Operational Technology (OT) Cybersecurity Standards Supporting Guidance

HRSD

Version 1.0

April 2026

1.0 Contents

2.0 Purpose

This document provides guidance supporting the implementation of OT cybersecurity standards across HRSD environments.

3.0 Objectives

This document is intended to support implementation of the OT Cybersecurity Standards by translating requirements into practical operational and engineering guidance. The objectives of this document are to:

- Provide practical guidance for implementing OT cybersecurity standards
- Support consistent application of controls across OT environments
- Translate requirements into operational and engineering practices
- Support risk management and visibility into system posture

4.0 Scope

This guidance applies to OT systems supporting HRSD operations, including ICS, SCADA systems, supporting infrastructure, and industrial networks.

5.0 Definitions

The following terms are used within this document and throughout the broader HRSD Cybersecurity Governance Program.

Term	Definition
Operational Technology (OT)	• The hardware and software systems that monitor, control, and automate physical processes in industrial environments. OT includes: • Industrial Control Systems (ICS), including PLCs, RTUs, and DCS • SCADA systems • Supporting infrastructure such as servers and workstations • Industrial networks including switches, routers, and firewalls • Associated assets required to operate and protect physical processes
Security Zone	A logical or physical grouping of assets with similar trust levels and security requirements.
Purdue Model Level 2	Control layer where supervisory control systems and HMIs operate.
System Acceptance	Formal approval that a system meets defined requirements and is ready for production use.

6.0 Architecture Standards

Architecture standards define how OT systems and networks are structured, segmented, and interconnected to support secure and reliable operations.

6.1 Asset Management (Architecture)

Defines how OT assets are identified, documented, and organized to support visibility and control.

6.1.1 Architecture Requirements

- Assets must be uniquely identifiable and tracked in a centralized inventory.
- Asset inventories must include key attributes such as system function, ownership, and network identity.
- Assets must be assigned to defined security zones based on function and criticality.
- Network topology diagrams must reflect asset placement, connectivity paths, and zone boundaries.
- OT/ICS assets must align to a zoned architecture consistent with the Purdue model.
- Each asset must have an assigned owner responsible for lifecycle and security.
- Asset inventory and network documentation should be maintained as part of system design, implementation, and turnover.

6.1.2 Implementation Considerations

- Asset data should be integrated with approved systems such as asset inventories, engineering systems of record, and monitoring platforms.
- ICS field devices should have defined and traceable connectivity paths.
- Standalone or non-networked assets should be documented or justified through risk-based exception.

6.1.3 Importance Explanation

Asset management is the continuous process of identifying, documenting, and maintaining a complete and accurate inventory of systems that support plant operations. The objective is to maintain visibility into what exists, where it is, how it is connected, and who is responsible for it. In OT environments, this includes:

- Control systems (PLCs, RTUs, DCS)
- SCADA systems and supporting servers
- Engineering workstations and operator interfaces
- Network and security infrastructure
- Field devices and associated software

6.1.4 Analogy

Asset management is similar to a hotel room ledger. The hotel knows every room, who occupies it, which keys work, and how rooms connect. If anything goes wrong, staff know exactly where to go, what to isolate, and who to call. In OT environments, assets represent the rooms, and network paths, access controls, and system configurations represent the keys and corridors.

6.1.5 Why it matters

- Supports safe and predictable operations
- Enables rapid incident response and recovery
- Enables practical implementation of least privilege and segmentation
- Supports controlled change and patch management
- Improves vendor access control and accountability
- Supports lifecycle planning and spare management
- Simplifies audit and compliance activities

6.1.6 Risk if not implemented

- Unknown or unmanaged assets introduce blind spots
- Increased risk of unauthorized access or manipulation
- Slower incident response and extended outages
- Increased risk of misconfiguration or failed changes

6.2 Identity and Access Control (Architecture)

Defines how access to OT systems is controlled, authenticated, and monitored.

6.2.1 Architecture Requirements

- Access to OT systems must follow role-based access control (RBAC) and least privilege principles.
- Unique user identities must be used for all access; shared accounts must be prohibited unless explicitly approved.
- Remote access to OT systems must be controlled, approved, and monitored.
- Direct access to Level 2 and below must be restricted and mediated through approved intermediate systems.
- Access mechanisms must support authentication, authorization, and accountability.
- Privileged access must be limited to defined roles and controlled based on operational need.

6.2.2 Implementation Considerations

- Remote access should be implemented using secure access methods such as VPNs, jump hosts, or access brokers.
- MFA should be used for remote and privileged access where technically feasible.
- Systems should enforce session timeouts, inactivity lockouts, and restrictions on concurrent sessions where supported.
- Domain-based authentication should be used where feasible; local accounts should be minimized and tightly controlled.
- Access events should be logged and monitored to support accountability and incident response.

6.2.3 Importance Explanation

Identity and access control defines how users and systems interact with OT environments. Unlike IT environments, OT access must balance security with operational availability and safety. In OT systems, access control applies to:

- Operators interacting with control systems
- Engineers performing maintenance and configuration
- Vendors providing support and troubleshooting
- Administrators managing infrastructure and security systems

6.2.4 Analogy

Access control is similar to key management in a facility. Each person is issued keys based on their role. Some keys open only specific rooms, while others provide broader access. Access is granted based on responsibility, not convenience. In OT systems, user accounts and permissions represent those keys, and access paths represent controlled entry points.

6.2.5 Why it matters

- Limits unauthorized access to critical systems
- Reduces risk of accidental or malicious system changes
- Enables traceability of user actions
- Supports safe vendor and remote access
- Protects critical processes from unintended disruption.

6.2.6 Risk if not implemented

- Unauthorized access to control systems

- Inability to trace actions during incidents
- Increased likelihood of system misconfiguration or misuse
- Elevated risk from vendor or remote access pathways

6.3 Architecture and System Design (Architecture)

Defines how OT systems are structured and interconnected to support segmentation and secure operation.

6.3.1 Architecture Requirements

- OT systems must be designed using a zoned architecture with defined trust boundaries.
- Systems must implement defense-in-depth through layered security controls.
- Network segmentation must be enforced through defined zones and controlled communication paths (conduits).
- Systems must align to the Purdue model or an approved equivalent architecture.
- System design must minimize implicit trust between components and zones.
- Unsupported or legacy systems must be isolated and managed to reduce risk exposure.

6.3.2 Implementation Considerations

- System designs should define:
  - Zone boundaries
  - Communication paths between zones
  - Allowed protocols and services
- Virtualized environments should enforce workload isolation and segmentation controls.
- System placement should consider redundancy, fault tolerance, and operational continuity.
- Systems should be designed to limit lateral movement between assets and zones.
- Vendor-supplied systems should be reviewed for alignment with segmentation and architecture requirements.
- Where full segmentation is not immediately feasible, systems should be designed to support future segmentation.

6.3.3 Importance Explanation

Architecture and system design define how OT systems are structured and how they interact. Strong architecture reduces risk by controlling how systems connect and interact, rather than relying solely on configuration or monitoring controls. This includes:

- Network layout and segmentation
- System placement and interconnection
- Trust relationships between systems
- Communication paths and dependencies

6.3.4 Analogy

System architecture is similar to designing a facility layout. Walls, doors, and controlled entry points determine how people move through the building. Some areas are restricted, while others are accessible based on role and purpose. In OT systems, zones represent secured areas, and communication paths represent controlled doorways between them.

6.3.5 Why it matters

- Limits propagation of failures and cyber events
- Reduces attack surface and lateral movement
- Supports safe and predictable system behavior

- Enables effective monitoring and control of system interactions
- Simplifies troubleshooting and system maintenance

6.3.6 Risk if not implemented

- Flat networks increase exposure and risk propagation
- Lack of segmentation allows uncontrolled system interaction
- Increased likelihood of cascading failures
- Difficulty isolating incidents or performing maintenance

6.4 Communication and Network Security (Architecture)

Defines how communication between OT systems is controlled and restricted.

6.4.1 Architecture Requirements

- Communication between OT systems must be restricted to defined and approved paths.
- Traffic between security zones must be controlled through enforcement points (e.g., firewalls or equivalent).
- Communication must follow least privilege principles, allowing only required protocols and services.
- Direct internet connectivity from OT systems must be prohibited unless explicitly approved.
- External connectivity must be limited, controlled, and monitored.

6.4.2 Implementation Considerations

- Firewall rules should be explicitly defined with documented justification for allowed traffic.
- Firewall rules should be reviewed periodically to ensure continued necessity and accuracy.
- VLANs and ACLs should be used to enforce segmentation and restrict inter-zone communication.
- Protocol use should be limited to required functionality and aligned with approved use cases.
- External-facing interfaces should be disabled unless required and approved through risk-based review.
- DMZ architectures should be used to isolate systems requiring external or cross-network communication.
- Communication flows should be documented as part of network architecture diagrams.

6.4.3 Importance Explanation

Communication and network security define how systems exchange data and how that communication is controlled. In OT environments, communication control applies to:

- System-to-system data exchange
- Control signals between devices
- External connections to vendors or enterprise systems

6.4.4 Analogy

Communication control is similar to controlling traffic between secured areas. Checkpoints determine who can pass between areas and under what conditions. Only authorized routes are allowed, and all other paths are blocked. In OT systems, firewalls, ACLs, and segmentation boundaries act as those checkpoints.

6.4.5 Why it matters

- Prevents unauthorized system interaction
- Limits attack surface and exposure
- Reduces risk of lateral movement between systems
- Supports controlled integration with enterprise and external systems

- Improves visibility into system communication behavior.

6.4.6 Risk if not implemented

- Uncontrolled communication paths between systems
- Increased exposure to external threats
- Difficulty identifying and isolating malicious activity
- Increased likelihood of cascading impacts across systems

6.5 Monitoring and Detection (Architecture)

Defines how system activity is observed to detect abnormal or unauthorized behavior.

6.5.1 Architecture Requirements

- OT systems must generate logs that support visibility into authentication, system activity, and configuration changes.
- Monitoring capabilities must be implemented in a manner that does not disrupt OT operations.
- Monitoring must support detection of abnormal or unauthorized activity within OT environments.
- Monitoring solutions must account for OT-specific protocols and system behaviors.

6.5.2 Implementation Considerations

- Logs should be forwarded to centralized monitoring platforms where technically feasible.
- Passive monitoring techniques should be used where active methods introduce operational risk.
- Monitoring systems should be configured to recognize OT/ICS protocols and expected communication patterns.
- Detection thresholds should be tuned to reduce noise while maintaining visibility into meaningful events.
- Time synchronization should be implemented across systems to support accurate event correlation.
- Monitoring coverage should prioritize critical systems and high-risk communication paths.

6.5.3 Importance Explanation

Monitoring and detection provide visibility into system behavior and enable identification of abnormal or unauthorized activity. In OT environments, monitoring must balance security visibility with operational safety and system stability. Monitoring applies to:

- User activity and access events
- System configuration changes
- Network communication patterns
- Device and process behavior

6.5.4 Analogy

Monitoring is similar to surveillance in a facility. Cameras and sensors observe activity and alert when something unexpected occurs. They do not interfere with operations but provide visibility into what is happening. In OT systems, logs and monitoring tools provide that visibility into system behavior.

6.5.5 Why it matters

- Enables detection of unauthorized or abnormal activity
- Supports incident response and investigation
- Provides visibility into system behavior and communication patterns
- Helps identify misconfigurations and operational issues
- Supports accountability and audit requirements.

6.5.6 Risk if not implemented

- Limited visibility into system activity
- Delayed detection of incidents or abnormal behavior
- Increased difficulty in investigating events
- Increased risk of undetected system compromise or misuse

6.6 Operational Resilience (Architecture)

Defines how OT systems maintain availability and recover from disruption.

6.6.1 Architecture Requirements

- OT systems must be designed to support continuity of operations under failure or degraded conditions.
- Critical systems must include redundancy or failover capability where required by operational needs.
- Systems must support restoration from backup to a known-good state.
- System design must account for dependencies that could impact availability or recovery.

6.6.2 Implementation Considerations

Backup processes should be implemented with defined schedules, retention, and validation procedures that account for the potential of long-duration adversary presence and delayed activation of malicious code. Backup retention should include multiple historical points over extended timeframes to support recovery from undetected compromise and restore systems to a known-good state prior to compromise.

- Backup data should be stored securely and protected from unauthorized modification or loss.
- Restoration procedures should be tested periodically to confirm recoverability.
- High-availability configurations should be implemented where system criticality requires continuous operation.
- Maintenance and patching activities should be planned to minimize operational impact.
- System dependencies should be documented to support recovery and troubleshooting efforts.

6.6.3 Importance Explanation

Operational resilience ensures that OT systems can continue to function or be restored quickly in the event of failure, disruption, or cybersecurity incident. In OT environments, resilience is critical because system downtime can directly impact physical processes, safety, and service delivery. Resilience applies to:

- System availability and failover
- Backup and recovery capabilities
- System dependencies and interconnections
- Planned maintenance and operational continuity

6.6.4 Analogy

Operational resilience is similar to having backup systems and contingency plans in a facility. If one system fails, another takes over or the system can be restored quickly, allowing operations to continue with minimal disruption.

6.6.5 Why it matters

- Reduces impact of system failures and cyber incidents
- Supports safe and continuous operation of physical processes
- Enables faster recovery and restoration
- Improves system reliability and availability
- Supports planned maintenance without disrupting operations.

6.6.6 Risk if not implemented

- Extended system downtime
- Inability to recover systems after failure or incident
- Increased operational disruption
- Greater risk to safety and service delivery

6.7 Physical and Environmental Security (Architecture)

Defines how OT systems are protected from physical access, tampering, and environmental conditions.

6.7.1 Architecture Requirements

- Physical access to OT systems must be controlled based on asset criticality.
- Critical OT systems must be protected from unauthorized physical access and tampering.
- Physical security controls must support the protection of control system infrastructure and supporting assets.

6.7.2 Implementation Considerations

- Physical access control systems should be implemented to restrict access to control system environments.
- Access events should be logged and retained where supported.
- Surveillance systems should be used where required to monitor sensitive areas.
- Control system hardware should be deployed in secured or restricted-access locations.
- Environmental protections (e.g., power, temperature, humidity) should be implemented to support system reliability.

6.7.3 Importance Explanation

Physical and environmental security protect OT systems from direct access, tampering, and environmental conditions that could impact system operation. In OT environments, physical access often provides a direct path to control systems and infrastructure. This includes:

- Control panels and cabinets
- Network equipment and communication infrastructure
- Servers and workstations supporting OT systems

6.7.4 Analogy

Physical security is similar to securing a control room or equipment enclosure. Locks, restricted access, and monitoring ensure that only authorized personnel can interact with critical systems.

6.7.5 Why it matters

- Prevents unauthorized access to control systems
- Reduces risk of tampering or accidental damage
- Protects system integrity and availability
- Supports safe and reliable operation.

6.7.6 Risk if not implemented

- Unauthorized physical access to systems
- Increased risk of tampering or system disruption
- Potential safety and operational impacts

7.0 Configuration Standards

Configuration standards establish requirements for configuring OT systems in accordance with approved secure baselines and supporting safe, reliable OT operations.

7.1 Asset Management (Configuration)

Defines how OT assets are identified, documented, and organized to support visibility and control.

7.1.1 Implementation Considerations

- Asset discovery mechanisms should be implemented to identify connected assets where technically feasible.
- Asset inventory systems should be configured to capture and maintain required asset attributes.
- Asset records should be updated following changes to configuration, location, or ownership.
- Asset identifiers should remain consistent across systems to support traceability.
- Systems managing asset data should be secured and access controlled.
- Asset inventory data should be integrated with approved systems of record where applicable.
- Standalone or non-networked assets should be documented or managed through approved exception processes.

7.1.2 Importance Explanation

Asset management ensures that systems are properly identified, tracked, and maintained throughout their lifecycle. In OT environments, accurate asset data supports system configuration, troubleshooting, and lifecycle management.

7.1.3 Analogy

Asset management is similar to maintaining an equipment register in a facility where each component is tracked, labeled, and recorded for maintenance and replacement.

7.1.4 Why it matters

- Enables accurate system configuration and maintenance
- Supports troubleshooting and incident response
- Reduces risk of unmanaged or unknown systems
- Improves visibility into system state and ownership

7.1.5 Risk if not implemented

- Incomplete or inaccurate asset data
- Increased risk of unmanaged systems
- Difficulty troubleshooting or responding to incidents
- Increased likelihood of configuration errors

7.2 Identity and Access Control (Configuration)

Defines how access to OT systems is controlled, authenticated, and monitored.

7.2.1 Implementation Considerations

- Systems should enforce unique user authentication.
- Default accounts should be disabled or removed prior to production use.
- Authentication mechanisms should enforce password policy requirements.
- Privileged access should be restricted and auditable.
- Remote access should be implemented using approved secure access methods such as VPNs or jump

hosts.
- Systems should enforce session timeout, inactivity lockout, and limitations on concurrent sessions where supported.
- Domain-based authentication should be used where feasible; local accounts should be minimized and tightly controlled.
- Access events should be logged and monitored.

7.2.2 Importance Explanation

Identity and access control ensures that only authorized users and systems can interact with OT environments and that those interactions are traceable.

7.2.3 Analogy

Access control is similar to issuing keys based on role and responsibility, where each key provides access only to authorized areas.

7.2.4 Why it matters

- Prevents unauthorized access to critical systems
- Reduces risk of accidental or malicious system changes
- Enables traceability of user actions
- Supports controlled vendor and remote access

7.2.5 Risk if not implemented

- Unauthorized access to systems
- Inability to trace user actions
- Increased risk of misuse or misconfiguration
- Elevated risk from remote or vendor access

7.3 Architecture and System Design (Configuration)

Defines how OT systems are structured and interconnected to support segmentation and secure operation.

7.3.1 Implementation Considerations

- Systems should be configured using approved hardened baselines.
- Only required services, ports, and protocols should be enabled.
- Insecure or legacy protocols should be disabled unless explicitly approved.
- Systems should be configured to support segmentation and isolation requirements.
- Systems should synchronize time with approved time sources.
- Virtualized systems should enforce isolation between workloads.

7.3.2 Importance Explanation

Configuration of system architecture ensures that systems operate securely within their intended design and do not introduce unnecessary risk through misconfiguration.

7.3.3 Analogy

System configuration is similar to setting up machinery correctly before operation, ensuring all controls and settings function as intended.

7.3.4 Why it matters

- Reduces attack surface
- Supports system stability and predictability
- Prevents unintended system behavior
- Aligns system operation with architectural intent

7.3.5 Risk if not implemented

- Increased exposure to threats
- System instability or unexpected behavior
- Misalignment with network segmentation
- Increased likelihood of compromise

7.4 Communication and Network Security (Configuration)

Defines how communication between OT systems is controlled and restricted.

7.4.1 Implementation Considerations

- Firewall rules should enforce least privilege communication paths.
- Network devices should restrict inter-zone traffic to approved flows only.
- VLANs and ACLs should be configured to enforce segmentation.
- External-facing interfaces should be disabled unless explicitly required and approved.
- DMZ systems should be hardened and isolated from internal control networks.

7.4.2 Importance Explanation

Configuration of communication controls ensures that systems only exchange necessary data and that communication is restricted to approved paths.

7.4.3 Analogy

Communication control is similar to regulating traffic through checkpoints where only authorized routes are permitted.

7.4.4 Why it matters

- Prevents unauthorized communication
- Reduces exposure to external threats
- Limits lateral movement
- Supports controlled system interaction

7.4.5 Risk if not implemented

- Uncontrolled communication between systems
- Increased exposure to threats
- Difficulty detecting abnormal activity
- Increased risk of cascading failures

7.5 Monitoring and Detection (Configuration)

Defines how system activity is observed to detect abnormal or unauthorized behavior.

7.5.1 Implementation Considerations

- Systems should generate logs for authentication, configuration changes, and system activity.

- Logs should be forwarded to centralized monitoring systems where feasible.
- Logging configurations should be protected from unauthorized modification.
- Monitoring tools should be configured to avoid disruption of OT operations.

7.5.2 Importance Explanation

Monitoring and detection provide visibility into system behavior and support identification of abnormal or unauthorized activity.

7.5.3 Analogy

Monitoring is similar to surveillance systems that observe activity without interfering with operations.

7.5.4 Why it matters

- Enables detection of abnormal behavior
- Supports incident response
- Provides system visibility
- Improves operational awareness

7.5.5 Risk if not implemented

- Limited visibility into system activity
- Delayed detection of issues
- Increased risk of undetected compromise
- Reduced ability to investigate incidents

7.6 Operational Resilience (Configuration)

Defines how OT systems maintain availability and recover from disruption.

7.6.1 Implementation Considerations

- Backup processes should be configured and operational prior to system acceptance.
- Backup data should be validated periodically.
- Systems should support restoration from backup.
- High-availability configurations should be implemented where required by system criticality.

7.6.2 Importance Explanation

Operational resilience ensures systems can continue operating or be restored quickly after disruption.

7.6.3 Analogy

Resilience is similar to having backup systems in place to continue operations when primary systems fail.

7.6.4 Why it matters

- Reduces downtime
- Supports recovery after incidents
- Improves system reliability
- Enables continued operations

7.6.5 Risk if not implemented

- Extended downtime
- Inability to recover systems

- Increased operational disruption
- Greater impact from failures

7.7 Physical and Environmental Security (Configuration)

Defines how OT systems are protected from physical access, tampering, and environmental conditions.

7.7.1 Implementation Considerations

- Physical access control systems should enforce role-based access where implemented.
- Physical security systems should log access events where supported.
- Control system hardware should be deployed in secured or restricted-access locations.
- Environmental protections should be implemented to support system reliability.

7.7.2 Importance Explanation

Physical and environmental security protect systems from direct access, tampering, and environmental conditions that could impact operation.

7.7.3 Analogy

Physical security is similar to securing equipment rooms with locks and controlled access.

7.7.4 Why it matters

- Prevents unauthorized physical access
- Reduces risk of tampering or damage
- Supports reliable system operation
- Protects critical infrastructure

7.7.5 Risk if not implemented

- Unauthorized access to systems
- Increased risk of tampering
- Potential system disruption
- Safety and operational impacts

8.0 Governance Standards

Governance standards establish ownership, accountability, and oversight of OT systems and controls.

8.1 Asset Management (Governance)

Defines how OT assets are identified, documented, and organized to support visibility and control.

8.1.1 Implementation Considerations

- Asset ownership should be assigned and documented.
- Asset inventories should be reviewed periodically for accuracy and completeness.
- Processes should exist for onboarding, modification, and decommissioning of assets.
- Asset management processes should be subject to periodic audit.

8.1.2 Importance Explanation

Governance ensures that asset management processes are consistently applied and maintained.

8.1.3 Analogy

Asset management governance is similar to maintaining an official registry of equipment ownership, where each asset has a designated owner responsible for its condition, use, and lifecycle.

8.1.4 Why it matters

- Ensures accountability
- Maintains inventory accuracy
- Supports lifecycle management

8.1.5 Risk if not implemented

- Lack of ownership and accountability
- Inaccurate or outdated inventories
- Increased operational risk

8.2 Identity and Access Control (Governance)

Defines how access to OT systems is controlled, authenticated, and monitored.

8.2.1 Implementation Considerations

- Access control models should be defined based on job function.
- Access provisioning and deprovisioning should follow approved processes.
- Access rights should be reviewed periodically.
- Exceptions for shared or elevated access should be documented and approved.

8.2.2 Importance Explanation

Governance ensures access controls are applied consistently and remain appropriate over time.

8.2.3 Analogy

Identity and access governance is similar to managing access permissions for a facility, where roles determine who is allowed access, and access is reviewed and adjusted over time.

8.2.4 Why it matters

- Maintains least privilege
- Reduces risk of unauthorized access
- Ensures accountability

8.2.5 Risk if not implemented

- Excessive or inappropriate access
- Increased security risk
- Lack of auditability

8.3 Architecture and System Design (Governance)

Defines how OT systems are structured and interconnected to support segmentation and secure operation.

8.3.1 Implementation Considerations

- Network segmentation and architecture changes should be reviewed and approved.
- Architecture documentation should be maintained and updated.
- Hardening baselines should be approved and maintained.

- System design decisions should be documented and traceable.

8.3.2 Importance Explanation

Governance ensures architectural decisions are controlled, consistent, and aligned with standards.

8.3.3 Analogy

Architecture governance is similar to maintaining approved building plans, where changes must be reviewed and approved to ensure the structure remains consistent and safe.

8.3.4 Why it matters

- Maintains system consistency
- Supports secure design
- Ensures traceability

8.3.5 Risk if not implemented

- Inconsistent system design
- Increased risk exposure
- Lack of documentation and control

8.4 Communication and Network Security (Governance)

Defines how communication between OT systems is controlled and restricted.

8.4.1 Implementation Considerations

- Communication protocols should be approved based on operational need.
- Firewall rule changes should follow formal processes.
- External connectivity should be risk-assessed and approved.

8.4.2 Importance Explanation

Governance ensures communication controls are managed and maintained appropriately.

8.4.3 Analogy

Communication governance is similar to managing approved routes between secured areas, where only authorized pathways are allowed and changes must be reviewed before being opened.

8.4.4 Why it matters

- Prevents unauthorized connectivity
- Maintains control over system communication
- Supports secure integration

8.4.5 Risk if not implemented

- Uncontrolled communication paths
- Increased exposure to threats
- Misconfiguration risk

8.5 Monitoring and Detection (Governance)

Defines how system activity is observed to detect abnormal or unauthorized behavior.

8.5.1 Implementation Considerations

- Responsibilities for monitoring and response should be defined.
- Monitoring coverage should be reviewed periodically.
- Logging and detection policies should be maintained.

8.5.2 Importance Explanation

Governance ensures monitoring systems are actively managed and effective.

8.5.3 Analogy

Monitoring governance is similar to assigning responsibility for reviewing security camera footage, ensuring that activity is observed, evaluated, and acted upon when necessary.

8.5.4 Why it matters

- Maintains visibility into systems
- Supports incident response
- Ensures monitoring effectiveness

8.5.5 Risk if not implemented

- Gaps in monitoring coverage
- Delayed incident detection
- Reduced situational awareness

8.6 Operational Resilience (Governance)

Defines how OT systems maintain availability and recover from disruption.

8.6.1 Implementation Considerations

- Disaster recovery and backup processes should have defined ownership.
- Recovery procedures should be tested and reviewed periodically.
- Change management processes should be enforced.
- System dependencies should be documented and maintained.

8.6.2 Importance Explanation

Governance ensures resilience processes are maintained and effective.

8.6.3 Analogy

Operational resilience governance is similar to maintaining and testing emergency response plans, where responsibilities are assigned and procedures are regularly reviewed to ensure readiness.

8.6.4 Why it matters

- Supports system recovery
- Maintains operational continuity
- Ensures preparedness

8.6.5 Risk if not implemented

- Inadequate recovery capability
- Increased downtime

- Operational disruption

8.7 Physical and Environmental Security (Governance)

Defines how physical access to OT systems is governed and controlled based on defined policies and responsibilities.

8.7.1 Implementation Considerations

- Physical access policies should be defined and enforced based on asset criticality.
- Physical access permissions should be assigned, reviewed, and revoked through defined processes.
- Physical access logs should be reviewed periodically where available.
- Responsibilities for physical security of OT systems should be clearly assigned and documented.

8.7.2 Importance Explanation

Governance of physical and environmental security ensures that access to OT systems is controlled, accountable, and consistently managed.

8.7.3 Analogy

Physical security governance is similar to managing access permissions for secured facilities, where access is granted, reviewed, and revoked based on defined roles and responsibilities.

8.7.4 Why it matters

- Ensures accountability for physical access
- Supports consistent enforcement of access controls
- Reduces risk of unauthorized or unmanaged access
- Aligns physical security with system criticality

8.7.5 Risk if not implemented

- Lack of accountability for physical access
- Inconsistent or unmanaged access permissions
- Increased risk of unauthorized access or tampering
- Reduced effectiveness of physical security controls

9.0 Planned Compliance and Roadmap Governance

Cybersecurity requirements defined in these standards represent the target state for OT systems. Systems must not be considered compliant unless requirements are met or an approved exception or remediation plan is in place.

- Systems that do not meet these requirements must be identified and documented through formal assessment.
- Gaps must be evaluated based on risk, operational impact, and system criticality.
- Remediation activities must be defined, prioritized, and tracked.
- Progress toward compliance must be managed through an approved improvement plan.

Unmet requirements are permitted only when:

- The gap is documented
- Risk is assessed and accepted at the appropriate level
- A defined remediation plan exists

10.0 Implementation and Turnover Guidance

This section provides guidance on how cybersecurity requirements should be implemented and validated during system delivery and turnover.

Cybersecurity requirements defined in this document represent the target state for OT systems. New systems should be delivered in alignment with this target state wherever technically feasible.

For systems that are not yet fully aligned:

- Gaps should be identified through assessment.
- Risks should be evaluated based on system criticality and operational impact.
- Remediation activities should be defined and prioritized.
- Progress toward alignment should be tracked and managed.

10.1 Implementation Expectations

System integrators, vendors, and project teams should design and implement systems to:

- Align with defined architecture standards, including segmentation and controlled communication paths
- Apply secure configuration baselines during system build and commissioning
- Remove default credentials and disable unnecessary services prior to production use
- Implement access controls consistent with defined identity and access requirements

10.2 Turnover Artifacts

To support secure operations and lifecycle management, the following artifacts should be produced during system delivery:

- Asset Inventory
  - Includes system components, network identifiers, and system roles
- Network Architecture Documentation
  - Reflects as-built connectivity, segmentation, and communication paths
- Configuration Backups
  - Enables restoration of systems to a known-good state
- Account and Access Documentation
  - Identifies user and administrative accounts and confirms removal of default credentials

10.3 Acceptance and Validation

System acceptance should consider cybersecurity requirements as part of overall project delivery.

- Delivered systems should be reviewed against defined standards
- Deviations should be documented and managed through approved processes
- Systems should not rely on undefined or unmanaged risk conditions

11.0 Standard Exceptions

This section defines requirements for managing deviations from these standards. These requirements apply to both new systems and existing systems operating under planned remediation.

- Exceptions must be formally documented and approved prior to implementation.
- Each exception must include a documented risk assessment and defined compensating controls.
- Exception approvals must align to defined authority based on risk level.
- Exceptions must have defined expiration dates and be reviewed periodically.
- A centralized record of active exceptions must be maintained and reviewed on a defined schedule.

12.0 Policy Compliance

- Systems and projects must demonstrate compliance with these standards prior to acceptance.
- All employees, contractors, vendors, and service providers with access to OT systems must comply with these standards.
- These standards are effective upon approval by the designated authority.
- Compliance with these standards is subject to audit and review. Non-compliance must be addressed through defined remediation or exception processes.
-

13.0 Approval

Approver Name	Approver Role or Title	Signature and Date (Digital or Wet)
Roger Caslow	CISO	
	Chief Engineer	
Bill Fosket	OT Cyber Manager	

14.0 Version History

Effective Date	Brief Description of Version or Change	Primary Author
04/30/2026	Initial version.	Bill Fosket