ex2**: Create and use templates (e.g., a risk register) to document cybersecurity risk information (e.g., risk description, exposure, treatment, and ownership) **Ex3**: Establish criteria for risk prioritization at the appropriate levels within the enterprise **Ex4**: Use a consistent list of risk categories to support integrating, aggregating, and comparing cybersecurity risks	ISA-62443-2-1 ISA-62443-3-2	Applies but needs change	Add Ex5: Include cyber-physical risk categories such as safety, health, environmental protection, equipment protection, and operational availability
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Risk Management Strategy (GV.RM)**: The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational	**GV.RM-07**: Strategic opportunities (i.e., positive risks) are identified and included in organizational cybersecurity risk discussions	**Ex1**: Define and communicate guidance and methods for identifying opportunities and including them in risk discussions (e.g., strengths, weaknesses, opportunities, and threats [SWOT] analysis) **Ex2**: Identify stretch goals and document them		Applies as is	

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
	risk decisions (formerly ID.RM)		**Ex3**: Calculate, document, and prioritize positive risks alongside negative risks			
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Cybersecurity Supply Chain Risk Management (GV.SC)**: Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders (formerly ID.SC)	**GV.SC-01**: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders (formerly ID.SC-01)	**Ex1**: Establish a strategy that expresses the objectives of the cybersecurity supply chain risk management program **Ex2**: Develop the cybersecurity supply chain risk management program, including a plan (with milestones), policies, and procedures that guide implementation and improvement of the program, and share the policies and procedures with the organizational stakeholders **Ex3**: Develop and implement program processes based on the strategy, objectives, policies, and procedures that are agreed upon and performed by the organizational stakeholders **Ex4**: Establish a cross-organizational mechanism that ensures alignment between functions that contribute to cybersecurity supply chain risk management, such as cybersecurity, IT, legal, human resources, and engineering	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-4-1	Applies but needs change	Add "operations" to the list of functions in Ex4

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Cybersecurity Supply Chain Risk Management (GV.SC)**: Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders (formerly ID.SC)	**GV.SC-02**: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally (formerly ID.AM-06)	**Ex1**: Identify one or more specific roles or positions that will be responsible and accountable for planning, resourcing, and executing cybersecurity supply chain risk management activities **Ex2**: Document cybersecurity supply chain risk management roles and responsibilities in policy **Ex3**: Create responsibility matrixes to document who will be responsible and accountable for cybersecurity supply chain risk management activities and how those teams and individuals will be consulted and informed **Ex4**: Include cybersecurity supply chain risk management responsibilities and performance requirements in personnel descriptions to ensure clarity and improve accountability **Ex5**: Document performance goals for personnel with cybersecurity risk management-specific responsibilities, and periodically measure them to demonstrate and improve performance **Ex6**: Develop roles and responsibilities for suppliers, customers, and business partners to address shared responsibilities for applicable cybersecurity risks, and integrate them into organizational policies and applicable third-party agreements **Ex7**: Internally communicate cybersecurity supply chain risk management roles and responsibilities for third parties	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-4-1	Applies as is	

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
			Ex8: Establish rules and protocols for information sharing and reporting processes between the organization and its suppliers			
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Cybersecurity Supply Chain Risk Management (GV.SC)**: Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders (formerly ID.SC)	**GV.SC-03**: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes (formerly ID.SC-02)	**Ex1**: Identify areas of alignment and overlap with cybersecurity and enterprise risk management **Ex2**: Establish integrated control sets for cybersecurity risk management and cybersecurity supply chain risk management **Ex3**: Integrate cybersecurity supply chain risk management into improvement processes **Ex4**: Escalate material cybersecurity risks in supply chains to senior	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-4-1	Applies as is	

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
			management, and address them at the enterprise risk management level			
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Cybersecurity Supply Chain Risk Management (GV.SC)**: Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders (formerly ID.SC)	**GV.SC-04**: Suppliers are known and prioritized by criticality	**Ex1**: Develop criteria for supplier criticality based on, for example, the sensitivity of data processed or possessed by suppliers, the degree of access to the organization's systems, and the importance of the products or services to the organization's mission **Ex2**: Keep a record of all suppliers, and prioritize suppliers based on the criticality criteria	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-4-1	Applies but needs change	Add "the impact on operations" to the list in Ex1

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Cybersecurity Supply Chain Risk Management (GV.SC)**: Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders (formerly ID.SC)	**GV.SC-05**: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties (formerly ID.SC-03)	**Ex1**: Establish security requirements for suppliers, products, and services commensurate with their criticality level and potential impact if compromised **Ex2**: Include all cybersecurity and supply chain requirements that third parties must follow and how compliance with the requirements may be verified in default contractual language **Ex3**: Define the rules and protocols for information sharing between the organization and its suppliers and sub-tier suppliers in contracts **Ex4**: Manage risk by including security requirements in contracts based on their criticality and potential impact if compromised **Ex5**: Define security requirements in service-level agreements (SLAs) for monitoring suppliers for acceptable security performance throughout the supplier relationship lifecycle **Ex6**: Contractually require suppliers to disclose cybersecurity features, functions, and vulnerabilities of their products and services for the life of the product or the term of service **Ex7**: Contractually require suppliers to provide and maintain a current component inventory (e.g., software or hardware bill of materials) for critical products **Ex8**: Contractually require suppliers to vet their employees and guard against insider threats **Ex9**: Contractually require suppliers to provide evidence of performing	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-4-1	Applies as is	

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
			acceptable security practices through, for example, self-attestation, conformance to known standards, certifications, or inspections **Ex10**: Specify in contracts the rights and responsibilities of the organization, its suppliers, and applicable lower-tier suppliers and supply chains, with respect to potential cybersecurity risks			

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Cybersecurity Supply Chain Risk Management (GV.SC)**: Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders (formerly ID.SC)	**GV.SC-06**: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships	**Ex1**: Perform thorough due diligence on prospective suppliers that is consistent with procurement planning and commensurate with the level of risk, criticality, and complexity of each supplier relationship **Ex2**: Assess the suitability of the technology and cybersecurity capabilities and the risk management practices of prospective suppliers **Ex3**: Conduct supplier risk assessments against business and applicable cybersecurity requirements, including lower-tier suppliers and the supply chain for critical suppliers **Ex4**: Assess the authenticity, integrity, and security of critical products prior to acquisition and use		Applies as is	
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Cybersecurity Supply Chain Risk Management (GV.SC)**: Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders (formerly ID.SC)	**GV.SC-07**: The risks posed by a supplier, their products and services, and other third parties are identified, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship (formerly ID.SC-02, ID.SC-04)	**Ex1**: Adjust assessment formats and frequencies based on the third party's reputation and the criticality of the products or services they provide **Ex2**: Evaluate third parties' evidence of compliance with contractual cybersecurity requirements, such as self-attestations, warranties, certifications, and other artifacts **Ex3**: Monitor critical suppliers to ensure that they are fulfilling their security obligations throughout the supplier relationship lifecycle using a variety of methods and techniques, such as inspections, audits, tests, or other forms of evaluation	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-4-1	Applies as is	

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
			Ex4: Monitor critical suppliers, services, and products for changes to their risk profiles, and reevaluate supplier criticality and risk impact accordingly **Ex5**: Plan for unexpected supplier and supply chain-related interruptions to ensure business continuity			
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Cybersecurity Supply Chain Risk Management (GV.SC)**: Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders (formerly ID.SC)	**GV.SC-08**: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities (formerly ID.SC-05)	**Ex1**: Define and use rules and protocols for reporting incident response and recovery activities and the status between the organization and its suppliers **Ex2**: Identify and document the roles and responsibilities of the organization and its suppliers for incident response **Ex3**: Include critical suppliers in incident response exercises and simulations **Ex4**: Define and coordinate crisis communication methods and protocols between the organization and its critical suppliers **Ex5**: Conduct collaborative lessons learned sessions with critical suppliers	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-4-1	Applies as is	

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Cybersecurity Supply Chain Risk Management (GV.SC)**: Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders (formerly ID.SC)	**GV.SC-09**: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle	**Ex1**: Policies and procedures require provenance records for all acquired technology products and services **Ex2**: Periodically provide risk reporting to leaders about how acquired components are proven to be untampered and authentic. **Ex3**: Communicate regularly among cybersecurity risk managers and operations personnel about the need to acquire software patches, updates, and upgrades only from authenticated and trustworthy software providers **Ex4**: Review policies to ensure that they require approved supplier personnel to perform maintenance on supplier products **Ex5**: Policies and procedure require checking upgrades to critical hardware for unauthorized changes	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-4-1	Applies but needs change	Add Ex6: Review product suppliers vulnerability disclosure and product update processes to ensure timely availability and mitigation of cybersecurity vulnerabilities
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Cybersecurity Supply Chain Risk Management (GV.SC)**: Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders (formerly ID.SC)	**GV.SC-10**: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement	**Ex1**: Establish processes for terminating critical relationships under both normal and adverse circumstances **Ex2**: Define and implement plans for component end-of-life maintenance support and obsolescence **Ex3**: Verify that supplier access to organization resources is deactivated promptly when it is no longer needed **Ex4**: Verify that assets containing the organization's data are returned or properly disposed of in a timely, controlled, and safe manner **Ex5**: Develop and execute a plan for terminating or transitioning supplier relationships that takes supply		Applies as is	

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
			chain security risk and resiliency into account **Ex6**: Mitigate risks to data and systems created by supplier termination **Ex7**: Manage data leakage risks associated with supplier termination			
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Roles, Responsibilities, and Authorities (GV.RR)**: Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated (formerly ID.GV-02)	**GV.RR-01**: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving	**Ex1**: Leaders (e.g., directors) agree on their roles and responsibilities in developing, implementing, and assessing the organization's cybersecurity strategy **Ex2**: Share leaders' expectations regarding a secure and ethical culture, especially when current events present the opportunity to highlight positive or negative examples of cybersecurity risk management **Ex3**: Leaders direct the CISO to maintain a comprehensive cybersecurity risk strategy and review and update it at least annually and after major events **Ex4**: Conduct reviews to ensure adequate authority and coordination among those	ISA-62443-2-1 ISA-62443-2-4 ISA-62443-4-1	Applies but needs change	Add Ex5: Foster a cybersecurity culture in the operational and engineering functions within the organization Modify Ex3: Leaders direct the appropriate senior leadership to maintain a comprehensive cybersecurity risk strategy…

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
			responsible for managing cybersecurity risk			
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Roles, Responsibilities, and Authorities (GV.RR)**: Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated (formerly ID.GV-02)	**GV.RR-02**: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced (formerly ID.AM-06, ID.GV-02, DE.DP-01)	**Ex1**: Document risk management roles and responsibilities in policy **Ex2**: Document who is responsible and accountable for cybersecurity risk management activities and how those teams and individuals are to be consulted and informed **Ex3**: Include cybersecurity responsibilities and performance requirements in personnel descriptions **Ex4**: Document performance goals for personnel with cybersecurity risk management responsibilities, and periodically measure performance to identify areas for improvement **Ex5**: Clearly articulate cybersecurity responsibilities within operations, risk functions, and internal audit functions	ISA-62443-2-1 ISA-62443-2-4 ISA-62443-4-1	Applies as is	

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Roles, Responsibilities, and Authorities (GV.RR)**: Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated (formerly ID.GV-02)	**GV.RR-03**: Adequate resources are allocated commensurate with cybersecurity risk strategy, roles and responsibilities, and policies	**Ex1**: Conduct periodic management reviews to ensure that those given cybersecurity risk management responsibilities have the necessary authority **Ex2**: Identify resource allocation and investment in line with risk tolerance and response **Ex3**: Provide adequate and sufficient people, process, and technical resources to support the cybersecurity strategy	ISA-62443-2-1 ISA-62443-2-4 ISA-62443-4-1	Applies but needs change	Add Ex4: The management review should include input about the current threat environment or information about significant incidents that have occurred in similar operations.
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Roles, Responsibilities, and Authorities (GV.RR)**: Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated (formerly ID.GV-02)	**GV.RR-04**: Cybersecurity is included in human resources practices (formerly PR.IP-11)	**Ex1**: Integrate cybersecurity risk management considerations into human resources processes (e.g., personnel screening, onboarding, change notification, offboarding) **Ex2**: Consider cybersecurity knowledge to be a positive factor in hiring, training, and retention decisions **Ex3**: Conduct background checks prior to onboarding new personnel for sensitive roles **Ex4**: Define and enforce obligations for personnel to be aware of, adhere to, and uphold security policies as they relate to their roles		Applies but needs change	Add Ex5: For cyber-physical systems ensure that personnel have knowledge about physical operations and their consequences.

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Policies, Processes, and Procedures (GV.PO)**: Organizational cybersecurity policies, processes, and procedures are established, communicated, and enforced (formerly ID.GV-01)	**GV.PO-01**: Policies, processes, and procedures for managing cybersecurity risks are established based on organizational context, cybersecurity strategy, and priorities and are communicated and enforced (formerly ID.GV-01)	**Ex1**: Create, disseminate, and maintain a risk management policy with statements of management intent, expectations, and direction **Ex2**: Periodically review policies and procedures to ensure that they align with risk management strategy objectives and priorities, as well as the high-level direction of the cybersecurity policy **Ex3**: Require approval from senior management on policies **Ex4**: Communicate cybersecurity risk management policies, procedures, and processes across the organization **Ex5**: Require personnel to acknowledge receipt of policies when first hired, annually, and whenever a policy is updated	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-4-1	Applies as is	
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Policies, Processes, and Procedures (GV.PO)**: Organizational cybersecurity policies, processes, and procedures are established, communicated, and enforced (formerly ID.GV-01)	**GV.PO-02**: Policies, processes, and procedures for managing cybersecurity risks are reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission (formerly ID.GV-01)	**Ex1**: Update policies based on periodic reviews of cybersecurity risk management results to ensure that policies and supporting processes adequately maintain risk at an acceptable level **Ex2**: Provide a timeline for reviewing changes to the organization's risk environment (e.g., changes in risk or in the organization's mission objectives), and communicate recommended policy updates **Ex3**: Update policies to reflect changes in legal and regulatory requirements **Ex4**: Update policies to reflect changes in technology (e.g., adoption of artificial intelligence) and changes to the business (e.g.,	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-4-1	Applies but needs change	Add Ex 5: Update policies to reflect changes in the threat environment

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
			acquisition of a new business, new contract requirements)			
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Oversight (GV.OV)**: Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy	**GV.OV-01**: Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction	**Ex1**: Measure how well the risk management strategy and risk results have helped leaders make decisions and achieve organizational objectives **Ex2**: Examine whether cybersecurity risk strategies that impede operations or innovation should be adjusted	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-4-1	Applies as is	
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Oversight (GV.OV)**: Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy	**GV.OV-02**: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks	**Ex1**: Review audit findings to confirm whether the existing cybersecurity strategy has ensured compliance with internal and external requirements **Ex2**: Review the performance oversight of those in cybersecurity-related roles to determine whether policy changes are necessary **Ex3**: Review strategy in light of cybersecurity incidents	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-4-1	Applies as is	

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	**Oversight (GV.OV)**: Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy	**GV.OV-03**: Organizational cybersecurity risk management performance is measured and reviewed to confirm and adjust strategic direction	**Ex1**: Review key performance indicators (KPIs) to ensure that organization-wide policies and procedures achieve objectives **Ex2**: Review key risk indicators (KRIs) to identify risks the organization faces, including likelihood and potential impact **Ex3**: Collect and communicate metrics on cybersecurity risk management with senior leadership	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-4-1	Applies as is	

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
IDENTIFY (ID): Help determine the current cybersecurity risk to the organization	**Asset Management (ID.AM)**: Assets (e.g., data, hardware software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy	**ID.AM-01**: Inventories of hardware managed by the organization are maintained	**Ex1**: Maintain inventories for all types of hardware, including IT, IoT, OT, and mobile devices **Ex2**: Constantly monitor networks to detect new hardware and automatically update inventories	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-3-2	Applies but needs change	-

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
IDENTIFY (ID): Help determine the current cybersecurity risk to the organization	**Asset Management (ID.AM)**: Assets (e.g., data, hardware software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy	**ID.AM-02**: Inventories of software, services, and systems managed by the organization are maintained	**Ex1**: Maintain inventories for all types of software and services, including commercial-off-the-shelf, open-source, custom applications, API services, and cloud-based applications and services **Ex2**: Constantly monitor all platforms, including containers and virtual machines, for software and service inventory changes **Ex3**: Maintain an inventory of the organization's systems	ISA 62443-3-2	Applies but needs change	-
IDENTIFY (ID): Help determine the current cybersecurity risk to the organization	**Asset Management (ID.AM)**: Assets (e.g., data, hardware software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy	**ID.AM-03**: Representations of the organization's authorized network communication and internal and external network data flows are maintained (formerly ID.AM-03, DE.AE-01)	**Ex1**: Maintain baselines of communication and data flows within the organization's wired and wireless networks **Ex2**: Maintain baselines of communication and data flows between the organization and third parties **Ex3**: Maintain documentation of expected network ports, protocols, and services that are typically used among authorized systems	ISA 62443-3-2	Applies but needs change	Add Ex4: Maintain documentation of data flows and restrictions between Security Zones Add Ex5: Deviation from expected performance of operations technology equipment under control
IDENTIFY (ID): Help determine the current cybersecurity risk to the organization	**Asset Management (ID.AM)**: Assets (e.g., data, hardware software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the	**ID.AM-04**: Inventories of services provided by suppliers are maintained	**Ex1**: Inventory all external services used by the organization, including third-party infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) offerings; APIs; and other externally hosted application services **Ex2**: Update the inventory when a new external service is going to be utilized to ensure adequate cybersecurity risk management	ISA 62443-2-1 ISA 62443-3-2	Applies but needs change	Add EX3: Inventory all third party remote access to OT systems and assure access complies with security policies

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
	organization's risk strategy		monitoring of the organization's use of that service			
IDENTIFY (ID): Help determine the current cybersecurity risk to the organization	**Asset Management (ID.AM)**: Assets (e.g., data, hardware software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy	**ID.AM-05**: Assets are prioritized based on classification, criticality, resources, and impact on the mission	**Ex1**: Define criteria for prioritizing each class of assets **Ex2**: Apply the prioritization criteria to assets **Ex3**: Track the asset priorities and update them periodically or when significant changes to the organization occur	ISA 62443-2-1 ISA 62443-3-2	Applies but needs change	Add Ex4: Partition OT assets into security zones based on their characteristics such as criticality, function, and administrative organization
IDENTIFY (ID): Help determine the current cybersecurity risk to the organization	**Asset Management (ID.AM)**: Assets (e.g., data, hardware software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy	**ID.AM-07**: Inventories of data and corresponding metadata for designated data types are maintained	**Ex1**: Maintain a list of the designated data types of interest (e.g., personally identifiable information, protected health information, financial account numbers, organization intellectual property) **Ex2**: Continuously discover and analyze ad hoc data to identify new instances of designated data types **Ex3**: Assign data classifications to designated data types through tags or labels **Ex4**: Track the provenance, data owner, and geolocation of each instance of designated data types	ISA 62443-3-2	Applies but needs change	Add Ex5: Classify OT data taking into account risks to operations if the data is compromised

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
IDENTIFY (ID): Help determine the current cybersecurity risk to the organization	**Asset Management (ID.AM)**: Assets (e.g., data, hardware software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy	**ID.AM-08**: Systems, hardware, software, and services are managed throughout their life cycle (formerly PR.DS-03, PR.IP-02, PR.MA-01, PR.MA-02)	**Ex1**: Integrate cybersecurity considerations throughout the life cycles of systems, hardware, software, and services **Ex2**: Integrate cybersecurity considerations into product life cycles **Ex3**: Identify unofficial uses of technology to meet mission objectives (i.e., shadow IT) **Ex4**: Identify redundant systems, hardware, software, and services that unnecessarily increase the organization's attack surface **Ex5**: Properly configure and secure systems, hardware, software, and services prior to their deployment in production **Ex6**: Update inventories when systems, hardware, software, and services are moved or transferred within the organization	ISA 62443-2-1 ISA 62443-3-2	Applies but needs change	Modify Ex5: and periodically inspect or test all configurations and security measures. Add Ex7: Establish policies, practices and procedures for asset management which includes security lifecycle updates for all OT assets
IDENTIFY (ID): Help determine the current cybersecurity risk to the organization	**Risk Assessment (ID.RA)**: The organization understands the cybersecurity risk to the organization, assets, and individuals.	**ID.RA-01**: Vulnerabilities in assets are identified, validated, and recorded (formerly ID.RA-01, PR.IP-12, DE.CM-08)	**Ex1**: Use vulnerability management technologies to identify unpatched and misconfigured software **Ex2**: Assess network and system architectures for design and implementation weaknesses that affect cybersecurity **Ex3**: Review, analyze, or test organization-developed software to identify design, coding, and default configuration vulnerabilities **Ex4**: Assess facilities that house critical computing assets for physical vulnerabilities and resilience issues **Ex5**: Monitor sources of cyber threat intelligence for information	ISA 62443-2-1 ISA 62443-2-3 ISA 62443-3-2	Applies but needs change	Modify ID.RA: The organization understands the cybersecurity risk to the organization, assets, individuals, operations, and physical enviroment

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
			on new vulnerabilities in products and services			
IDENTIFY (ID): Help determine the current cybersecurity risk to the organization	**Risk Assessment (ID.RA)**: The organization understands the cybersecurity risk to the organization, assets, and individuals.	**ID.RA-02**: Cyber threat intelligence is received from information sharing forums and sources	**Ex1**: Configure cybersecurity tools and technologies with detection or response capabilities to securely ingest cyber threat intelligence feeds **Ex2**: Receive and review advisories from reputable third parties on current threat actors and their tactics, techniques, and procedures (TTPs) **Ex3**: Monitor sources of cyber threat intelligence for information on the types of vulnerabilities that emerging technologies may have	ISA 62443-2-1 ISA 62443-2-3 ISA 62443-3-2 ISA 62443-4-1	Applies but needs change	-
IDENTIFY (ID): Help determine the current cybersecurity risk to the organization	**Risk Assessment (ID.RA)**: The organization understands the cybersecurity risk to the organization, assets, and individuals.	**ID.RA-03**: Internal and external threats to the organization are identified and recorded	**Ex1**: Use cyber threat intelligence to maintain awareness of the types of threat actors likely to target the organization and the TTPs they are likely to use **Ex2**: Perform threat hunting to look for signs of threat actors within the environment **Ex3**: Implement processes for identifying internal threat actors	ISA 62443-2-1 ISA 62443-3-2	Applies as is	

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
IDENTIFY (ID): Help determine the current cybersecurity risk to the organization	**Risk Assessment (ID.RA)**: The organization understands the cybersecurity risk to the organization, assets, and individuals.	**ID.RA-04**: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	**Ex1**: Business leaders and cybersecurity risk management practitioners work together to estimate the likelihood and impact of risk scenarios and record them in risk registers **Ex2**: Enumerate the potential business impacts of unauthorized access to the organization's communications, systems, and data processed in or by those systems **Ex3**: Account for the potential impacts of cascading failures for systems of systems	ISA 62443-3-2	Applies but needs change	Add EX4: Include physical consequences and impacts to health, safety and the environment in the risk assessment for OT systems
IDENTIFY (ID): Help determine the current cybersecurity risk to the organization	**Risk Assessment (ID.RA)**: The organization understands the cybersecurity risk to the organization, assets, and individuals.	**ID.RA-05**: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk and inform risk prioritization	**Ex1**: Develop threat models to better understand risks to the data and identify appropriate risk responses **Ex2**: Prioritize cybersecurity resource allocations and investments based on estimated likelihoods and impacts	ISA 62443-2-1 ISA 62443-3-2	Applies as is	
IDENTIFY (ID): Help determine the current cybersecurity risk to the organization	**Risk Assessment (ID.RA)**: The organization understands the cybersecurity risk to the organization, assets, and individuals.	**ID.RA-06**: Risk responses are chosen from the available options, prioritized, planned, tracked, and communicated (formerly ID.RA-06, RS.MI-03)	**Ex1**: Apply the vulnerability management plan's criteria for deciding whether to accept, transfer, mitigate, or avoid risk **Ex2**: Apply the vulnerability management plan's criteria for selecting compensating controls to mitigate risk **Ex3**: Track the progress of risk response implementation (e.g., plan of action and milestones [POA&M], risk register) **Ex4**: Use risk assessment findings to inform risk response decisions and actions **Ex5**: Communicate planned risk responses to affected stakeholders in priority order	ISA 62443-2-1 ISA 62443-3-2	Applies as is	

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
IDENTIFY (ID): Help determine the current cybersecurity risk to the organization	**Risk Assessment (ID.RA)**: The organization understands the cybersecurity risk to the organization, assets, and individuals.	**ID.RA-07**: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked (formerly part of PR.IP-03)	**Ex1**: Implement and follow procedures for the formal documentation, review, testing, and approval of proposed changes and requested exceptions **Ex2**: Document the possible risks of making or not making each proposed change, and provide guidance on rolling back changes **Ex3**: Document the risks related to each requested exception and the plan for responding to those risks **Ex4**: Periodically review risks that were accepted based upon planned future actions or milestones	ISA 62443-2-1 ISA 62443-3-2	Applies but needs change	Add Ex5: Document OT system risks where updates and patches cannot be deployed in a safe or timely manner
IDENTIFY (ID): Help determine the current cybersecurity risk to the organization	**Risk Assessment (ID.RA)**: The organization understands the cybersecurity risk to the organization, assets, and individuals.	**ID.RA-08**: Processes for receiving, analyzing, and responding to vulnerability disclosures are established (formerly RS.AN-05)	**Ex1**: Conduct vulnerability information sharing between the organization and its suppliers following the rules and protocols defined in contracts **Ex2**: Assign responsibilities and verify the execution of procedures for processing, analyzing the impact of, and responding to cybersecurity threat, vulnerability, or incident disclosures by suppliers, customers, partners, and government cybersecurity organizations	ISA 62443-2-1 ISA 62443-2-3 ISA 62443-3-2 ISA 62443-4-1	Applies but needs change	-
IDENTIFY (ID): Help determine the current cybersecurity risk to the organization	**Risk Assessment (ID.RA)**: The organization understands the cybersecurity risk to the organization, assets, and individuals.	**ID.RA-09**: The authenticity and integrity of hardware and software are assessed prior to acquisition and use (formerly PR.DS-08)	**Ex1**: Assess the authenticity and cybersecurity of critical technology products and services prior to acquisition and use	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-2-3 ISA 62443-3-2	Applies as is	

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
IDENTIFY (ID): Help determine the current cybersecurity risk to the organization	**Improvement (ID.IM)**: Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all Framework Functions	**ID.IM-01**: Continuous evaluation is applied to identify improvements	**Ex1**: Perform self-assessments of critical services that take current threats and TTPs into consideration **Ex2**: Invest in third-party assessments or independent audits of the effectiveness of the organization's cybersecurity program to identify areas that need improvement **Ex3**: Constantly evaluate compliance with selected cybersecurity requirements through automated means	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-3-2 ISA 62443-4-1	Applies but needs change	Ex4: Audit and validate all assessment personnel for capability relative to their security assessment role and responsibility.
IDENTIFY (ID): Help determine the current cybersecurity risk to the organization	**Improvement (ID.IM)**: Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all Framework Functions	**ID.IM-02**: Security tests and exercises, including those done in coordination with suppliers and relevant third parties, are conducted to identify improvements (formerly ID.SC-05, PR.IP-10, DE.DP-03)	**Ex1**: Identify improvements for future incident response activities based on findings from incident response assessments (e.g., tabletop exercises and simulations, tests, internal reviews, independent audits) **Ex2**: Identify improvements for future business continuity, disaster recovery, and incident response activities based on exercises performed in coordination with critical service providers and product suppliers **Ex3**: Involve internal stakeholders (e.g., senior executives, legal department, HR) in security tests and exercises as appropriate **Ex4**: Perform penetration testing to identify opportunities to improve the security posture of selected high-risk systems **Ex5**: Exercise contingency plans for responding to and recovering from the discovery that products or services did not originate with the contracted supplier or partner or	ISA 62443-2-1 ISA 62443-3-2	Applies but needs change	Add Ex7: Identify risks to operations from any security tests and exercises such as penetration tests, and obtain owner approval before executing them.

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
			were altered before receipt **Ex6**: Collect and analyze performance metrics using security tools and services to inform improvements to the cybersecurity program			
IDENTIFY (ID): Help determine the current cybersecurity risk to the organization	**Improvement (ID.IM)**: Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all Framework Functions	**ID.IM-03**: Lessons learned during execution of operational processes, procedures, and activities are used to identify improvements (formerly PR.IP-07, PR.IP-08, DE.DP-05, RS.IM-01, RS.IM-02, RC.IM-01, RC.IM-02)	**Ex1**: Conduct collaborative lessons learned sessions with suppliers **Ex2**: Annually review cybersecurity policies, processes, and procedures to take lessons learned into account **Ex3**: Use metrics to assess operational cybersecurity performance over time		Applies but needs change	Modify Ex2: Review cybersecurity policies, processes, and procedures to take lessons learned into account annually or at a period defined by a risk assessment.

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
IDENTIFY (ID): Help determine the current cybersecurity risk to the organization	**Improvement (ID.IM)**: Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all Framework Functions	**ID.IM-04**: Cybersecurity plans that affect operations are communicated, maintained, and improved (formerly PR.IP-09)	**Ex1**: Establish contingency plans (e.g., incident response, business continuity, disaster recovery) for responding to and recovering from adverse events that can interfere with operations, expose confidential information, or otherwise endanger the organization's mission and viability **Ex2**: Include contact and communication information, processes for handling common scenarios, and criteria for prioritization, escalation, and elevation in all contingency plans **Ex3**: Create a vulnerability management plan to identify and assess all types of vulnerabilities and to prioritize, test, and implement risk responses **Ex4**: Communicate cybersecurity plans (including updates) to those responsible for carrying them out and to affected parties **Ex5**: Review and update all cybersecurity plans annually or when a need for significant improvements is identified	ISA 62443-2-1 ISA 62443-3-2 ISA 62443-4-1	Applies but needs change	Add Ex6: Establish recovery plans for OT systems, and test the capability of all recovery operations periodically.

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk	**Identity Management, Authentication, and Access Control (PR.AA)**: Access to physical and logical assets is limited to authorized users, services, and hardware, and is managed commensurate with the assessed risk of unauthorized access (formerly PR.AC)	**PR.AA-01**: Identities and credentials for authorized users, services, and hardware are managed by the organization (formerly PR.AC-01)	**Ex1**: Initiate requests for new access or additional access for employees, contractors, and others, and track, review, and fulfill the requests, with permission from system or data owners when needed **Ex2**: Issue, manage, and revoke cryptographic certificates and identity tokens, cryptographic keys (i.e., key management), and other credentials **Ex3**: Select a unique identifier for each device from immutable hardware characteristics or an identifier securely provisioned to the device **Ex4**: Physically label authorized hardware with an identifier for inventory and servicing purposes	ISA 62443-2-1 ISA 62443-3-3	Applies as is	
PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk	**Identity Management, Authentication, and Access Control (PR.AA)**: Access to physical and logical assets is limited to authorized users, services, and hardware, and is managed commensurate with the assessed risk of unauthorized access (formerly PR.AC)	**PR.AA-02**: Identities are proofed and bound to credentials based on the context of interactions (formerly PR.AC-06)	**Ex1**: Verify a person's claimed identity at enrollment time using government-issued identity credentials (e.g., passport, visa, driver's license) **Ex2**: Issue credentials only to individuals (i.e., no credential sharing)	ISA 62443-2-1 ISA 62443-3-3	Applies but needs change	Add Ex3: Implement separate identification and authentication realms for OT systems.

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk	**Identity Management, Authentication, and Access Control (PR.AA)**: Access to physical and logical assets is limited to authorized users, services, and hardware, and is managed commensurate with the assessed risk of unauthorized access (formerly PR.AC)	**PR.AA-03**: Users, services, and hardware are authenticated (formerly PR.AC-03, PR.AC-07)	**Ex1**: Require multifactor authentication **Ex2**: Enforce policies for the minimum strength of passwords, PINs, and similar authenticators **Ex3**: Periodically reauthenticate users, services, and hardware based on risk (e.g., in zero trust architectures)	ISA 62443-2-1 ISA 62443-3-3	Applies as is	
PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk	**Identity Management, Authentication, and Access Control (PR.AA)**: Access to physical and logical assets is limited to authorized users, services, and hardware, and is managed commensurate with the assessed risk of unauthorized access (formerly PR.AC)	**PR.AA-04**: Identity assertions are protected, conveyed, and verified	**Ex1**: Protect identity assertions that are used to convey authentication and user information through single sign-on systems **Ex2**: Protect identity assertions that are used to convey authentication and user information between federated systems **Ex3**: Implement standards-based approaches for identity assertions in all contexts, and follow all guidance for the generation (e.g., data models, metadata), protection (e.g., digital signing, encryption), and verification (e.g., signature validation) of identity assertions	ISA 62443-2-1 ISA 62443-3-3	Applies as is	
PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk	**Identity Management, Authentication, and Access Control (PR.AA)**: Access to physical and logical assets is limited to authorized users, services, and hardware, and is managed commensurate with the assessed risk of unauthorized access (formerly PR.AC)	**PR.AA-05**: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties (formerly PR.AC-01, PR.AC-03, PR.AC-04)	**Ex1**: Review logical and physical access privileges periodically and whenever someone changes roles or leaves the organization, and promptly rescind privileges that are no longer needed **Ex2**: Take attributes of the requester and the requested resource into account for authorization decisions (e.g., geolocation, day/time, requester endpoint's cyber health) **Ex3**: Restrict access and privileges	ISA 62443-2-1 ISA 62443-3-3	Applies but needs change	Add Ex5: Prevent loss of access for accounts that are essential to protect health, safety or the environment

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
			to the minimum necessary (e.g., zero trust architecture) **Ex4**: Periodically review the privileges associated with critical business functions to confirm proper separation of duties			
PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk	**Identity Management, Authentication, and Access Control (PR.AA)**: Access to physical and logical assets is limited to authorized users, services, and hardware, and is managed commensurate with the assessed risk of unauthorized access (formerly PR.AC)	**PR.AA-06**: Physical access to assets is managed, monitored, and enforced commensurate with risk (formerly PR.AC-02, PR.PT-04)	**Ex1**: Use security guards, security cameras, locked entrances, alarm systems, and other physical controls to monitor facilities and restrict access **Ex2**: Employ additional physical security controls for areas that contain high-risk assets **Ex3**: Escort guests, vendors, and other third parties within areas that contain business-critical assets	ISA 62443-2-1	Applies as is	
PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk	**Awareness and Training (PR.AT)**: The organization's personnel are provided cybersecurity awareness and training so they can perform their cybersecurity-related tasks	**PR.AT-01**: Users are provided awareness and training so they possess the knowledge and skills to perform general tasks with security risks in mind (formerly PR.AT-01, PR.AT-03, RS.CO-01)	**Ex1**: Provide basic cybersecurity awareness and training to employees, contractors, partners, suppliers, and all other users of the organization's non-public resources **Ex2**: Train users to recognize social engineering attempts and other common attacks, report attacks and suspicious activity, comply with acceptable use policies, and perform basic cyber hygiene tasks (e.g., patching software, choosing passwords, protecting credentials) **Ex3**: Explain the consequences of cybersecurity policy violations, both to individual users and the organization as a whole	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-4-1	Applies as is	

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
			Ex4: Periodically assess or test users on their understanding of basic cybersecurity practices **Ex5**: Require annual refreshers to reinforce existing practices and introduce new practices			
PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk	**Awareness and Training (PR.AT)**: The organization's personnel are provided cybersecurity awareness and training so they can perform their cybersecurity-related tasks	**PR.AT-02**: Individuals in specialized roles are provided awareness and training so they possess the knowledge and skills to perform relevant tasks with security risks in mind (formerly PR.AT-02, PR.AT-03, PR.AT-04, PR.AT-05)	**Ex1**: Identify the specialized roles within the organization that require additional cybersecurity training, such as physical and cybersecurity personnel, finance personnel, senior leadership, and anyone with access to business-critical data **Ex2**: Provide role-based cybersecurity awareness and training to all those in specialized roles, including contractors, partners, suppliers, and other third parties **Ex3**: Periodically assess or test users on their understanding of cybersecurity practices for their specialized roles **Ex4**: Require annual refreshers to reinforce existing practices and introduce new practices	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-4-1	Applies as is	

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk	**Data Security (PR.DS)**: Data is managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information	**PR.DS-01**: The confidentiality, integrity, and availability of data-at-rest are protected (formerly PR.DS-01, PR-DS.05, PR.DS-06, PR.PT-02)	**Ex1**: Use encryption, digital signatures, and cryptographic hashes to protect the confidentiality and integrity of stored data in files, databases, virtual machine disk images, container images, and other resources **Ex2**: Use full disk encryption to protect data stored on user endpoints **Ex3**: Confirm the integrity of software by validating signatures **Ex4**: Restrict the use of removable media to prevent data exfiltration **Ex5**: Physically secure removable media containing unencrypted sensitive information, such as within locked offices or file cabinets	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-3-3	Applies as is	
PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk	**Data Security (PR.DS)**: Data is managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information	**PR.DS-02**: The confidentiality, integrity, and availability of data-in-transit are protected (formerly PR.DS-02, PR.DS-05)	**Ex1**: Use encryption, digital signatures, and cryptographic hashes to protect the confidentiality and integrity of network communications **Ex2**: Automatically encrypt or block outbound emails and other communications that contain sensitive data, depending on the data classification **Ex3**: Block access to personal email, file sharing, file storage services, and other personal communications applications and services from organizational systems and networks **Ex4**: Prevent reuse of sensitive data from production environments (e.g., customer records) in development, testing, and other non-production environments	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-3-3	Applies as is	

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk	**Data Security (PR.DS)**: Data is managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information	**PR.DS-09**: Data is managed throughout its life cycle, including destruction (formerly PR.IP-06)	**Ex1**: Securely destroy stored data based on the organization's data retention policy using the prescribed destruction method **Ex2**: Securely sanitize data storage when hardware is being retired, decommissioned, reassigned, or sent for repairs or replacement **Ex3**: Offer methods for destroying paper, storage media, and other physical forms of data storage	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-3-3 ISA 62443-4-1 ISA 62443-4-2	Applies as is	
PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk	**Data Security (PR.DS)**: Data is managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information	**PR.DS-10**: The confidentiality, integrity, and availability of data-in-use are protected (formerly PR.DS-05)	**Ex1**: Remove data that must remain confidential (e.g., from processors and memory) as soon as it is no longer needed **Ex2**: Protect data in use from access by other users and processes of the same platform	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-3-3 ISA 62443-4-1 ISA 62443-4-2	Applies as is	
PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk	**Data Security (PR.DS)**: Data is managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information	**PR.DS-11**: Backups of data are created, protected, maintained, and tested (formerly PR.IP-04)	**Ex1**: Continuously back up critical data in near-real-time, and back up other data frequently at agreed-upon schedules **Ex2**: Test backups and restores for all types of data sources at least annually **Ex3**: Securely store some backups offline and offsite so that an incident or disaster will not damage them **Ex4**: Enforce geolocation restrictions for data backup storage	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-3-3 ISA 62443-4-2	Applies as is	

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk	**Platform Security (PR.PS)**: The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability	**PR.PS-01**: Configuration management practices are applied (formerly PR.IP-01, PR.IP-03, PR.PT-02, PR.PT-03)	**Ex1**: Establish, test, deploy, and maintain hardened baselines that enforce the organization's cybersecurity policies and provide only essential capabilities (i.e., principle of least functionality) **Ex2**: Review all default configuration settings that may potentially impact cybersecurity when installing or upgrading software	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-4-1	Applies as is	
PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk	**Platform Security (PR.PS)**: The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability	**PR.PS-02**: Software is maintained, replaced, and removed commensurate with risk (formerly PR.IP-12, PR.MA-02)	**Ex1**: Perform routine and emergency patching within the timeframes specified in the vulnerability management plan **Ex2**: Update container images, and deploy new container instances to replace rather than update existing instances **Ex3**: Replace end-of-life software and service versions with supported, maintained versions **Ex4**: Uninstall and remove unauthorized software and services that pose undue risks **Ex5**: Uninstall and remove any unnecessary software components (e.g., operating system utilities) that attackers might misuse **Ex6**: Define and implement plans for software and service end-of-life maintenance support and obsolescence	ISA 62443-2-1 ISA 62443-2-3 IEC 62443-2-4 ISA 62443-4-1	Applies as is	

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk	**Platform Security (PR.PS)**: The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability	**PR.PS-03**: Hardware is maintained, replaced, and removed commensurate with risk (formerly PR.MA-01)	**Ex1**: Replace hardware when it lacks needed security capabilities or when it cannot support software with needed security capabilities **Ex2**: Define and implement plans for hardware end-of-life maintenance support and obsolescence **Ex3**: Perform hardware disposal in a secure, responsible, and auditable manner	ISA 62443-2-1 ISA 62443-2-3 IEC 62443-2-4 ISA 62443-4-1	Applies as is	
PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk	**Platform Security (PR.PS)**: The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability	**PR.PS-04**: Log records are generated and made available for continuous monitoring (formerly PR.PT-01)	**Ex1**: Configure all operating systems, applications, and services (including cloud-based services) to generate log records **Ex2**: Configure log generators to securely share their logs with the organization's logging infrastructure systems and services **Ex3**: Configure log generators to record the data needed by zero-trust architectures	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-3-3 ISA 62443-4-1 ISA 62443-4-2	Applies as is	
PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk	**Platform Security (PR.PS)**: The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability	**PR.PS-05**: Installation and execution of unauthorized software are prevented	**Ex1**: When risk warrants it, restrict software execution to permitted products only or deny the execution of prohibited and unauthorized software **Ex2**: Verify the source of new software and the software's integrity before installing it **Ex3**: Configure platforms to use only approved DNS services that block access to known malicious domains **Ex4**: Configure platforms to allow the installation of organization-approved software only	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-4-1	Applies as is	

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk	**Platform Security (PR.PS)**: The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability	**PR.PS-06**: Secure software development practices are integrated and their performance is monitored throughout the software development life cycle	**Ex1**: Protect all components of organization-developed software from tampering and unauthorized access **Ex2**: Secure all software produced by the organization, with minimal vulnerabilities in their releases **Ex3**: Maintain the software used in production environments, and securely dispose of software once it is no longer needed	ISA 62443-4-1	Applies as is	
PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk	**Technology Infrastructure Resilience (PR.IR)**: Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience	**PR.IR-01**: Networks and environments are protected from unauthorized logical access and usage (formerly PR.AC-03, PR.AC-05, PR.DS-07, PR.PT-04)	**Ex1**: Logically segment organization networks and cloud-based platforms according to trust boundaries and platform types (e.g., IT, IoT, OT, mobile, guests), and permit required communications only between segments **Ex2**: Logically segment organization networks from external networks, and permit only necessary communications to enter the organization's networks from the external networks **Ex3**: Implement zero trust architectures to restrict network access to each resource to the minimum necessary **Ex4**: Check the cyber health of endpoints before allowing them to access and use production resources	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-3-2	Applies but needs change	Add Ex5: Logically segment IT networks and OT networks and permit required communications only between segments Add Ex6: Logically and physically segment Health/Safety/Environmental networks from all other networks and permit required communications only between segments

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk	**Technology Infrastructure Resilience (PR.IR)**: Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience	**PR.IR-02**: The organization's technology assets are protected from environmental threats (formerly PR.IP-05)	**Ex1**: Protect organizational equipment from known environmental threats, such as flooding, fire, wind, and excessive heat and humidity **Ex2**: Include protection from environmental threats and provisions for adequate operating infrastructure in requirements for service providers that operate systems on the organization's behalf		Applies as is	
PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk	**Technology Infrastructure Resilience (PR.IR)**: Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience	**PR.IR-03**: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations (formerly PR.PT-05)	**Ex1**: Avoid single points of failure in systems and infrastructure **Ex2**: Use load balancing to increase capacity and improve reliability **Ex3**: Use high-availability components like redundant storage and power suppliers to improve system reliability	ISA 62443-2-1 IEC 62443-2-4	Applies as is	
PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk	**Technology Infrastructure Resilience (PR.IR)**: Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience	**PR.IR-04**: Adequate resource capacity to ensure availability is maintained (formerly PR.DS-04)	**Ex1**: Monitor usage of storage, power, compute, network bandwidth, and other resources **Ex2**: Forecast future needs, and scale resources accordingly	ISA 62443-2-1 IEC 62443-2-4	Applies as is	

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
DETECT (DE): Find and analyze possible cybersecurity attacks and compromises	**Continuous Monitoring (DE.CM)**: Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events	**DE.CM-01**: Networks and network services are monitored to find potentially adverse events (formerly DE.CM-01, DE.CM-04, DE.CM-05, DE.CM-07)	**Ex1**: Monitor DNS, BGP, and other network services for adverse events **Ex2**: Monitor wired and wireless networks for connections from unauthorized endpoints **Ex3**: Monitor facilities for unauthorized or rogue wireless networks **Ex4**: Compare actual network flows against baselines to detect deviations **Ex5**: Monitor network communications to identify changes in security postures for zero trust purposes	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-3-3 MLM-038A	Applies but needs change	Add Ex6: Monitor network communications to identify the misuse or manipulation of common and operational protocols Add Ex7: Monitor internal and external network zone boundaries for adverse events

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
DETECT (DE): Find and analyze possible cybersecurity attacks and compromises	**Continuous Monitoring (DE.CM)**: Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events	**DE.CM-02**: The physical environment is monitored to find potentially adverse events	**Ex1**: Monitor logs from physical access control systems (e.g., badge readers) to find unusual access patterns (e.g., deviations from the norm) and failed access attempts **Ex2**: Review and monitor physical access records (e.g., from visitor registration, sign-in sheets) **Ex3**: Monitor physical access controls (e.g., door locks, latches, hinge pins) for signs of tampering **Ex4**: Monitor the physical environment using alarm systems, cameras, and security guards	ISA 62443-2-1	Applies but needs change	Add Ex5: Monitor the physical equipment enclosures using cabinet alarms, electronic keys, and physical inspections
DETECT (DE): Find and analyze possible cybersecurity attacks and compromises	**Continuous Monitoring (DE.CM)**: Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events	**DE.CM-03**: Personnel activity and technology usage are monitored to find potentially adverse events (formerly DE.CM-03, DE.CM-07)	**Ex1**: Use behavior analytics software to detect anomalous user activity to mitigate insider threats **Ex2**: Monitor logs from logical access control systems to find unusual access patterns and failed access attempts **Ex3**: Continuously monitor deception technology, including user accounts, for any usage	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-3-3	Applies as is	
DETECT (DE): Find and analyze possible cybersecurity attacks and compromises	**Continuous Monitoring (DE.CM)**: Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events	**DE.CM-06**: External service provider activities and services are monitored to find potentially adverse events (formerly DE.CM-06, DE.CM-07)	**Ex1**: Monitor remote administration and maintenance activities that external providers perform on organizational systems **Ex2**: Monitor cloud-based services, internet service providers, and other service providers for deviations from expected behavior	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-3-3	Applies but needs change	Add Ex3: Monitor the actions of service providers that perform actions while onsite.

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
DETECT (DE): Find and analyze possible cybersecurity attacks and compromises	**Continuous Monitoring (DE.CM)**: Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events	**DE.CM-09**: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events (formerly PR.DS-06, PR.DS-08, DE.CM-04, DE.CM-05, DE.CM-07)	**Ex1**: Monitor email, web, file sharing, collaboration services, and other common attack vectors to detect malware, phishing, data leaks and exfiltration, and other adverse events **Ex2**: Monitor authentication attempts to identify attacks against credentials and unauthorized credential reuse **Ex3**: Monitor software configurations for deviations from security baselines **Ex4**: Use technologies with a presence on endpoints to detect cyber health issues (e.g., missing patches, malware infections, unauthorized software), and redirect the endpoints to a remediation environment before access is authorized	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-3-3	Applies but needs change	Add Ex5: Monitor the attempted or successful use of privileged services or commands to identify privilege escalation attacks
DETECT (DE): Find and analyze possible cybersecurity attacks and compromises	**Adverse Event Analysis (DE.AE)**: Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents (formerly DE.AE, DE.DP-02)	**DE.AE-02**: Potentially adverse events are analyzed to better understand associated activities	**Ex1**: Use security information and event management (SIEM) or other tools to continuously monitor log events for known malicious and suspicious activity **Ex2**: Utilize up-to-date cyber threat intelligence in log analysis tools to improve detection accuracy and characterize threat actors, their methods, and indicators of compromise **Ex3**: Regularly conduct manual reviews of log events for technologies that cannot be sufficiently monitored through automation	ISA 62443-2-1 ISA 62443-3-2 ISA 62443-3-3	Applies as is	

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
			Ex4: Use log analysis tools to generate reports on their findings			
DETECT (DE): Find and analyze possible cybersecurity attacks and compromises	**Adverse Event Analysis (DE.AE)**: Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents (formerly DE.AE, DE.DP-02)	**DE.AE-03**: Information is correlated from multiple sources	**Ex1**: Constantly transfer log data generated by other sources to a relatively small number of log servers **Ex2**: Use event correlation technology (e.g., SIEM) to collect information captured by multiple sources **Ex3**: Utilize cyber threat intelligence to help correlate events among log sources	ISA 62443-2-1 ISA 62443-3-3	Applies as is	
DETECT (DE): Find and analyze possible cybersecurity attacks and compromises	**Adverse Event Analysis (DE.AE)**: Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents (formerly DE.AE, DE.DP-02)	**DE.AE-04**: The estimated impact and scope of adverse events are determined	**Ex1**: Use SIEMs or other tools to estimate impact and scope, and review and refine the estimates **Ex2**: A person creates their own estimates of impact and scope	ISA 62443-2-1 ISA 62443-3-2	Applies but needs change	Add Ex3: Evaluate impacts, such as health, safety, environmental, production downtime, regulatory, reputational, etc. from adverse events to understand the worst-case, unmitigated and mitigated consequences

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
DETECT (DE): Find and analyze possible cybersecurity attacks and compromises	**Adverse Event Analysis (DE.AE)**: Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents (formerly DE.AE, DE.DP-02)	**DE.AE-06**: Information on adverse events is provided to authorized staff and tools (formerly DE.DP-04)	**Ex1**: Use cybersecurity software to generate alerts and provide them to the security operations center (SOC), incident responders, and incident response tools **Ex2**: Incident responders and other authorized personnel can access log analysis findings at all times **Ex3**: Automatically create and assign tickets in the organization's ticketing system when certain types of alerts occur **Ex4**: Manually create and assign tickets in the organization's ticketing system when technical staff discover indicators of compromise	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-3-3	Applies as is	
DETECT (DE): Find and analyze possible cybersecurity attacks and compromises	**Adverse Event Analysis (DE.AE)**: Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents (formerly DE.AE, DE.DP-02)	**DE.AE-07**: Cyber threat intelligence and other contextual information are integrated into the analysis	**Ex1**: Securely provide cyber threat intelligence feeds to detection technologies, processes, and personnel **Ex2**: Securely provide information from asset inventories to detection technologies, processes, and personnel **Ex3**: Rapidly acquire and analyze vulnerability disclosures for the organization's technologies from suppliers, vendors, and third-party security advisories	ISA 62443-2-1 ISA 62443-3-2	Applies but needs change	Add Ex4: Securely provide process-related information and events to detection technologies, processes, and personnel
DETECT (DE): Find and analyze possible cybersecurity attacks and compromises	**Adverse Event Analysis (DE.AE)**: Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents (formerly DE.AE, DE.DP-02)	**DE.AE-08**: Incidents are declared when adverse events meet the defined incident criteria (formerly DE.AE-05)	**Ex1**: Apply incident criteria to known and assumed characteristics of activity in order to determine whether an incident should be declared **Ex2**: Take known false positives into account when applying incident criteria	ISA 62443-2-1	Applies as is	

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
RESPOND (RS): Take action regarding a detected cybersecurity incident	**Incident Management (RS.MA)**: Responses to detected cybersecurity incidents are managed (formerly RS.RP)	**RS.MA-01**: The incident response plan is executed once an incident is declared in coordination with relevant third parties (formerly RS.RP-01, RS.CO-04)	**Ex1**: Detection technologies automatically report confirmed incidents **Ex2**: Request incident response assistance from the organization's incident response outsourcer **Ex3**: Designate an incident lead for each incident	ISA 62443-2-1 ISA 62443-3-3 ICS4ICS.org	Applies but needs change	Add Ex4: Activate the incident response team for the incident Add Ex5: Initiate emergency response as needed for OT incidents NOTE: Refer to ICS4ICS.org which uses FEMA Incident Command System for OT emergency response
RESPOND (RS): Take action regarding a detected cybersecurity incident	**Incident Management (RS.MA)**: Responses to detected cybersecurity incidents are managed (formerly RS.RP)	**RS.MA-02**: Incident reports are triaged and validated (formerly RS.AN-01, RS.AN-02)	**Ex1**: Preliminarily review incident reports to confirm that they are cybersecurity-related and necessitate incident response activities **Ex2**: Apply criteria to estimate the severity of an incident	ISA 62443-2-1 ICS4ICS.org	Applies but needs change	Modify Ex2: Apply critieria to estimate the criticality, severity, and scope of an incident
RESPOND (RS): Take action regarding a detected cybersecurity incident	**Incident Management (RS.MA)**: Responses to detected cybersecurity incidents are managed (formerly RS.RP)	**RS.MA-03**: Incidents are categorized and prioritized (formerly RS.AN-04, RS.AN-02)	**Ex1**: Further review and categorize incidents based on the type of incident (e.g., data breach, ransomware, DDoS, account compromise) **Ex2**: Prioritize incidents based on their scope, likely impact, and time-critical nature **Ex3**: Select incident response strategies for active incidents by balancing the need to quickly recover from an incident with the need to observe the attacker or conduct a more thorough investigation	ISA 62443-2-1 ICS4ICS.org	Applies but needs change	Modify Ex1: Further review and categorize incidents based on the type of incident (e.g. data breach, ransomware, DDoS, account compromise, insider threat, process manipulation)

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
RESPOND (RS): Take action regarding a detected cybersecurity incident	**Incident Management (RS.MA)**: Responses to detected cybersecurity incidents are managed (formerly RS.RP)	**RS.MA-04**: Incidents are escalated or elevated as needed (formerly RS.AN-02, RS.CO-04)	**Ex1**: Track and validate the status of all ongoing incidents **Ex2**: Coordinate incident escalation or elevation with designated internal and external stakeholders	ISA 62443-2-1 ICS4ICS.org	Applies as is	
RESPOND (RS): Take action regarding a detected cybersecurity incident	**Incident Management (RS.MA)**: Responses to detected cybersecurity incidents are managed (formerly RS.RP)	**RS.MA-05**: The criteria for initiating incident recovery are applied	**Ex1**: Apply incident recovery criteria to known and assumed characteristics of the incident to determine whether incident recovery processes should be initiated **Ex2**: Take the possible operational disruption of incident recovery activities into account	ISA 62443-2-1 ICS4ICS.org	Applies as is	
RESPOND (RS): Take action regarding a detected cybersecurity incident	**Incident Analysis (RS.AN)**: Investigation is conducted to ensure effective response and support forensics and recovery activities	**RS.AN-03**: Analysis is performed to determine what has taken place during an incident and the root cause of the incident	**Ex1**: Determine the sequence of events that occurred during the incident and which assets and resources were involved in each event **Ex2**: Attempt to determine what vulnerabilities, threats, and threat actors were directly or indirectly involved in the incident **Ex3**: Analyze the incident to find the underlying, systemic root causes **Ex4**: Check any cyber deception technology for additional information on attacker behavior	ISA 62443-2-1	Applies as is	
RESPOND (RS): Take action regarding a detected cybersecurity incident	**Incident Analysis (RS.AN)**: Investigation is conducted to ensure effective response and support forensics and recovery activities	**RS.AN-06**: Actions performed during an investigation are recorded and the records' integrity and provenance are preserved (formerly part of RS.AN-03)	**Ex1**: Require each incident responder and others (e.g., system administrators, cybersecurity engineers) who perform incident response tasks to record their actions and make the record immutable **Ex2**: Require the incident lead to document the incident in detail and be responsible for preserving the integrity of the documentation and	ISA 62443-2-1	Applies as is	

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
			the sources of all information being reported			
RESPOND (RS): Take action regarding a detected cybersecurity incident	**Incident Analysis (RS.AN)**: Investigation is conducted to ensure effective response and support forensics and recovery activities	**RS.AN-07**: Incident data and metadata are collected, and their integrity and provenance are preserved	**Ex1**: Collect, preserve, and safeguard the integrity of all pertinent incident data and metadata (e.g., data source, date/time of collection) based on evidence preservation and chain-of-custody procedures	ISA 62443-2-1	Applies as is	
RESPOND (RS): Take action regarding a detected cybersecurity incident	**Incident Analysis (RS.AN)**: Investigation is conducted to ensure effective response and support forensics and recovery activities	**RS.AN-08**: The incident's magnitude is estimated and validated	**Ex1**: Review other potential targets of the incident to search for indicators of compromise and evidence of persistence **Ex2**: Automatically run tools on targets to look for indicators of compromise and evidence of persistence	ISA 62443-2-1	Applies as is	
RESPOND (RS): Take action regarding a detected cybersecurity incident	**Incident Response Reporting and Communication (RS.CO)**: Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies	**RS.CO-02**: Internal and external stakeholders are notified of incidents	**Ex1**: Follow the organization's breach notification procedures after discovering a data breach incident, including notifying affected customers **Ex2**: Notify business partners and customers of incidents in accordance with contractual requirements **Ex3**: Notify law enforcement agencies and regulatory bodies of incidents based on criteria in the incident response plan and management approval	ISA 62443-2-1	Applies as is	

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
RESPOND (RS): Take action regarding a detected cybersecurity incident	**Incident Response Reporting and Communication (RS.CO)**: Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies	**RS.CO-03**: Information is shared with designated internal and external stakeholders (formerly RS.CO-03, RS.CO-05)	**Ex1**: Securely share information consistent with response plans and information sharing agreements **Ex2**: Voluntarily share information about an attacker's observed TTPs, with all sensitive data removed, with an Information Sharing and Analysis Center (ISAC) **Ex3**: Notify HR when malicious insider activity occurs **Ex4**: Regularly update senior leadership on the status of major incidents **Ex5**: Follow the rules and protocols defined in contracts for incident information sharing between the organization and its suppliers **Ex6**: Coordinate crisis communication methods between the organization and its critical suppliers	ISA 62443-2-1	Applies as is	
RESPOND (RS): Take action regarding a detected cybersecurity incident	**Incident Mitigation (RS.MI)**: Activities are performed to prevent expansion of an event and mitigate its effects	**RS.MI-01**: Incidents are contained	**Ex1**: Cybersecurity technologies (e.g., antivirus software) and cybersecurity features of other technologies (e.g., operating systems, network infrastructure devices) automatically perform containment actions **Ex2**: Allow incident responders to manually select and perform containment actions **Ex3**: Allow a third party (e.g., internet service provider, managed security service provider) to perform containment actions on behalf of the organization **Ex4**: Automatically transfer compromised endpoints to a remediation virtual local area network (VLAN)	ISA 62443-2-1 IEC 62443-2-4 ISA 62443-3-3	Applies but needs change	Modify Ex4: Obtain approval from appropriate managers and/or stakeholders to perform containment actions as defined in the incident response plan and/or incident response playbooks Add Ex5: Segment and/or isolate network zones to prevent the spread of an incident via physical or logical means Add Ex6: The risks, such as health, safety, and environmental, should be considered when performing containment actions.

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
RESPOND (RS): Take action regarding a detected cybersecurity incident	**Incident Mitigation (RS.MI)**: Activities are performed to prevent expansion of an event and mitigate its effects	**RS.MI-02**: Incidents are eradicated	**Ex1**: Cybersecurity technologies and cybersecurity features of other technologies (e.g., operating systems, network infrastructure devices) automatically perform eradication actions **Ex2**: Allow incident responders to manually select and perform eradication actions **Ex3**: Allow a third party (e.g., managed security service provider) to perform eradication actions on behalf of the organization	ISA 62443-2-1	Applies but needs change	Add Ex4: Obtain approval from appropriate managers and/or stakeholders to perform eradication actions as defined in the incident response plan and/or incident response playbooks Add Ex5: The risks, such as health, safety, and environmental, should be considered when performing eradication actions.
RECOVER (RC): Restore assets and operations that were impacted by a cybersecurity incident	**Incident Recovery Plan Execution (RC.RP)**: Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents	**RC.RP-01**: The recovery portion of the incident response plan is executed once initiated from the incident response process	**Ex1**: Begin recovery procedures during or after incident response processes **Ex2**: Make all individuals with recovery responsibilities aware of the plans for recovery and the authorizations required to implement each aspect of the plans	ISA 62443-2-1 ISA 62443-2-4 ISA 62443-3-3 ISA 62443-4-2	Applies but needs change	Modify RC.RP: Restoration activities are performed to ensure the ~~operational~~ availability of systems, services, and *operations*...
RECOVER (RC): Restore assets and operations that were impacted by a cybersecurity incident	**Incident Recovery Plan Execution (RC.RP)**: Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents	**RC.RP-02**: Recovery actions are determined, scoped, prioritized, and performed	**Ex1**: Select recovery actions based on the criteria defined in the incident response plan and available resources **Ex2**: Change planned recovery actions based on a reassessment of organizational needs and resources	ISA 62443-2-1 ISA 62443-2-4 ISA 62443-3-3 ISA 62443-4-2	Applies but needs change	Modify RC.RP: Restoration activities are performed to ensure the ~~operational~~ availability of systems, services, and *operations*...
RECOVER (RC): Restore assets and operations that were impacted by a cybersecurity incident	**Incident Recovery Plan Execution (RC.RP)**: Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents	**RC.RP-03**: The integrity of backups and other restoration assets is verified before using them for restoration	**Ex1**: Check restoration assets for indicators of compromise, file corruption, and other integrity issues before use	ISA 62443-2-1 ISA 62443-2-4 ISA 62443-3-3 ISA 62443-4-2	Applies but needs change	Modify RC.RP: Restoration activities are performed to ensure the ~~operational~~ availability of systems, services, and *operations*...

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
RECOVER (RC): Restore assets and operations that were impacted by a cybersecurity incident	**Incident Recovery Plan Execution (RC.RP)**: Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents	**RC.RP-04**: Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms	**Ex1**: Use business impact and system categorization records (including service delivery objectives) to validate that essential services are restored in the appropriate order **Ex2**: Work with system owners to confirm the successful restoration of systems and the return to normal operations **Ex3**: Monitor the performance of restored systems to verify the adequacy of the restoration	ISA 62443-2-1 ISA 62443-2-4 ISA 62443-3-3 ISA 62443-4-2	Applies but needs change	Modify RC.RP: Restoration activities are performed to ensure the ~~operational~~ availability of systems, services, and *operations*...
RECOVER (RC): Restore assets and operations that were impacted by a cybersecurity incident	**Incident Recovery Plan Execution (RC.RP)**: Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents	**RC.RP-05**: The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed	**Ex1**: Check restored assets for indicators of compromise and remediation of root causes of the incident before production use **Ex2**: Verify the correctness and adequacy of the restoration actions taken before putting a restored system online	ISA 62443-2-1 ISA 62443-2-4 ISA 62443-3-3 ISA 62443-4-2	Applies but needs change	Modify RC.RP: Restoration activities are performed to ensure the ~~operational~~ availability of systems, services, and *operations*...
RECOVER (RC): Restore assets and operations that were impacted by a cybersecurity incident	**Incident Recovery Plan Execution (RC.RP)**: Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents	**RC.RP-06**: The criteria for determining the end of incident recovery are applied, and incident-related documentation is completed	**Ex1**: Prepare an after-action report that documents the incident itself, the response and recovery actions taken, and lessons learned **Ex2**: Declare the end of incident recovery once the criteria are met	ISA 62443-2-1 ISA 62443-2-4 ISA 62443-3-3 ISA 62443-4-2	Applies but needs change	Modify RC.RP: Restoration activities are performed to ensure the ~~operational~~ availability of systems, services, and *operations*...

Function	Category	Subcategory	Implementation Examples	Informative References	Applicability to OT Systems	Recommended Change
RECOVER (RC): Restore assets and operations that were impacted by a cybersecurity incident	**Incident Recovery Communication (RC.CO)**: Restoration activities are coordinated with internal and external parties	**RC.CO-03**: Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders	**Ex1**: Securely share recovery information, including restoration progress, consistent with response plans and information sharing agreements **Ex2**: Regularly update senior leadership on recovery status and restoration progress for major incidents **Ex3**: Follow the rules and protocols defined in contracts for incident information sharing between the organization and its suppliers **Ex4**: Coordinate crisis communication between the organization and its critical suppliers	ISA 62443-2-1 ISA 62443-2-4 ISA 62443-3-3 ISA 62443-4-2	Applies as is	
RECOVER (RC): Restore assets and operations that were impacted by a cybersecurity incident	**Incident Recovery Communication (RC.CO)**: Restoration activities are coordinated with internal and external parties	**RC.CO-04**: Public updates on incident recovery are properly shared using approved methods and messaging (formerly RC.CO-01, RC.CO-02)	**Ex1**: Follow the organization's breach notification procedures for recovering from a data breach incident **Ex2**: Explain the steps being taken to recover from the incident and to prevent a recurrence	ISA 62443-2-1 ISA 62443-2-4 ISA 62443-3-3 ISA 62443-4-2	Applies as is	