



APTA SS-TCS-RP-003-26

First Published: September 28, 2026

Transit Cybersecurity Working Group

Operational Technology Cybersecurity Maturity Framework

Part 2: OT-CMF Tactical Guidance for Implementing and Maturing Operational Technology Rail Cyber Systems

Abstract: This document provides tactical and strategic guidance for implementing the APTA Operational Technology Cybersecurity Maturity Framework (OT-CMF) across transit agency environments. It serves as the practical companion to [APTA SS-CCS-RP-006-23](#), “Operational Technology Cybersecurity Maturity Framework (OT-CMF) Overview,” enabling agencies to translate maturity framework principles into measurable, sustainable progress. Developed for agencies at all stages of cybersecurity development, this guidance is designed to help transit teams launch, assess and evolve operational technology (OT) cybersecurity programs tailored to the complex realities of public transportation systems.

Keywords: building automation systems (BAS), bus depot, communications-based train control (CBTC), cybersecurity, implementation roadmap, industrial control systems (ICS), operational technology (OT), OT-CMF, positive train control (PTC), radio, signaling, supervisory control and data acquisition (SCADA), vehicles

Summary: This tactical implementation guide helps transit agencies apply the APTA OT-CMF in operational settings. It presents structured actions for each of the six maturity levels, offering accessible steps, templates and checklists to support internal assessment, control implementation and leadership alignment. The document also defines return on investment rationale, maturity progression rules and criteria for advancing cybersecurity capability across domains. While the 2023 OT-CMF overview describes the six maturity levels and associated domains, this tactical guide defines what each level looks like in practice. It offers realistic examples, tier-based checklists and proven strategies based on agency feedback and national guidance (e.g., NIST, IEC 62443 and CISA). This structure allows agencies at any starting point to advance cybersecurity outcomes while aligning with broader sector and federal expectations.



Foreword

The American Public Transportation Association is a standards development organization in North America. The process of developing standards is managed by the APTA Standards Program's Standards Development Oversight Council (SDOC). These activities are carried out through several standards policy and planning committees that have been established to address specific transportation modes, safety and security requirements, interoperability, and other topics.

APTA used a consensus-based process to develop this document and its continued maintenance, which is detailed in the [manual for the APTA Standards Program](#). This document was drafted in accordance with the approval criteria and editorial policy as described. Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

This document was prepared by the Transit Cybersecurity Working Group, as directed by the Security and Emergency Management Standards Policy and Planning Committee.

This document represents a common viewpoint of those parties concerned with its provisions, namely transit operating/planning agencies, manufacturers, consultants, engineers and general interest groups. The application of any recommended practices or guidelines contained herein is voluntary. APTA standards are mandatory to the extent incorporated by an applicable statute or regulation. In some cases, federal and/or state regulations govern portions of a transit agency's operations. In cases where there is a conflict or contradiction between an applicable law or regulation and this document, consult with a legal adviser to determine which document takes precedence.

This is a new document.



Table of Contents

Foreword	ii
Participants.....	vi
Introduction.....	vii
Scope and purpose	vii
1. OT-CMF overview and justification	1
1.1 Maturity levels overview	1
1.2 OT-CMF implementation benefits.....	2
1.3 Budget justification and funding alignment.....	3
1.4 Making the case for maturity-level investments.....	3
1.5 Understanding cybersecurity maturity	4
1.6 Transit system standardization.....	5
1.7 Successful implementation of security controls.....	5
1.8 NIST program management controls.....	6
2. Understanding the OT-CMF maturity levels	6
2.1 Six-level framework overview.....	6
2.2 Maturity progression guidance.....	7
2.3 Role of domains and controls in maturity progression	7
2.4 Supplemental control implementation information	7
2.5 Planning for implementation of Tier 1 OT-CMF controls.....	8
3. OT-CMF quick start: Initial assessment and Level 1	9
3.1 Quick start guidance	9
3.2 Understanding levels and tiers	9
3.3 Using the pre-assessment tool.....	10
3.4 Performing a domain-by-domain gap analysis	11
3.5 Building the OT asset inventory and architecture map.....	11
3.6 Integrating risk and business impact into the assessment	12
3.7 Creating a practical action plan.....	12
3.8 Maturity roadmap planning.....	13
4. Implementing basic tenets of the OT-CMF (Tier 1)	14
4.1 Getting started: Prioritization and planning.....	14
4.2 Descriptions of key Tier 1 controls.....	15
4.3 Real-world implementation tips.....	16
4.4 Network segmentation and zoning.....	16
4.5 Success indicators	18
5. Transitioning from Tier 1 to Tier 2 controls	19
5.1 Implementing Level 2 (Tier 1 controls).....	19
5.2 Implementing Level 3 (Tier 2 controls).....	21
5.3 Preparing to govern and measure performance.....	23
6. Tools and practices beyond Level 3 maturity	23
6.1 Cybersecurity performance metrics	24



6.2 Continuous monitoring tools.....	24
6.3 Segmentation, governance and validation	24
6.4 Configuration and change validation	25
6.5 Incident response exercises.....	25
6.6 Vendor cybersecurity oversight	25
6.7 Integration of enterprise risk management.....	25
6.8 Governance	25
6.9 Change control request	28
6.10 Change Advisory Board.....	29
6.11 Example workflows (summarized)	29
6.12 OT life cycle management checklist.....	29
6.13 Vendor cybersecurity compliance checklist.....	30
6.14 OT risk register template.....	31
6.15 Key performance indicators	31
6.16 Integrating cybersecurity with physical safety and security	32
Related APTA standards.....	34
References.....	34
Definitions.....	36
Abbreviations and acronyms.....	38
Document history	39
Appendix A: CISA recommended practices.....	40
Appendix B: OT-CMF maturity levels – implementation reference.....	41
Appendix C: Facility risk assessment template	42
Appendix D: Shared log integration workflow	43
Appendix E: OT-CMF quick-start visual progress tracker.....	44
Appendix F: Small agency toolkit	45
Appendix G: Mature agency toolkit.....	47
Appendix H: Sample Change Control Request Form template.....	49
Appendix I: How Tier 3 is used in practice.....	50
Appendix J: Joint response plan sample	52
Appendix K: Out-of-scope item discussion	53

List of Figures and Tables

Table 1 Benefits of OT-CMF Implementation.....	3
Table 2 Practical Decision Chart.....	8
Table 3 Understanding Levels and Tiers.....	10



Table 4	OT-CMF Pre-Assessment Tool.....	10
Table 5	Maturity Level Target Chart.....	13
Table 6	Maturity Goals by OT-CMF Domain.....	13
Table 7	Tier 1 Implementation Planning Example.....	15
Table 8	Sample OT Governance Maturity Checklist	27
Figure 1	Sample Cybersecurity RACI Chart.....	28
Table 9	Integration Checklist	32
Table 10	Collaboration Protocols.....	33



Participants

The American Public Transportation Association greatly appreciates the contributions of **Ahmed Idrees, Sound Transit, CCSWG sub-chair**, primary writers, Michael A. Echols, Ahmed Idrees, Dr. Julius Smith, Tim Coogan, Mark Johnston, Jack Odeen, Rafi Khan, Kenneth Blackwell, Matthew Dimmick and the **OT-CMF Tactical Guide Sub-Group**, who provided the primary effort in the drafting of this document.

At the time this standard was completed, the working group included the following members:

Dr. Julius Smith, *Dallas Areas Rapid Transit*, Chair
Timothy Coogan, *Regional Transportation District*, Vice Chair
Matthew Dimmick, *STV Inc.*, Secretary

Leslie Barnes, *WDG Consulting*
Kenneth Blackwell, *VTA*
Carl Buck, *TSE*
Anthony Canderini, *Google Mandiant*
Sangetta Chomal, *Alstom*
Mike Curnow, *AECOM*
Mark Curry, *Secheron*
Juan Degree-Hayes, *TSA*
Todd Ellis, *Hatch LTD*
George Fosu, *AECOM*
Jessie Gill, *BCRTD*
Michael Godfrey, *WDG Consulting*
Patrick Guest, *NICTD*
Kevin Harnett, *IOACTIVE*
Susan Howard, *Michael Baker*
Shaked Kafzan, *Cervello*
Rafi Khan, *NJ Transit*
Danielle Jablanski, *STV*
Breanna Johnson, *TSA*
Mark Johnston, *TriMet*

Rachel Gragg, *CATS*
Alan Jones, *Lextran*
Jerry Joyce, *Hatch LTD*
Tri Le, *Armand*
Chris McKay, *TSA*
David Moskowitz, *CATS*
Marvin Muhumusa, *WMATA*
Charlotte Muller, *Cylus*
Abayomi Muse, *Safety Transit Solutions*
Jack Oden, *Parsons*
Giampaolo Orrigo, *Alstom*
Erin Plemons, *ENSCO*
Mark Salsberg, *WGD Consulting*
Miki Shifman, *Cylus*
Edward Taylor, *TSA*
Jerrica Terry, *TSA*
Dave Teumim, *Teumim Technical LLC*
Paul Townsend, *TSA*
Catrina Tran, *TSA*
Joel Waugh, *WMATA*
Jessica Weiland, *Wonderment*

Project team

Polly Hanson, *American Public Transportation Association*
Brian Heanue, *American Public Transportation Association*
Michael Echols, *Max Cybersecurity LLC, MBA, CISSP*



Introduction

This introduction is not part of APTA SS-TCS-RP-003-26, “Operational Technology Cybersecurity Maturity Framework.”

The OT-CMF is designed for transit agencies to systematically launch and mature their OT cybersecurity programs. It includes the following:

- **Tiered maturity levels (0–5):** These levels span from “on-ramp” (Level 0) through to the most advanced state (Level 5, Optimized). The baseline realistic target is commensurate with size, mission and resources. These are described in detail in [APTA SS-CCS-RP-006-23](#), “Operational Technology Cybersecurity Maturity Framework (OT-CMF) Overview.”
- **Interpretative guidance:** For each step within a tier, there’s a brief discussion on how to apply it in OT contexts, including transit and ICS specifics.
- **Implementation support:** This implementation guide goes deeper into building-block elements for maturing cybersecurity programs.

This tactical implementation guide provides a hands-on companion to the OT-CMF by translating its maturity levels into tangible, repeatable practices. This guide uses OT-CMF maturity levels to assess program maturity and control tiers to sequence implementation actions. It is designed to support both executive leaders and OT practitioners as they assess, build and operationalize cybersecurity controls.

By following this guidance, agencies can methodically build OT security resilience, reduce cybersecurity risk and prepare for emerging digital threats.

APTA recommends the use of this document by:

- individuals or organizations that operate rail transit systems;
- individuals or organizations that contract with others for the operation of rail transit systems; and
- individuals or organizations that influence how rail transit systems are operated (including but not limited to consultants, designers and contractors).

Scope and purpose

This recommended practice supplements—not replaces—existing safety, cybersecurity or regulatory standards. It equips transit agencies with a scalable, domain-based roadmap for advancing OT cybersecurity maturity. Agencies of all sizes and capacities can use this guide to assess where they stand, identify high-impact gaps and implement critical controls aligned to their operational risk. The document is also intended to unify how security is defined across transit agencies, supporting shared benchmarks and investment planning. Through this approach, APTA empowers agencies to build defensible, adaptable OT security programs that serve both mission and safety imperatives.

Operational Technology Cybersecurity Maturity Framework

Part 2: OT-CMF Tactical Guidance for Implementing and Maturing Operational Technology Rail Cyber Systems

1. OT-CMF overview and justification

1.1 Maturity levels overview

A transit agency is a complex organization with assets and equipment managed through supervisory control and communications systems housed in office buildings, depots, hubs, stations, and along rail corridors. These systems operate across the network—in wayside bungalows, signal houses, tunnels, maintenance yards, power and refueling stations, storage facilities, garages, and both local and central operations control rooms—to support safe and efficient service.

Failing to establish an OT cybersecurity program presents real risks. This is particularly true in transportation environments where system interdependencies are tightly linked to safety. An absence of cybersecurity awareness and management can leave critical operations vulnerable to disruption, compromise and potential safety risk.

Developing OT cybersecurity maturity is critical to empowering transit operations and associated stakeholders in enhancing their cybersecurity posture and having a structured maturity plan. The APTA OT-CMF provides a practical tool designed to help transit agencies objectively assess and improve their OT security posture. It enables organizations to align their policies and technologies with industry best practices from NIST, CISA (see Appendix A), IEC 62443, APTA and other recognized standards bodies specifically around transit-focused technology.

The APTA OT-CMF defines six maturity (tier) levels, beginning with Level 0 (“On-Ramp”) through to Level 5 (“Optimized”):

- **Level 0, Baseline (On-Ramp):** Initial awareness is established and agencies begin foundational planning and alignment activities. Practices are informal or undocumented.
- **Level 1, Initiated:** Recommended controls are adopted without formal processes or documentation.
- **Level 2, Planned:** Level 1 is built upon by establishing security roles and responsibilities; a risk management program; and documented policies, procedures and processes. The agency begins to incorporate key risk indicators (KRIs) and key performance indicators (KPIs) aligned with OT-CMF guidance.
- **Level 3, Operationalized:** All recommended controls are documented, implemented and assessed at least annually. Agencies maintain and annually update improvement plans to enhance the efficiency and effectiveness of controls. This is a proactive approach to managing cybersecurity risk.

APTA SS-TCS-RP-003-26
Operational Technology Cybersecurity Maturity Framework

- **Level 4, Managed:** Continuous monitoring and orchestration tools and technologies are introduced to actively respond to and adapt to evolving threats.
- **Level 5, Optimized:** Full automation of monitoring and response is achieved using advanced technologies (including AI) that support continuous efficiency improvements, better performance and real-time reporting.

Importantly, the OT-CMF recognizes that not all agencies will reach the highest levels of maturity. Level 3 should be considered the realistic and essential target for most transit systems. At this level, agencies demonstrate a strong foundation: leadership commitment, documented policies, operational procedures, program management, performance evaluation and well-defined incident response capabilities.

Level 4 builds on this foundation by introducing optimization through technologies such as artificial intelligence and the orchestration of cybersecurity controls. Level 5 represents a future-facing goal in which decision-making is enhanced by curated data, and systems can autonomously recommend and implement policy and risk adjustments.

While some agencies may adopt selected practices from higher levels, a maturity level can be claimed only when all practices at that level are fully and consistently implemented. For example, an agency that has fully implemented all Level 3 practices and only a few from Level 4 remains at Level 3 maturity.

1.2 OT-CMF implementation benefits

Implementing the OT-CMF provides a strong return on investment (ROI) for transit agencies by creating a roadmap to enhance system reliability, reducing cybersecurity risk, improving response readiness, and enabling strategic planning aligned with federal and state mandates. While the development of an OT cybersecurity program requires upfront commitment and planning, the long-term benefits to safety, cost-efficiency, resilience and compliance significantly outweigh the initial investment.

The OT-CMF supports agency leadership by providing a structure to assess current posture, identify areas for improvement, and justify cybersecurity spending within capital and operating budgets. Rather than being viewed as a compliance exercise, implementation of the OT-CMF should be understood as an investment in organizational resilience, asset longevity and risk-informed operations. By aligning cybersecurity practices with operational priorities, the framework enables more strategic decision-making and long-term planning. It also facilitates communication between technical teams and executive leadership, creating a shared understanding of cybersecurity risks and the value of proactive mitigation.

Implementation of the OT-CMF will provide significant improvements in the following areas:

- **Asset visibility and life cycle management:** Enhanced visibility into critical field and facility assets allows for better life cycle planning, targeted maintenance and improved budgeting for tech refresh.
- **Enhanced safety and security:** Increasing cybersecurity maturity improves the resilience of control systems and contributes to safer, more secure passenger services.
- **Reduced risk of downtime and compromise:** By formalizing access control, implementing secure configurations and documenting procedures, agencies lower the likelihood of service interruptions, unplanned outages and cybersecurity incidents.
- **Improved compliance posture:** Agencies mature their ability to meet TSA Security Directive 1582-21-01E - Enhancing Public Transportation and Passenger Railroad Cybersecurity requirements, as well as aligning with NIST SP 800-82 and IEC 62443 guidance.
- **Optimized use of resources:** OT-CMF provides agencies with a roadmap for prioritizing security investments. Rather than attempting to secure everything at once, the framework enables informed decisions that match risk capacity, mission priority and budget.

APTA SS-TCS-RP-003-26
Operational Technology Cybersecurity Maturity Framework

- **Vendor management improvements:** With documented security zones and clear control expectations, agencies gain leverage in holding vendors accountable for secure configurations, updates and system behavior.
- **Crisis preparedness and response:** Agencies with mature incident response capabilities and monitoring tools respond faster to disruptions, reduce downtime and protect public trust.

1.3 Budget justification and funding alignment

The OT-CMF aids transit agencies in communicating cybersecurity investment needs by offering clear, standards-aligned language and maturity-based goals that can be linked to capital and operating budgets:

- **Capital planning integration:** Agencies can align OT-CMF level advancement goals (e.g., achieving Level 3 maturity) with capital projects, such as train control modernization or SCADA upgrades. This allows cybersecurity costs to be embedded into the life cycle of large infrastructure investments.
- **Operational cost efficiency:** As agencies mature their monitoring, logging and asset management practices, they often see reductions in recurring costs related to outages, emergency maintenance or noncompliance penalties.
- **Grant and federal funding eligibility:** Agencies that demonstrate structured cybersecurity planning using frameworks like the OT-CMF are better positioned to receive federal infrastructure funds, including DHS transit security grants and FTA capital investment grants.
- **Justifying staff resources:** Agencies can identify gaps in technical and governance staffing and build business cases for adding dedicated OT cybersecurity roles or contractor support.

1.4 Making the case for maturity-level investments

OT-CMF maturity levels represent a progression from ad hoc and undocumented practices to optimized, data-driven and resilient operations. Even modest progress toward Level 2 or Level 3 can:

- reduce audit findings and security exceptions;
- improve procurement efficiency through better scoping and technical requirements;
- enable faster system recovery after cybersecurity events;
- foster cross-functional collaboration between IT, OT, operations and engineering;
- prepare transit agencies for future and likely more prescriptive federal rules and regulations; and
- reduce costs of cybersecurity insurance.

Table 1 summarizes the tangible and strategic returns associated with OT-CMF implementation.

TABLE 1
Benefits of OT-CMF Implementation

Benefit Category	ROI Impact
Asset management	Accurate inventory, reduced obsolescence, better maintenance and life cycle management
Risk management	Fewer incidents, faster response, better resilience metrics, enhanced service reliability
Compliance	Lower audit risk, TSA SD 1582 alignment, regulatory confidence
Resource allocation	Focused investments, minimized waste, optimized staffing
System uptime	Fewer outages, improved reliability of critical systems
Public confidence	Demonstrated governance, transparency and accountability
Supply chain management	Vendors might provide better ROI impact, ensuring procurement of qualified systems and solutions, many of which are semi-custom in the OT world

APTA SS-TCS-RP-003-26
Operational Technology Cybersecurity Maturity Framework

Investments in OT cybersecurity maturity are not theoretical. These investments translate into more reliable transit service, with fewer emergency repairs and a reduced burden on frontline staff. Agencies that invest early see long-term cost savings and risk reduction.

By treating cybersecurity as a strategic investment, transit agencies that implement the OT-CMF position themselves for sustainable growth, increased resilience, and improved safety and service delivery for the passengers and communities they serve.

The OT-CMF complements other assessment frameworks but focuses specifically on the unique nature of OT environments. This includes sensors, actuators, controllers and field devices that often operate outside traditional IT cybersecurity architectures. These environments demand tailored approaches and heightened sensitivity to operational constraints and safety requirements.

By implementing the OT-CMF, agencies can:

- establish a baseline understanding of their current capabilities;
- gain system-wide visibility into their OT infrastructure;
- plan for consistent, measurable and standardized growth in cybersecurity maturity; and
- equip leadership with a management tool to guide investment, prioritization and evolution.

Achieving maturity is not about how much money is spent or how many tools are deployed. Even agencies at early maturity stages can launch effective cybersecurity programs with focused coordination and management of their OT systems. There should be no financial barriers to adopting the OT-CMF or accessing related guidance materials. While some agencies may need to engage external experts for specific best-practice implementations, such as access control configuration or risk assessment, the core resource requirements are internal: staff time, alignment of service models and targeted investment in technologies that fit the agency's needs. There are real risks associated with absent OT cybersecurity programs, including safety and security concerns with not having an understanding of interdependencies for critical systems.

1.5 Understanding cybersecurity maturity

It is important to understand the context of developing cybersecurity maturity. The OT-CMF is a tool for transit agencies and not a judgment statement. To secure the sector, transit agencies must be able to discuss the policy and technology approach that right-sizes the best practices produced by NIST, CISA and other leading standards organizations. Most transit agencies will never reach Level 4 or Level 5. The goal should be for transit agencies to reach Level 3 maturity.

Level 3 maturity will ensure that agencies have appropriate cybersecurity leadership, policies, procedures, management, evaluation programs and response capabilities. Level 4 is designed to guide agencies to optimize and integrate artificial intelligence with automation of controls. The Level 5 expectations are a goal of the future, where optimization also includes presenting decision-makers with curated information for making policy and risk adjustments that the system autonomously implements.

The OT-CMF is a companion to leading assessment tools. The focus of the OT-CMF is on OT systems and the environments that harbor sensors, actuators and controllers. It is a sensitive environment that requires special attention. Some of these components are not monitored via a traditional cybersecurity network. The OT-CMF provides a structured approach to understand the baseline of current capabilities, establishing a foundation for consistent evaluation and growth planning. It allows an organization to see the whole OT system. It is also a management tool for transit agency leadership to identify opportunities for growth, investment and evolution. Even at the lowest levels of maturity, many agencies need to plan for OT

management to deploy a successful program. Maturity does not come from spending the most money or implementing the most tools.

There should be no financial cost to develop or gain access to resources and documents that support OT-CMF implementation. While implementing best practices, like access control and risk assessment, a third-party consultant or vendor may be required to provide OT expertise. Otherwise, resource requirements are limited to staff time and the cost of service and technologies to meet an agency's requirements.

1.6 Transit system standardization

This document is designed to be a companion to APTA SS-CCS-RP-006-23, "Operational Technology Cybersecurity Maturity Framework (OT-CMF) Overview." The goal of this guide is to assist organizations to implement the principles and practices found in the OT-CMF. The OT-CMF allows a flexible application of cybersecurity best practices for OT. It creates direction on aligning cybersecurity program efforts.

APTA SS-CCS-RP-006-23 provides instructions on the following:

- Selecting cybersecurity OT controls
- Cybersecurity OT controls management
- Implementing the operations of technology controls
- Measuring the success of the OT controls
- Achieving higher OT control maturity levels

The security controls selected should be documented in the security plan to provide an overview of the security requirements for the OT security program and describe the security controls in place or planned for meeting those requirements. The controls may be applied to the security of BAS, bus depot, CBTC, cybersecurity, ICS, OT, OT PTC, radio signaling, SCADA and vehicle charging infrastructure.

When identifying and establishing potential controls, it is important to remember that a control can often apply across multiple processes, systems and/or assets in multiple operating units throughout the enterprise. These controls are referred to as "common controls." Common controls are those that, once implemented, provide a security function that is inheritable by other organizational systems and processes.

Enterprise-level controls apply across the enterprise, while common controls can be implemented at various levels. Common controls are often at the enterprise level; however, individual business units can implement common controls, which would then apply to systems and processes within that business unit. Policies and procedures developed and implemented at the enterprise level could be common to an entire organization. However, for example, a policy developed by the finance department that mandates multifactor authentications for all financial applications is not an enterprise control but would be inheritable, and therefore common, by all applicable systems in the finance department. This same perspective applies to OT security controls.

1.7 Successful implementation of security controls

Implementing controls is only the beginning of the process, and every agency must continuously adjust, maintain or improve the implemented controls. These efforts strengthen the agency's ability to carry out a risk management strategy that protects and preserves its long-term operations. From the moment controls are implemented, the agency must test controls to determine if they are adequate for the level of protection required and to ensure that they meet the established risk management objectives.

1.8 NIST program management controls

NIST program management controls, as outlined in NIST SP 800-53, provide a framework for establishing and maintaining an effective information security program at the organizational level. These controls are designed to be implemented above the system level and serve as foundational elements that support consistent cybersecurity governance across an agency's portfolio of systems and operations. Key areas include risk management strategy, information security resources, enterprise architecture alignment, and roles and responsibilities for security oversight. Unlike system-specific controls, program management controls emphasize organization-wide coordination, enabling leadership to integrate cybersecurity into strategic planning, budgeting and operational risk management. This strategic approach supports sustained cybersecurity maturity and ensures that security efforts align with mission objectives, compliance requirements and evolving threat landscapes.

The successful implementation of OT security controls depends on the successful implementation of organization-wide program management controls. The way organizations implement the program management controls depends on specific organizational characteristics including, for example, the size, complexity and mission/business requirements of the organizations.

The program management controls complement the security controls and focus on the programmatic, organization-wide information security requirements that are independent of any system and are essential for managing information security programs.

Organizations should document program management controls in the information security program plan. The organization-wide OT security plan supplements the individual security plans developed for each information system. Together, the security plans for the individual OT systems and the information security program cover the totality of security controls employed by the transit organization.

2. Understanding the OT-CMF maturity levels

2.1 Six-level framework overview

The OT-CMF defines six maturity levels that reflect the growth and advancement of an agency's OT cybersecurity capabilities. These levels allow agencies to assess their current state, define realistic goals and track progress over time.

- **Level 0, Baseline (On-Ramp):** Level 0, Baseline (On-Ramp): Initial awareness is established and agencies begin foundational planning and alignment activities. Practices are informal or undocumented.
- **Level 1, Initiated:** Policies and procedures are being drafted. Cybersecurity champions are identified. Baseline assessments are initiated.
- **Level 2, Planned:** A programmatic approach is adopted. Risk management and governance structures are in development. Strategic investments are underway.
- **Level 3, Operationalized:** Standard procedures are implemented. Incident response, training and continuous monitoring are active. Controls are enforced.
- **Level 4, Managed:** Enterprise-wide integration. Performance metrics and risk data inform operational and policy adjustments.
- **Level 5, Optimized:** Predictive and adaptive controls. Automated response capabilities. Advanced analytics and automated and adaptive decision-support capabilities are integrated with risk management.

2.2 Maturity progression guidance

Advancement through the levels requires full and consistent implementation of each level's controls and processes. Agencies should not claim a maturity level unless all practices within that level are fully met. For example, if an agency has fully implemented Level 3 practices but only partially addressed Level 4, it remains at Level 3. Each level builds on the one before. Transit agencies should not skip levels but instead use the OT-CMF as a ladder to build enduring cyber resilience.

2.3 Role of domains and controls in maturity progression

2.3.1 Levels vs. tiers (how to use this guide)

- **OT-CMF maturity levels** define the overall stage of an agency's cybersecurity capability and are used to assess and communicate program maturity.
- **OT-CMF control tiers** group controls by implementation priority and complexity and are used to guide which actions an agency should take within a given maturity level.

Control tiers support maturity progression but do not independently determine organizational maturity. Agencies progress through levels sequentially. Within each level, agencies implement controls by tier. **Tiers support levels; they do not replace them.**

The OT-CMF is organized around capability domains (e.g., asset management, incident response, configuration management). Within each domain, specific practices and controls guide implementation based on the maturity level.

- **Domains:** Focus areas where capability must be built (e.g., access control, patch management)
- **Controls:** Actionable steps or safeguards aligned to each domain
- **Tiers:** Prioritized levels of control criticality (Tier 1 = foundational, Tier 2 = strategic, Tier 3 = advanced)

Controls within each tier map directly to maturity levels. For example:

- **Tier 1** controls support Level 1 and Level 2 maturity.
- **Tier 2** controls support Level 3 maturity.
- **Tier 3** controls support Level 4 and Level 5 maturity.

2.4 Supplemental control implementation information

Depending on the actual control, excellent supplemental OT information can be found in several locations and should be used to inform control selection and implementation. The best sources of supplemental information include the following:

- **APTA SS-CCS-004-16**, "Securing Control and Communications Systems in Rail Transit Environments, Part IIb: Protecting the Operationally Critical Security Zone." This APTA document offers excellent and practical descriptions of its controls, including additional references and supplementary information.
- **NIST SP 800-82**, "Guide to Industrial Control Systems (ICS) Security." The purpose of NIST SP 800-82 is to provide guidance for securing ICS, including SCADA and DCS systems, PLCs, and other systems performing industrial control functions. In many cases it provides ICS control enhancements to NIST SP 800-53 controls by providing additional ICS supplemental guidance and ICS control tailoring. **Table 2** shows how additional ICS context is provided to a NIST SP 800-53 control.

TABLE 2
Practical Decision Chart

If the Agency Is Trying To...	Primary Source to Use	Why
Decide what controls to implement and in what order	OT-CMF	OT-CMF defines priority, sequencing and maturity alignment
Implement controls in a rail or transit environment	APTA Part IIIb	Provides transit-specific operational, safety and legacy context
Translate a control into ICS-appropriate technical safeguards	NIST SP 800-82	Adds ICS tailoring and examples to enterprise controls
Explain or defend controls to auditors, TSA or oversight bodies	OT-CMF + NIST SP 800-82	Shows prioritization and technical rigor
Design network zoning or security zones	APTA Part IIIb → NIST SP 800-82	Transit zoning first, then ICS technical depth
Handle PLC, SCADA or field device constraints	NIST SP 800-82	Addresses availability, safety and real-time constraints
Build a phased roadmap without overwhelming staff	OT-CMF	Designed explicitly for staged maturity growth

By applying controls in a phased and prioritized manner, agencies can build maturity across each domain without being overwhelmed. This structured approach ensures that cybersecurity programs grow with operational and fiscal capacity, rather than relying solely on reactive or ad hoc investments.

It's important to understand that the OT-CMF is built around capability domains. These are key areas where agencies need to develop cybersecurity strength, such as asset management, incident response and configuration management. Each domain includes specific controls, which are clear, actionable steps or safeguards to put in place. Controls are grouped into tiers based on importance:

- **Tier 1** = foundational controls (supporting early maturity levels 1 and 2)
- **Tier 2** = strategic controls (supporting Level 3)
- **Tier 3** = advanced controls (supporting higher maturity levels 4 and 5)

This structure allows agencies to work on the most critical items first, and then gradually add more advanced measures. By following the tiers in order, organizations can strengthen cybersecurity in manageable steps, building capacity over time and avoiding the chaos of purely reactive or one-off investments.

To support ease of use, the complete OT-CMF maturity level definitions and implementation characteristics are provided in Appendix B, which serves as a concise reference for agencies planning and assessing their cybersecurity maturity progression.

2.5 Planning for implementation of Tier 1 OT-CMF controls

Security controls are protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity and availability) specified for an information system. Safeguards may include security features; management constraints; personnel security; and security of physical structures, areas and devices. The following are some important considerations for security controls:

- The security controls selected, based on the security categorization of the OT, should be documented in the security plan to provide an overview of the security requirements for the OT security program.

APTA SS-TCS-RP-003-26
Operational Technology Cybersecurity Maturity Framework

- Agencies should adopt a strategic approach to implementation. The strategic approach will assist as a traffic cop for the myriad activities (i.e., governance, maintenance, investment, procurement, training) that must all work together to make an OT program successful.
- The implementation of Tier 1 controls may require the rethinking of current approaches, and new compensating controls may need to be identified.
- Organizational safety teams may need to be consulted, as the desired approach may change a long-standing process. The implementation document should describe the security controls in place or plans for meeting security requirements.
- Not all controls may be appropriate for all OT applications. HVAC systems and smart elevators may use select controls, as an example. Controls can be utilized for receiving security alerts and advisories, as well as the verification of security functions on the information system.

The agency-wide OT security program plan supplements the individual security plans developed for each organizational information system. Together, the security plans for the individual OT systems and the information security program cover the totality of security controls employed by the organization. Implementing controls is only the beginning of the process, and every agency must continuously adjust, maintain or improve the implemented controls. From the moment controls are implemented, the agency must test them to determine if they are adequate for the level of protection required to meet the established risk management objectives.

SMALL AGENCY TIP: In small organizations, cybersecurity roles may be combined. Assign key responsibilities to existing staff (e.g., IT manager, operations supervisor), and document role boundaries clearly.

3. OT-CMF quick start: Initial assessment and Level 1

3.1 Quick start guidance

Transit agencies beginning OT-CMF implementation should start with this section. The steps in this section guide agencies through the minimum activities required to establish Level 1 (Initiated) maturity and begin Tier 1 control implementation. Agencies should complete these steps before advancing to later sections of this guide.

Reference the following:

- **Appendix B:** Refer to the appendix for maturity definitions.
- **Section 4:** After completing this section, proceed to Tier 1 controls.

3.2 Understanding levels and tiers

Maturity levels describe where the agency is. (“How mature is our OT cybersecurity program?”)

Tiers describe what should be implemented next. (“Which controls should we implement at this stage?”)

This is summarized in [Table 3](#).

APTA SS-TCS-RP-003-26
Operational Technology Cybersecurity Maturity Framework

TABLE 3

Understanding Levels and Tiers

Level	What It Means	Which Tiers Apply
Level 0, Baseline (On-Ramp)	No formal program	Tier 1 (planning only)
Level 1, Initiated	Program launched	Tier 1
Level 2, Planned	Governance forming	Tier 1 + select Tier 2
Level 3, Operationalized	Controls active	Tier 1 + Tier 2
Level 4, Managed	Optimized ops	Tier 2 + Tier 3
Level 5, Optimized	Adaptive	Tier 3

3.3 Using the pre-assessment tool

The OT-CMF Pre-Assessment Tool (**Table 4**) provides a simple checklist to help agencies determine if they are at or above Level 1 maturity. This tool is designed for easy use by both cybersecurity leadership and operations personnel.

Instructions for use:

- Answer each of the 9 questions with “Yes” or “No.”
- Each “Yes” equals 1 point.
- A score of 9 means the agency has completed the foundational elements of Level 1.
- A score of 0–8 means the agency is still at Level 0 and must complete basic foundational steps before advancing.

TABLE 4

OT-CMF Pre-Assessment Tool

#	Question (Aligned to Level 1 Requirements Only)	Yes/No
1	Has the agency obtained formal acknowledgment and approval for the adoption of the OT-CMF from divisional or executive leadership?	
2	Has executive leadership allocated or formally committed resources sufficient to support Level 1 OT-CMF implementation activities, including coordination, awareness and assessment?	
3	Has the agency appointed one or more security liaisons across the organization to coordinate cybersecurity program activities within their respective business units, including OT systems?	
4	Has the organization defined, reviewed and approved the business function for each operational technology asset?	
5	Does the cybersecurity program collaborate with relevant business units to document and communicate OT security operating procedures and processes?	
6	Does the agency communicate known cybersecurity threats affecting OT systems to relevant internal stakeholders?	
7	Has the agency implemented a cybersecurity hygiene and awareness program that includes personnel with OT responsibilities?	
8	Has the agency formally committed, through a charter, policy or equivalent mechanism, to reviewing recommended OT-CMF controls and performing an OT cybersecurity self-assessment at least annually?	
9	Does the agency revise and republish approved OT cybersecurity procedures and processes when material changes occur to systems, architecture or operating environments?	

APTA TRANSIT TIP: Post this tool in a shared location so the agency’s engineering, IT and cybersecurity teams can collaborate on the answers.

3.4 Performing a domain-by-domain gap analysis

Transit technicians and managers should break down their maturity assessment into manageable focus areas called “domains.” These domains include key categories like access control, asset management, patch management and incident response.

Below is a step-by-step “how to do it” guide that will help agency implementors to achieve the gap analysis goals:

- **Review the Level 1–specific OT-CMF domain list below:**
 - Governance and leadership
 - Program management and coordination
 - Asset management
 - Policies, procedures and documentation
 - Threat awareness and communication
 - Training and awareness
 - Vulnerability management
 - Assessment and continuous improvement
- **For each domain, write down what the agency currently does.**
 - Example: “For access control, we use passwords but no multifactor authentication.”
- **Compare the agency’s practices with the Tier 1 controls.**
- **Mark gaps where agency practice does not meet the control.**
- **Create a table that includes the following:**
 - Domain
 - Current practice
 - Gaps
 - Needed improvements
 - Responsible person/team

APTA TRANSIT TIP: Assign each domain to a different team member so the analysis can be done in parallel.

3.5 Building the OT asset inventory and architecture map

Before they can protect the agency’s systems, personnel need to know what and where they are. The asset inventory and network architecture diagram are the foundation of OT security.

3.5.1 Steps for transit technicians

1. **Walk through each facility and collect data:**
 - Include substations, signal houses, power systems, maintenance depots, SCADA endpoints, data center, fare equipment, elevators, etc. See Appendix C for a facility risk assessment template.
2. **Capture the following details:**
 - System specifics
 - Asset name/identifier
 - IP address or serial number
 - Operating system or firmware

- Location (room/facility)
 - System and equipment criticality (low/medium/high) (criticality is an important part of the risk management process)
- 3. Draw an architecture map:**
- Show how assets connect to one another
 - Highlight internet-connected devices
 - Identify unmonitored or legacy equipment

3.5.2 CISA guidance for asset inventory

Agencies should align their inventory approach with the CISA “Foundations for OT Cybersecurity: Asset Inventory” guide, which outlines four critical functions of inventory efforts:

1. **Visibility:** Strive for comprehensive visibility into OT-connected devices at every network layer.
2. **Quality:** Establish inventory procedures that produce accurate, trustworthy data.
3. **Utility:** Ensure that the inventory informs multiple OT use cases, including patching, risk analysis and incident response.
4. **Sustainability:** Build processes that can be maintained across the life cycle of systems.

APTA TRANSIT TIP: If the agency lacks automated tools, use a whiteboard or a digital tool like Visio, Draw.io or even PowerPoint to draw the network. Involve someone from operations and maintenance.

3.6 Integrating risk and business impact into the assessment

Once assets and gaps are identified, the next step is deciding what to fix first. Risk and business impact help guide that decision. Perform these steps to prioritize identified gaps:

1. **Identify which systems are most critical to service.**
 - Example: “If this signal controller fails, trains will stop.”
2. **List risks for each asset or system.**
 - Unauthorized access
 - System crash
 - Unpatched vulnerability
3. **Estimate the impact.**
 - Safety impact
 - Operational impact (delays, downtime)
 - Cost (fines, recovery)
4. **Use this to rank gaps as high, medium or low priority.**

APTA TRANSIT TIP: Create a risk heat map. High-risk/high-impact items should be addressed first, regardless of budget cycles.

3.7 Creating a practical action plan

Once all relevant data has been collected, the next step is to translate those findings into a clear, actionable plan that is easy for all stakeholders to understand. A well-structured plan turns assessment results into concrete steps, timelines and responsibilities, ensuring that progress is both measurable and achievable. By following these step-by-step instructions, even small or resource-limited agencies can confidently begin advancing their OT cybersecurity maturity.

APTA SS-TCS-RP-003-26
Operational Technology Cybersecurity Maturity Framework

The OT-CMF is intentionally designed to scale to any size organization, adapt to changing realities and enable incremental improvements. This approach prevents teams from feeling overwhelmed, fosters steady momentum, and ensures that both field personnel and decision-makers remain aligned on priorities and progress.

SMALL AGENCY TIP: If formal risk assessments are not feasible, begin with a basic spreadsheet inventory of assets and their most likely threats. Prioritize risks using a simple high/medium/low scale.

3.8 Maturity roadmap planning

Table 5 sets a recommended target maturity level per domain. In the OT-CMF, each level represents a *stage of cybersecurity maturity*, from ad hoc and reactive to fully optimized and risk-managed.

TABLE 5
Maturity Level Target Chart

Level	Maturity Level	Description
Level 0	Baseline (On-Ramp)	No formal process. OT Cybersecurity is ad hoc or nonexistent.
Level 1	Initiated	Basic awareness. Some governance, roles or activities identified.
Level 2	Planned	Activities are documented. Planning is underway but not consistently applied.
Level 3	Operationalized	Controls are implemented and used consistently.
Level 4	Managed	Processes are monitored and measured. Roles are clearly defined.
Level 5	Optimized	Activities are continuously improved and integrated into strategic planning.

Table 6 illustrates recommended minimum maturity goals by OT-CMF domain. These targets reflect a risk-informed approach that supports federal expectations, resilience best practices and the realities of transit operations. Agencies may tailor these targets further based on asset criticality, resource availability and cybersecurity risk appetite. These targets are guidance, not mandates, and provide examples of scaled implementation for smaller agencies. Agencies with limited OT exposure or staff may adapt to these targets flexibly, using the OT-CMF to inform just-in-time maturity development aligned with asset criticality. Remember, this simply serves as a planning tool to help agencies prioritize maturity advancement over time. Agencies should adapt these targets to fit their specific operational context.

TABLE 6
Maturity Goals by OT-CMF Domain

OT-CMF Domain	Recommended Minimum Target Level	Description of Expectation at Target Level
1. Governance and risk management	Level 4 (Managed)	Agency has formal policies, documented risk frameworks and recurring risk reviews.
2. Asset management	Level 3 (Operationalized)	Inventories are maintained, validated and integrated with planning and response.
3. Identity and access management	Level 2 (Planned)	Access policies are documented; role-based controls are implemented and reviewed.
4. Data security	Level 2 (Planned)	OT-relevant data handling procedures (e.g., logs, configs) are enforced and backed up.
5. Security continuous monitoring	Level 3 (Operationalized)	Continuous OT monitoring in place with alert triage and incident response integration.

TABLE 6
Maturity Goals by OT-CMF Domain

OT-CMF Domain	Recommended Minimum Target Level	Description of Expectation at Target Level
6. Configuration management	Level 2 (Planned)	Baselines for OT systems are defined and change control is maturing.
7. Maintenance	Level 2 (Planned)	Preventive and corrective maintenance activities are logged and tracked.
8. Protective technology	Level 3 (Operationalized)	Firewalls, segmentation and basic threat detection are deployed and tuned.
9. Detection processes	Level 3 (Operationalized)	OT-specific anomaly detection and log review processes are in place (see also Appendix D).
10. Response and recovery	Level 4 (Managed)	OT incident response and recovery plans are exercised and resourced.

4. Implementing basic tenets of the OT-CMF (Tier 1)

Tier 1 controls represent the essential security functions every transit agency should implement as a baseline. These foundational measures are selected based on their high impact, low complexity and broad applicability across different OT environments. Implementing Tier 1 controls brings agencies into alignment with the Initiated and Planned levels of the OT-CMF maturity model. This is where agencies begin formalizing responsibilities, establishing repeatable procedures, and implementing basic controls that reduce cybersecurity risk and improve system visibility.

Tier 1 controls focus on practical steps in five key areas: visibility, access, hygiene, monitoring and configuration. These are designed to be achievable regardless of agency size or budget and serve as prerequisites for more advanced cybersecurity maturity.

APTA TRANSIT TIP: Tier 1 controls help prevent the most common cybersecurity incidents. These incidents include unauthorized access, poor patching and unmonitored device changes.

4.1 Getting started: Prioritization and planning

Agencies must approach OT-CMF implementation with a structured plan that prioritizes high-value actions and aligns with available resources. This section outlines how to set priorities, define a roadmap, and assign responsibilities so that implementation efforts are both practical and sustainable.

Before implementation, agencies should do the following:

- 1. Identify which Tier 1 controls they already partially or fully meet.**
 - Review existing systems, procedures, and tools to determine where current practices align with Tier 1 control expectations. For example, if a team is already logging OT events but not reviewing them regularly, that control would be marked “partially met.”
- 2. Prioritize remaining controls based on risk, criticality and ease of implementation.**
 - Not all controls need to be implemented at once. Begin with those that protect the most critical systems or are easiest to deploy. Controls that address internet-exposed devices, weak credentials or outdated firmware should be high priority.

- 3. Assign responsible teams or owners for each control.**
 - Designate someone from the OT, IT, engineering or maintenance teams to be accountable for implementing each control. Clear ownership ensures follow-through and avoids duplication.
- 4. Include Tier 1 implementation in capital and operational work plans.**
 - Controls should be aligned with existing project timelines and budgets. Integrating control implementation into maintenance windows, modernization projects or grant proposals helps secure necessary funding and buy-in.

Table 7 contains an example of a planning tool for implementing Tier 1.

TABLE 7
Tier 1 Implementation Planning Example

Control ID	Control Name	Current Status	Owner	Priority	Target Completion
CM-8	Asset Inventory	Partial	OT Engineer	High	Q3 FY2026
AC-2	Account Management	Not started	IT Security	Medium	Q4 FY2026

4.2 Descriptions of key Tier 1 controls

Agencies beginning their OT-CMF journey at Tier 1 should focus on a set of essential, foundational controls. These controls provide immediate risk reduction, are relatively low-cost to implement, and establish the groundwork for advancing to higher tiers. The descriptions in this section explain the purpose of each Tier 1 control, outline basic implementation steps, and highlight how they scale with agency size and complexity.

Here are examples of foundational Tier 1 controls and how a transit agency can implement them:

- **CM-8: Asset Inventory**
 - Maintain a complete, accurate list of OT devices. This is the foundation of all security decisions. Agencies must understand what assets exist before they can protect them.
 - Include key metadata like physical location, OS version, firmware version, assigned owner and operational role.
 - Update the inventory anytime devices are installed, removed or upgraded. Use spreadsheets or asset management systems as appropriate.
- **AC-2: Account Management**
 - Ensure that all users accessing OT systems are authorized. Create a list of users and their roles.
 - Remove unused accounts and restrict shared log-ins. Set account expiration policies for temporary users.
 - Conduct quarterly reviews of account lists to detect drift or unauthorized access.
- **IR-1: Incident Response Policy and Procedures**
 - Develop a written incident response procedure specific to OT systems (e.g., SCADA or signals).
 - Identify clear roles, contacts and escalation paths in the event of an incident.
 - Perform tabletop exercises to ensure that staff are familiar with the process before a real event occurs.
- **SI-3: Malicious Code Protection**
 - Install antivirus or anti-malware tools on all client and possibly server-side computers.
 - Assess configuration management controls consisting of Change Control Board for approval of new/updated software/firmware prior to installation and rollout. This is a key activity when malicious software and misconfigurations can be introduced to the system.

APTA SS-TCS-RP-003-26
Operational Technology Cybersecurity Maturity Framework

- Use file integrity monitoring on nontraditional systems (e.g., controllers).
- Train staff to spot signs of tampering or compromise, including unusual behavior, unauthorized log-ins or unplanned reboots.
- **AU-12: Audit Generation**
 - Configure OT systems to generate logs for log-in attempts, configuration changes and alarms.
 - Agencies should store logs in a centralized system or network share with at least 30-day retention.
 - Assign a technician or team to review these logs weekly or after any suspicious event.

SMALL AGENCY TIP: Focus first on controls that reduce the highest risks at the lowest cost, such as strong password policies, secure remote access and basic patching routines.

4.3 Real-world implementation tips

Experience shows that successful OT-CMF implementation depends on simple, repeatable practices that fit into day-to-day operations. This section provides hands-on advice that agencies of any size can apply immediately. The goal is to help agencies avoid common pitfalls, leverage existing resources and build confidence by demonstrating early wins.

- **Start small. Begin with one system (e.g., signal or SCADA).**
 - Piloting controls in a single system helps build knowledge, demonstrate value and refine procedures before expanding.
- **Use manual tools like spreadsheets if automation isn't available.**
 - Agencies don't need expensive tools to get started. Excel or Google Sheets can track inventories, account reviews and logs. Appendix E contains a sample progress tracker.
- **Involve maintenance and field techs. They know where devices are.**
 - Field personnel have firsthand knowledge of equipment locations and configurations. Involve them early in asset inventory and control discussions.
- **Review what IT is already doing, because some controls may overlap.**
 - Leverage existing practices from enterprise IT, such as patch management tools, identity and access systems, or backup policies.
- **Set monthly review meetings to track progress.**
 - Progress should be reviewed regularly across stakeholders to remove roadblocks and maintain momentum. Use dashboards or charts for visibility.

APTA TRANSIT TIP: Track control implementation progress on a shared dashboard visible to operations, engineering and cybersecurity teams.

4.4 Network segmentation and zoning

Effective implementation of OT cybersecurity requires robust network segmentation to limit the spread of threats and enforce security boundaries. Segmentation ensures that critical control systems are isolated from less-trusted networks, while still allowing necessary communications through controlled and monitored pathways.

4.4.1 Purpose of segmentation

- **Restrict lateral movement:** Prevent attackers who gain access to one part of the network from moving freely into critical OT systems.

- **Contain failures and malware:** Limit the blast radius of misconfigurations, malware or ransomware outbreaks by enforcing boundaries.
- **Enhance monitoring and control:** Provide well-defined perimeters where security monitoring, intrusion detection and access control policies can be consistently applied.
- **Support compliance and governance:** Demonstrate structured risk reduction practices aligned with frameworks like NIST CSF, guidelines like NIST SP 800-53 Rev 5, and standards like IEC 62443.

4.4.2 Segmentation models

Segmentation can be designed using structured models that help define clear security layers and communication boundaries. These models provide a framework for aligning OT network design with best practices, ensuring consistency and scalability. Common approaches include the following:

- **Purdue model for ICS security:** Apply Purdue architecture zoning—enterprise to field devices.
- **Zones and conduits:** Group assets by function and sensitivity and manage communication through secured conduits (e.g., firewalls, gateways).
- **APTA zones:** See APTA SS-CCS-RP-002-13, “Securing Control and Communications Systems in Rail Transit Environments, Part II: Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones.”

4.4.3 Segmentation techniques

Segmentation can be achieved through a variety of technical methods, each offering different levels of protection and complexity. Agencies should choose techniques that match their maturity level, risk profile and available resources. Key approaches include the following:

- **Firewalls and VLANs:** Segment networks at a basic level by using firewalls to enforce traffic rules and VLANs to separate traffic flows. For example, create distinct VLANs for IT systems, OT controllers and guest access, with firewall rules limiting cross-VLAN communication.
- **Secure conduits:** Establish controlled communication paths between zones, protected by encryption, authentication and monitoring. Examples include VPN tunnels for remote access, or firewalled conduits between a control network and an operations center.
- **Data diodes/unidirectional gateways:** Deploy one-way communication devices in highly critical environments to ensure that data can flow out (e.g., to a monitoring center) but not back in. This prevents command traffic from reaching sensitive control systems.
- **Micro-segmentation:** Use software-defined networking (SDN) or host-based firewalls to enforce identity-based policies at a granular level, such as restricting a single engineering workstation to communicate only with its associated PLCs. This allows fine-grained access control and rapid isolation during incidents.

4.4.4 Implementation guidance by agency size

The way segmentation is implemented will depend heavily on the size, resources and maturity of the agency. Smaller agencies can achieve meaningful security gains with simple, low-cost measures, while mature agencies with larger infrastructures should invest in layered defenses and advanced monitoring. The following guidance provides practical approaches for both contexts. See also Appendix F for more on small agencies and Appendix G for more on mature agencies.

Small agencies:

- Start with VLAN-based separation between business IT and OT networks.
- Deploy a firewall at the IT/OT boundary.
- Limit remote access strictly and monitor with simple logging tools.

Mature agencies:

- Implement full Purdue zoning, including DMZ layers for data exchange.
- Apply deep packet inspection firewalls at critical conduits.
- Integrate micro-segmentation and real-time monitoring for anomaly detection.
- Use data diodes for one-way data flows from OT to enterprise systems.

4.4.5 Segmentation governance and maintenance

Strong governance is essential to ensure that segmentation strategies remain effective over time. Governance defines ownership, accountability and repeatable processes for sustaining secure zones and conduits across the OT environment. This includes policy enforcement, ongoing validation and leadership oversight to adapt controls as the operational landscape evolves.

- **Document and validate segmentation policies.** Maintain written policies that define zone boundaries and communication paths, and test them annually to ensure that they reflect current architecture and threats.
- **Review firewall and VLAN settings quarterly.** Conduct scheduled reviews of rulesets and VLANs to detect drift, outdated rules or misconfigurations that weaken segmentation.
- **Embed segmentation into change and incident processes.** Ensure that any system changes or incident responses include checks to verify that segmentation controls are preserved or updated.
- **Test segmentation with red teams or pen tests.** Use external assessments to identify weaknesses and confirm that segmentation controls are working as intended.

4.5 Success indicators

These are some indications that an agency has successfully implemented Tier 1:

- **The inventory includes all major OT systems and devices.**
 - All assets are documented with details such as owner, location and configuration information. There are no unidentified, untracked or unmanaged devices connected to the operational environment.
- **Each OT user has a documented account with defined access roles.**
 - Role-based access controls are in place, aligned to job responsibilities and reviewed on a regular schedule. Generic, shared or default credentials have been eliminated to ensure accountability and traceability.
- **There is a designated primary cybersecurity coordinator or incident response lead, and tested procedures are in place.**
 - Staff across the organization know exactly whom to contact and what steps to take in the event of suspicious activity, a cybersecurity incident or a system failure. Incident response procedures are documented, tested and updated based on lessons learned.
- **At least one log source is actively monitored and reviewed.**
 - Security logs and alerts are consistently collected, analyzed and used to guide follow-up investigations. Issues identified through log reviews are tracked to resolution, improving both response speed and accuracy.
- **Cybersecurity training reaches OT staff, not just IT employees.**
 - Field technicians, control system operators and other OT personnel receive security awareness training tailored to their work environment and daily responsibilities. Training is reinforced regularly to maintain awareness and readiness.

These practices lay the foundation for moving toward Tier 2 and Tier 3 controls. Without Tier 1, higher maturity levels are not possible.

APTA TRANSIT TIP: Celebrate Tier 1 completion with a formal milestone presentation to leadership to reinforce momentum.

4.5.1 Alignment with industry guidance

The practices in this tier align with multiple industry-recognized frameworks and guidance documents, including the following:

- **CISA OT Cybersecurity: Asset Inventory Guidance (2024)**
 - Encourages organizations to begin with foundational visibility, accuracy and sustainability of asset records.
- **NIST SP 800-82 Rev. 3: Guide to Industrial Control Systems Security**
 - Recommends establishing asset inventory and defining initial cybersecurity roles and responsibilities as critical early steps in ICS environments.
- **TSA Security Directive 1582/1580-21-01 Series**
 - Requires passenger and freight rail agencies to designate a cybersecurity coordinator and maintain basic awareness of OT asset configurations.
- **IEC 62443-2-1: Security Program Requirements for IACS Asset Owners**
 - Calls for defining roles, responsibilities and inventory mechanisms as part of baseline security practices.

APTA CROSSWALK NOTE: These Tier 1 activities form the foundational bedrock that enables alignment with the APTA OT-CMF and prepares agencies for future regulatory and operational requirements.

5. Transitioning from Tier 1 to Tier 2 controls

5.1 Implementing Level 2 (Tier 1 controls)

At maturity Level 2 (Planned), transit agencies are expected to move from initial, reactive practices to proactive and standardized governance. This includes implementing policy frameworks, documenting procedures and aligning cybersecurity responsibilities with organizational roles.

The focus in Level 2 is on formalizing what may have previously been ad hoc processes, building governance infrastructure, and enabling consistent oversight of OT security functions. Agencies at this level begin establishing performance metrics and integrating cybersecurity maturity into broader risk and business operations. Level 2 is where an agency's cybersecurity efforts become sustainable, repeatable and embedded in operations.

APTA TRANSIT TIP: If resources are limited, focus on documenting current practices, assigning responsibility and using checklists to introduce consistency. This section is about building forward momentum.

5.1.1 Core governance components to operationalize

To support Level 2 implementation, the following governance components should be introduced and integrated into the agency's cybersecurity program:

- **Governance structure:** Create or formalize an OT cybersecurity governance team or steering committee that includes stakeholders from IT, operations, engineering and leadership. This group sets priorities, approves policies and tracks maturity progress.

APTA SS-TCS-RP-003-26
Operational Technology Cybersecurity Maturity Framework

- **OT cybersecurity policy:** Develop a written OT cybersecurity policy aligned with existing IT security policies. This policy should cover asset management, access controls, change management and system recovery, specifically tailored for OT environments.
- **Roles and responsibilities matrix:** Define who is responsible, accountable, consulted and informed (RACI) for key OT cybersecurity functions. Ensure that all controls and response actions have assigned owners across departments.
- **Performance metrics and KPIs:** Establish performance indicators for OT cybersecurity such as number of completed asset updates, frequency of account reviews and incident response readiness. Use dashboards or monthly reports to drive accountability.
- **Integration with risk management:** Integrate OT cybersecurity considerations into the agency's enterprise risk management (ERM) framework. Cybersecurity risks should be included in risk registers and reviewed regularly by executive leadership.
- **Policy compliance monitoring:** Develop a process to monitor compliance with cybersecurity policies. This may include audits, control checklists or review cycles.

APTA TRANSIT TIP: Begin by aligning OT policy with already-approved IT security documents. This accelerates adoption.

5.1.2 Organizational engagement strategy

Achieving Level 2 maturity requires more than just technical improvements. It demands active participation from the entire organization. Cybersecurity must be positioned as a shared responsibility that supports the agency's mission, operational reliability and public trust. This means engaging leadership, integrating cybersecurity into departmental operations, and building a culture where awareness and preparedness are part of everyday work. By fostering communication, collaboration and consistent policy reinforcement, agencies can ensure that cybersecurity practices are understood, supported and sustained at all levels of the organization.

To succeed at Level 2, agencies must bring the majority of the organization along. This includes the following:

- **Executive engagement:** Regularly brief leadership on cybersecurity risks, maturity progress and budget needs. Emphasize how cybersecurity supports safety, continuity and public trust.
- **Departmental integration:** Align cybersecurity roles with engineering, maintenance, procurement and planning functions. Establish cybersecurity liaisons in each department.
- **Cross-training and awareness:** Host awareness sessions on OT threats, conduct tabletop exercises and rotate team members through joint OT/IT assignments.
- **Policy communication campaign:** Use emails, posters and internal briefings to explain new policies and reinforce expectations.

APTA TRANSIT TIP: Frame cybersecurity as a safety and reliability function to increase buy-in from operations staff.

5.1.3 Readiness to advance

Reaching the point where an agency is ready to advance beyond Level 2 signals that cybersecurity practices have moved from being newly established to consistently embedded in daily operations. At this stage, policies are not just written but are actively followed and enforced, performance metrics are tracked and inform decision-making, and OT cybersecurity is part of regular risk discussions. Governance structures are functioning across departments, and staff at all levels understand their specific role in protecting operational

technology. This organizational alignment forms the foundation for the Operationalized maturity level and sets the stage for the data-driven, automated capabilities of the Managed level.

Agencies with the following characteristics are ready to move beyond Level 2:

- Policies are routinely followed and enforced.
- KPIs are tracked and used to guide decisions.
- Risk discussions include OT cybersecurity.
- Governance is active and coordinated across departments.
- Staff can describe their role in the cybersecurity program.

These governance structures form the backbone of the Operationalized maturity level and prepare agencies for the data-driven and automated controls of the Managed level.

5.2 Implementing Level 3 (Tier 2 controls)

At Level 3 (Operationalized), the emphasis shifts from implementing controls to managing them through documented procedures, performance metrics and formal governance. The goal is to ensure that controls are consistent, effective and continually verified across OT environments.

At Level 3, transit agencies begin executing cybersecurity practices consistently across their OT environments. Policies and procedures established in earlier stages are now implemented through routine operational workflows. Cybersecurity responsibilities are integrated into engineering, maintenance and system management activities, ensuring that core security controls are applied consistently across OT systems.

Desired outcomes:

- Repeatable, documented workflows for core OT security activities
- Governance structures that review risk and performance data
- Evidence-based assurance via monitoring, testing and audits

5.2.1 Control objectives at Level 3

Level 3 marks a shift from foundational implementation to disciplined, measurable cybersecurity management. It uses Tier 2 controls. Agencies at this stage move beyond simply meeting baseline requirements and instead apply structured, risk-based approaches to guide decisions and allocate resources. Continuous monitoring and validation ensure that both technical and procedural controls remain effective, while OT asset management is integrated across the entire life cycle. This extends from commissioning to retirement. Vendor relationships are strengthened through enforceable cybersecurity requirements, and incident data is analyzed for trends that drive meaningful program improvements. This maturity level emphasizes formalized processes that are repeatable, accountable and aligned with long-term operational goals.

Level 3 introduces disciplined practices for the following:

- Risk-based prioritization of cybersecurity resources
- Continuous control monitoring and validation (technical and procedural)
- Life cycle-based OT asset management (commissioning → operations → retirement)
- Vendor cybersecurity compliance enforcement across the supply chain
- Incident trend analysis and response enhancement to drive improvements

Agencies at this stage go beyond checklists to adopt formal, measurable processes.

SMALL AGENCY TIP: Don't aim to fully meet Level 3 maturity all at once. Pick a few high-impact controls to implement first, such as access reviews or software patching, and grow from there.

5.2.2 Key practices to operationalize

Operationalizing Level 3 maturity requires embedding cybersecurity practices into the daily management of OT systems, so they become routine, measurable and enforceable. This stage is about ensuring that processes are not just documented but actively followed and continuously improved. Agencies focus on structured change management, full life cycle asset planning and holding vendors accountable for security across the supply chain. Risk is tracked in a dedicated OT register, providing clear visibility into priorities and driving informed investment decisions. Regular internal audits validate that policies and security controls are effective. This ensures that cybersecurity remains an integral part of operational excellence rather than a one-time initiative.

The following components support Level 3 implementation:

- **Change management controls:** All system modifications follow a formal change request workflow including risk/impact assessment, cybersecurity review, rollback planning, approvals and post implementation validation.
- **Asset life cycle plans:** Every critical system has a life cycle plan covering inventory, configuration baselines, vulnerability/patch cadence, obsolescence dates, support status and secure decommissioning.
- **Vendor evaluation and enforcement:** Agencies should require third parties to demonstrate compliance via audits or attestations and contracts include security clauses, right to audit, software bill of materials (SBOM) and software of unknown provenance (SOUP) expectations, incident notification, and patch SLAs.
- **OT risk register:** Maintain an OT-specific register aligned to enterprise risk, with owners, inherent/residual ratings, control mapping and tracked actions used to prioritize investments.
- **Periodic internal audits:** Agencies should conduct self-assessments against OT-CMF policies and practices, generate corrective actions, assign owners and due dates, and verify closure.

5.2.3 Common pitfalls and how to avoid them

Even with disciplined processes in place, Level 3 efforts can stall if common mistakes go unaddressed. The most frequent issues involve treating requirements as paperwork exercises, working with incomplete or outdated asset data, and relying on vendor assurances without verification. Addressing these pitfalls early ensures that Level 3 practices remain actionable, accurate and impactful.

Avoid these potential pitfalls:

- **Treating Level 3 as paperwork:** Tie every artifact to a decision (e.g., risk register → budget, CCR → risk acceptance).
- **Incomplete asset data:** Automate discovery and require ownership before go-live.
- **Vendor blind spots:** Enforce evidence, not promises; embed audit rights.
- **KPI vanity metrics:** Favor outcome measures (risk reduced, mean time to respond [MTTR] improved) over activity counts.
- **Audit findings without closure:** Create CAP trackers with due dates, owners and effectiveness checks.

5.2.4 Level 4 readiness indicators

To reach Level 4 (Managed) maturity, an agency must have achieved all items in Level 3. Level 4 reflects a mature and optimized OT cybersecurity posture where processes are proactive, repeatable and measured. At this level, organizations have formalized governance structures, have integrated cybersecurity into operations, and use data-driven approaches to continuously improve. While not the final stage of maturity, Level 4 indicates a high degree of operational discipline and risk-aware decision-making. *Most organizations will never fully reach this level. However, it should be an agency goal and in the roadmap.*

Organizations are prepared to move to Level 4 when the following are true:

- **Cybersecurity data informs operational decisions:** Threat intel, vulnerability data and incident trends are integrated into daily planning and real-time operations; risk is translated for operational leaders.
- **Internal audits drive corrective actions:** Findings are documented, prioritized and remediated via structured CAPs with verification and effectiveness checks.
- **Risk and control performance are reported to leadership:** Quantified risk and KPIs are routinely reported; governance bodies act on trends and resourcing needs.
- **Change control, patching and asset retirement are standardized:** Organization-wide procedures are enforced; exceptions are rare, documented and time-bound.
- **Third-party vendors meet or exceed requirements:** Vendors are vetted pre-award, bound by security clauses and monitored for ongoing compliance.

SMALL AGENCY TIP: If Level 4 and Level 5 feel out of reach, use them as a long-term target. Build a roadmap to gradually implement the most realistic elements of those tiers over time.

5.3 Preparing to govern and measure performance

While Level 3 (Operationalized) focuses on consistent execution of cybersecurity practices, agencies must also develop mechanisms to measure performance and validate control effectiveness. Implementing controls alone does not guarantee that they remain effective as systems evolve, technologies change and threat actors adapt.

The next stage of maturity requires agencies to introduce governance structures, measurement tools and operational management processes that allow leadership to evaluate cybersecurity performance, identify gaps and prioritize improvements. These capabilities enable agencies to transition from simply executing cybersecurity activities to actively managing cybersecurity risk across the OT environment.

While the Operationalized level focuses on consistent execution of cybersecurity practices, agencies must also develop mechanisms to measure performance and validate control effectiveness. The tools and practices described in Chapter 6 support agencies in strengthening governance, improving oversight, and advancing toward Managed maturity (Level 4).

6. Tools and practices beyond Level 3 maturity

Section 5 describes how agencies “operationalize” cybersecurity practices. This section provides practical tools and reference materials that agencies can use to implement, measure and sustain those practices as they advance toward Level 4 (Managed) maturity.

Agencies that have reached the Operationalized maturity level have implemented cybersecurity practices across their OT environments. The tools and practices described in this section support agencies in advancing

beyond this level by introducing mechanisms to measure performance, validate controls and strengthen governance. These capabilities enable agencies to transition toward the Managed maturity level of the OT-CMF.

However, implementing controls consistently is only one step in building a resilient cybersecurity program and maturing OT cybersecurity. Transit agencies must also develop the ability to measure performance, validate effectiveness and adapt controls as systems and threats evolve. Without these capabilities, cybersecurity practices may stagnate or fail to keep pace with operational changes.

This section introduces tools, governance practices, and operational mechanisms that help agencies advance beyond Level 3 (Operationalized) toward a Level 4 (Managed) cybersecurity program. These practices focus on improving visibility, accountability and oversight across OT environments.

Key practices introduced in this section include the following:

- Establishing cybersecurity performance metrics.
- Validating security controls through audits and testing.
- Strengthening governance and cross-department coordination.
- Integrating cybersecurity checks into engineering and maintenance workflows.
- Implementing tools that support asset visibility, monitoring and configuration management.

These capabilities allow agencies to transition from executing cybersecurity practices to actively managing them, which is the defining characteristic of the Managed maturity level.

Transit agencies should view these tools and practices as enablers of continuous improvement, helping security teams detect gaps, validate controls and prioritize investments that strengthen operational resilience.

6.1 Cybersecurity performance metrics

Transit agencies advancing beyond the Operationalized level should begin establishing cybersecurity performance metrics that measure the effectiveness of implemented controls. Metrics help agencies determine whether security practices are functioning as intended and provide insight into areas that require improvement. Examples may include tracking the percentage of OT assets inventoried, the number of unauthorized access attempts detected or the time required to respond to cybersecurity incidents. These metrics provide leadership and technical teams with objective information to guide future cybersecurity investments and operational decisions.

6.2 Continuous monitoring tools

Continuous monitoring tools improve the visibility of OT networks and systems by detecting abnormal behavior and potential security events. Agencies should begin evaluating and deploying monitoring technologies capable of identifying unusual network activity, unauthorized communications or system configuration changes. While smaller agencies may rely on basic logging or network monitoring, larger systems may implement specialized OT monitoring platforms designed to analyze industrial protocols and detect anomalies across the control environment.

6.3 Segmentation, governance and validation

Strong governance is necessary to ensure that network segmentation strategies remain effective as systems evolve. Agencies should begin establishing processes to regularly validate security zones and conduits and confirm that segmentation controls are operating as intended. This includes documenting segmentation policies, reviewing firewall and VLAN configurations, and incorporating segmentation checks into change

management and incident response procedures. Periodic testing, including penetration testing or controlled assessments, can help confirm that segmentation boundaries effectively limit unauthorized movement within the OT environment.

6.4 Configuration and change validation

Configuration management practices should evolve to ensure that system changes are tracked and validated. Agencies should maintain baseline configurations for critical OT systems and verify that changes are reviewed and documented through a formal change management process. These practices help prevent configuration drift and reduce the risk of unintended security weaknesses introduced during maintenance, upgrades or vendor activities.

6.5 Incident response exercises

Agencies should begin conducting incident response exercises to validate the effectiveness of cybersecurity procedures and coordination across operational teams. Tabletop exercises allow technical staff, operations personnel and leadership to practice responding to simulated cybersecurity incidents. These exercises help identify gaps in communication, clarify roles and responsibilities, and improve overall readiness to respond to real-world cyber events affecting transit operations.

6.6 Vendor cybersecurity oversight

Transit agencies rely heavily on vendors for system installation, maintenance and operational support. As cybersecurity programs mature, agencies should strengthen oversight of vendor access and security practices. This may include requiring vendors to follow established cybersecurity policies, document remote access procedures, and incorporate cybersecurity expectations into procurement and contract requirements. Agencies should thoroughly evaluate vendor access control processes to ensure that all vendor access methods, authorized or otherwise, are identified, documented and appropriately controlled.

6.7 Integration of enterprise risk management

Cybersecurity risks affecting operational technology should be incorporated into the agency's broader enterprise risk management processes. Agencies should begin reporting cybersecurity risks, incidents and mitigation activities to leadership and governance bodies responsible for organizational risk oversight. This integration helps ensure that cybersecurity considerations are reflected in strategic planning, investment decisions and operational priorities.

6.8 Governance

Strong governance ensures that OT cybersecurity practices remain consistent, accountable and aligned with organizational priorities. As agencies mature beyond the Operationalized level, governance mechanisms help formalize decision-making, clarify ownership of cybersecurity activities, and establish repeatable processes for oversight and reporting. Governance tools provide structure for coordinating cybersecurity efforts across operations, engineering, safety and executive leadership.

The governance tools described in this section provide practical templates and processes that agencies can use to strengthen oversight of their OT cybersecurity programs. These tools support consistent policy implementation, improve communication across stakeholders, and ensure that cybersecurity risks are regularly reviewed as part of the agency's broader operational and risk management activities.

Sections 6.8.1 through 6.8.4 introduce specific governance artifacts that help agencies define responsibilities, track program maturity and maintain a predictable operating rhythm for cybersecurity management. Together,

these tools help agencies move from executing cybersecurity activities to actively managing and governing their OT cybersecurity programs.

6.8.1 Sample governance policy template outline

- **Purpose and scope:**
 - Clearly state the objectives of the policy and its role in protecting the agency's OT assets.
 - Define which OT systems, networks, devices and users are covered.
 - Include boundaries of applicability (e.g., in-house systems, vendor-managed systems, remote access scenarios).
- **Roles and responsibilities:**
 - Identify key stakeholders, such as OT system owners, operators, cybersecurity leads, IT security support and executive sponsors.
 - Define each role's specific responsibilities for safeguarding OT systems, maintaining documentation and responding to incidents.
 - Establish decision-making authority for security exceptions, risk acceptance and policy updates.
- **Security requirements:**
 - Define minimum security standards for access control, authentication and account management (e.g., role-based access, password complexity).
 - Specify change management procedures for OT systems, including approval workflows, testing and rollback plans.
 - Outline requirements for monitoring network activity, system logs and security events, including alert thresholds and escalation triggers.
- **Training requirements:**
 - Establish mandatory, role-specific cybersecurity training for OT staff, contractors and relevant IT personnel.
 - Include frequency of training (e.g., annual refreshers, new-hire onboarding, post-incident retraining).
 - Address specialized training needs for incident responders, system administrators and field techs.
- **Incident reporting procedures:**
 - Define the process for identifying, escalating and documenting cybersecurity incidents.
 - Specify time frames for reporting different types of incidents based on severity.
 - Include communication protocols for notifying leadership, regulatory bodies and stakeholders.
- **Compliance requirements:**
 - Mandate regular audits, vulnerability assessments and penetration tests to evaluate the cybersecurity posture.
 - Require documentation and tracking of findings, with corrective action plans and deadlines.
 - Establish a review cycle for the governance policy to ensure alignment with evolving threats, industry standards and regulatory changes.

6.8.2 OT governance maturity checklist

To evaluate and improve OT cybersecurity governance, organizations can use a structured maturity checklist. This tool helps assess current practices, identify gaps and prioritize areas for development across key governance domains. The sample checklist shown in [Table 8](#) offers a practical framework for measuring progress against industry best practices and aligning OT cybersecurity efforts with organizational risk management goals.

TABLE 8
Sample OT Governance Maturity Checklist

Governance Element	In Place	Owner	Review Date
OT Cybersecurity Policy	✓	CISO	10/01/2025
Governance Committee Charter		COO	
Role and Responsibility Matrix	✓	Cyber Lead	09/15/2025
Cyber KPIs Defined		OT Manager	
Risk Register Updated	✓	Risk Officer	10/23/2025

APTA TRANSIT TIP: Use this checklist to track governance adoption milestones and report quarterly to executives.

6.8.3 Governance and operating rhythm

Consistent governance and operating rhythm keep OT cybersecurity efforts focused, measurable and aligned with organizational priorities. By following a predictable schedule of monthly, quarterly, semiannual and annual activities, agencies ensure that leadership regularly reviews OT risks, evaluates control performance and tracks vendor compliance. This structured cadence supports proactive decision-making, reinforces accountability and ensures that cybersecurity remains an ongoing operational priority rather than an ad hoc activity.

- **Monthly:** OT risk review, control KPI dashboard to OT leadership.
- **Quarterly:** Internal audit sampling, trend analysis, vendor performance review.
- **Semiannually:** Playbook/tabletop exercises, policy refresh, life cycle roadmap update.
- **Annually:** Program review to executive committee, budget alignment to top OT risks.

6.8.4 RACI snapshot

Using a RACI chart is very effective for managing risk ownership. A clear RACI framework that defines who is responsible, accountable, consulted and informed ensures that every aspect of the OT cybersecurity program is owned and executed effectively. By formally assigning these roles across operations, safety, engineering, procurement, legal and executive leadership, agencies can streamline communication, eliminate gaps in responsibility and foster collaboration. This clarity of ownership helps maintain momentum and ensures that cybersecurity decisions are informed by the right expertise at the right time.

- **Responsible:** OT cybersecurity operations, system owners
- **Accountable:** CISO/OT security manager
- **Consulted:** Operations, safety, engineering, procurement, legal
- **Informed:** Executive leadership, board/oversight bodies

Figure 1 shows a sample RACI chart for a cybersecurity program.

APTA SS-TCS-RP-003-26
Operational Technology Cybersecurity Maturity Framework

FIGURE 1
Sample Cybersecurity RACI Chart

RACI Chart Cybersecurity in Safety and Security Certification			
Position →	Safety Certification Professional	Security Certification Professional	Cybersecurity Coordinator
Tasks ↓			
Certifiable Elements List	R	I	I
Preliminary Hazard Analysis (PHA)	R	I	C
Threat and Vulnerability Assessment (TVA)	A	R	C
Criteria Conformance Checklist	R	C	I

- R Responsible – The individual(s) who must complete the task or deliverable (direct contributors).
- A Accountable – Ensure accountability to project deadlines and completion (key stakeholders)
- C Consulted – Key opinions that weigh heavily on successful project completion (legal, cybersecurity, compliance, finance, etc.).
- I Informed – Represent individuals that should be kept in the loop on project progress, changes, etc. but do not have a specific decision-making authority or specialty required for the project to be successfully completed

Agencies should use these processes to ensure consistency and enable clear reporting to leadership. The governance tools presented in this section help agencies strengthen oversight, measure cybersecurity performance and establish the management processes required to sustain a mature OT cybersecurity program.

6.9 Change control request

A “change control request” (CCR), sometimes called a “change configuration request,” is the starting point in the workflows below for ensuring that any critical system modification goes through proper review and authorization before being put into production. It’s a formal document or system entry used to propose, review and approve changes to OT systems, configurations or processes. A CCR typically includes the following:

- A description of the change
- The reason for the change
- Risk and impact assessment (including cybersecurity review)
- Testing and rollback plans
- Required approvals before implementation

The CCR form is a standardized document used to formally propose, assess, approve and track modifications to operational systems, assets or processes. It ensures that all changes, whether standard, normal or emergency, are evaluated for their potential impact on safety, reliability and cybersecurity before implementation. The form captures essential information such as the change rationale, affected controls, risk assessment and required approvals, while also documenting contingency measures, testing requirements and post-change validation. By using a consistent CCR process, organizations can maintain operational integrity; regulatory compliance; and coordinated communication across operations, safety, cybersecurity and vendor stakeholders.

A sample CCR Form and required data fields are provided in Appendix H.

6.10 Change Advisory Board

A Change Advisory Board (CAB) is a cross-functional group that often includes OT system owners, cybersecurity leaders, operations managers and sometimes vendor representatives that review and approve proposed changes before implementation. The CAB's role is to do the following:

- Evaluate the technical, operational and cybersecurity impacts of a proposed change.
- Ensure that risks are identified and mitigated.
- Confirm that necessary testing, rollback and documentation are in place.
- Approve or reject the change request based on risk and business priorities.

In the **CCR → Security Review → CAB Approval → Implement → Validate → Close** workflow, the CAB step ensures that no critical change moves forward without multi-stakeholder oversight.

APTA TRANSIT TIP: Tier 3 is where cybersecurity becomes how operations are managed and not just protected.

6.11 Example workflows (summarized)

Workflows translate policy into repeatable, real-world actions that teams can follow consistently. The examples below illustrate how Tier 3 agencies handle common OT cybersecurity activities such as change management, vulnerability remediation and incident trend analysis using structured steps that ensure that security, safety and operational continuity remain balanced. Each workflow is designed to provide clear checkpoints, accountability and feedback loops so that lessons learned directly improve future performance. Appendix I contains more information on how Tier 3 is used in practice.

1. **CCR → Security Review → CAB Approval → Implement → Validate → Close**
 - Security sign-off required for all critical changes; emergency path with retrospective review.
2. **Vulnerability → Risk Triage → Patch/Safe Mode Compensating Controls → Validate**
 - Safety and uptime constraints incorporated into risk decisions with documented exceptions.
3. **Incident Trend Review → Root Cause → Control Enhancement → KPI Update**
 - Trends feed back into playbooks training, and technology tuning.

6.12 OT life cycle management checklist

Purpose: Standardize asset life cycle governance from intake to retirement. The implementor should ensure that every OT system and device follows a consistent governance process from the time it is introduced into the environment until its final decommissioning. This prevents oversight gaps, reduces security risk and maintains operational reliability throughout the asset's life.

- **Asset ID, owner, location, criticality, safety impact.**
 - Every asset should have a unique identifier, an assigned owner responsible for its operation and security, a documented physical or network location, a criticality rating, and an assessment of any safety implications if the asset fails or is compromised.
- **Baseline configuration and hardening standard recorded.**
 - At deployment, the asset's configuration should be documented, including security hardening settings (e.g., disabling unused ports, default credentials removed, secure protocols enabled). This baseline serves as a reference for future audits and troubleshooting.

- **Patch/vulnerability cadence and maintenance windows defined.**
 - Establish a schedule for applying patches and updates, based on vendor recommendations and risk assessment. Define maintenance windows to minimize operational disruption while ensuring timely remediation of security vulnerabilities.
- **Backup/restore verification schedule and RTO/RPO targets.**
 - Specify how often backups are performed, determine how frequently restore tests are conducted, and define recovery time objective (RTO) and recovery point objective (RPO) targets to guide disaster recovery planning.
- **Support status (vendor EOS/EOL), migration plan, funding source.**
 - Track vendor end-of-support (EOS) and end-of-life (EOL) dates to proactively plan for upgrades or replacements. Include migration strategies and confirm budget allocation to avoid unplanned downtime or unsupported systems.
- **Secure decommissioning steps (data purge, chain of custody, disposal).**
 - Define and follow procedures for safely removing assets from service, including secure data wiping, maintaining a documented chain of custody, and using approved disposal methods to prevent data leakage or hardware misuse.

6.13 Vendor cybersecurity compliance checklist

Purpose: Verify third-party compliance and supply chain risk controls. This ensures that all vendors, contractors and service providers handling OT systems meet defined cybersecurity requirements and maintain controls that reduce supply chain risk. This process protects against vulnerabilities introduced by external partners and enforces accountability through documented evidence.

- **Security requirements mapped to contract, evidence (SOC 2/ISO/IEC 27001, IEC 62443 conformity, SBOM, secure development attestations).**
 - Security obligations should be explicitly stated in procurement and service contracts, with vendors required to provide proof of compliance. Acceptable evidence may include third-party certifications (SOC 2, ISO/IEC 27001), OT-specific standards (IEC 62443), a software bill of materials (SBOM), and secure development process attestations.
- **Vulnerability disclosure and patch SLA (e.g., critical ≤ 30 days).**
 - Vendors must have a formal vulnerability disclosure process and commit to a service level agreement (SLA) for delivering patches, especially for critical vulnerabilities. Time frames should be risk-based (e.g., applying patches for critical issues within 30 days of discovery).
- **Remote access controls (MFA, just-in-time, session recording).**
 - Any vendor remote access to OT systems must use strong authentication (e.g., multifactor authentication), be provisioned only when needed (“just-in-time” access), and have session activities recorded for audit and investigation purposes.
- **Incident notification timelines, cybersecurity insurance, PoA&M handling.**
 - Contracts require vendors to notify the agency of security incidents within a defined time frame, carry appropriate levels of cybersecurity insurance, and provide plans of action and milestones (PoA&Ms) for remediating identified weaknesses.
- **Penetration test/secure by design documentation and remediation proof.**
 - Vendors should supply recent penetration testing results or secure-by-design documentation for their products and services, along with proof that identified vulnerabilities have been addressed. This ensures that security is considered from the design phase through deployment. Additional guidance can be found in the [North American Transit Cybersecurity Consortium Operational Technology Procurement Requirements](#).

6.14 OT risk register template

The OT risk register is a centralized tool for documenting, monitoring and managing risks to operational technology systems and processes. It provides a structured method for capturing risk details, assessing their likelihood and impact, identifying existing controls, and tracking the effectiveness of mitigation measures over time. By consolidating this information into a single register, organizations can ensure consistent risk evaluation, assign clear ownership, and maintain visibility into treatment plans and progress. The template supports proactive decision-making by enabling trend analysis; linking evidence; and aligning actions with targeted treatment strategies such as acceptance, mitigation, transfer or avoidance—ensuring operational resilience and compliance with safety, reliability and cybersecurity requirements.

Fields:

- Risk ID
- Description
- Asset/Process
- Threat/Vector
- Inherent Likelihood/Impact
- Existing Controls
- Control Effectiveness
- Residual Risk
- Trend
- Owner
- Target Treatment (accept/mitigate/transfer/avoid)
- Actions
- Due date
- Status
- Evidence link

6.15 Key performance indicators

To ensure effective implementation and continuous improvement of OT cybersecurity, it's critical to define and track clear KPIs. These metrics help organizations measure how well they are securing their operational technology environment and where attention is needed.

6.15.1 Purpose of KPIs

KPIs provide visibility into the ongoing health, maturity and responsiveness of an OT cybersecurity program. They promote accountability, guide resource allocation and support informed decision-making by translating cybersecurity goals into measurable outcomes.

Examples of OT cybersecurity KPIs:

- **Number of completed asset updates:** Track how many OT assets have received firmware updates, security patches or configuration changes within a defined period. This metric ensures that systems are being maintained against known vulnerabilities.
- **Frequency of account reviews:** Monitor how regularly user accounts and access privileges are reviewed. This is particularly important for privileged and administrative accounts. Reviews help reduce risks related to stale or unauthorized access.

- **Incident response readiness:** Assess preparedness through metrics like time to detect (TTD), time to respond (TTR), number of incident response exercises conducted, and percentage of staff trained in IR procedures. This reflects how quickly and effectively the organization can respond to cybersecurity events.

SMALL AGENCY TIP: Track cybersecurity progress using a simple monthly checklist or Excel-based log. Agencies don't need enterprise tools to create visibility and accountability.

6.15.2 Operationalizing KPIs

Agencies should use visual tools such as dashboards and monthly reports to present KPI data to stakeholders, from site managers to executive leadership. Dashboards help identify trends, anomalies and areas needing action. Regular reporting reinforces accountability across departments and supports compliance with internal policies and external regulations.

6.16 Integrating cybersecurity with physical safety and security

Ensure that OT-CMF cybersecurity controls are aligned and coordinated with the physical security and safety systems to maintain comprehensive protection of critical assets and operational integrity. Transit agencies rely heavily on physical infrastructure (signal rooms, substations, control panels), which, if accessed or tampered with, can cause severe service disruption or safety incidents. Cybersecurity measures must therefore complement physical safeguards (see [Table 9](#)).

TABLE 9
Integration Checklist

Area	Consideration	Action Step
Access control	Are OT environments physically restricted to authorized personnel?	Map cyber assets to their physical locations; align with badge/access logs.
Surveillance	Are critical OT facilities monitored by cameras?	Coordinate camera feeds with cybersecurity monitoring to cross-verify incidents.
Alarm integration	Do physical alarms notify cybersecurity teams of intrusions?	Configure physical alarms (e.g., door sensors) to trigger SIEM alerts.
Safety systems	Are safety protocols aware of cybersecurity threats?	Collaborate with safety officers to define joint response scenarios.
Maintenance access	Is there oversight for contractors accessing physical/cyber systems?	Log access times and cross-check with system activity. Consider temporary account provisioning.

6.16.1 Recommended collaboration protocols

Effective OT-CMF implementation requires seamless coordination between cybersecurity, physical security and safety teams. Cybersecurity incidents often have physical consequences, and physical breaches can create cybersecurity vulnerabilities. The collaboration protocols shown in [Table 10](#) establish clear roles, responsibilities and communication pathways to ensure that all security domains work together toward unified protection of transit operations. See Appendix J for a sample joint response plan.

APTA SS-TCS-RP-003-26
Operational Technology Cybersecurity Maturity Framework

TABLE 10
Collaboration Protocols

Role	Responsibility
Safety manager	Ensure that operational safety protocols align with cyber incident response plans.
Physical security lead	Coordinate physical access policies with OT asset locations.
OT security lead	Align cybersecurity measures with physical security and response procedures.
Incident response coordinator	Ensure that joint drills include both physical and cyber intrusion scenarios.

Related APTA standards

- APTA SS-CCS-RP-002-13**, “Securing Control and Communications Systems in Rail Transit Environments, Part II: Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones”
- APTA SS-CCS-004-16**, “Securing Control and Communications Systems in Rail Transit Environments, Part IIIb: Protecting the Operationally Critical Security Zone”
- APTA SS-CCS-RP-006-23**, “Operational Technology Cybersecurity Maturity Framework (OT-CMF) Overview”

References

- Cybersecurity and Infrastructure Security Agency, Secure By Design Series, November 29, 2023.
<https://www.cisa.gov/news-events/news/cisa-announces-secure-design-alert-series-how-vendor-decisions-can-reduce-harm-global-scale>
- Cybersecurity and Infrastructure Security Agency, “Recommended Cybersecurity Practices for Industrial Control Systems,” June 2021.
https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf
- ISA Global Security Alliance, “Security Lifecycles in the ISA/IEC 62443 Series: Security of Industrial Automation and Control Systems,” October 2020.
<https://isagca.org/hubfs/2022%20ISA%20Website%20Redesigns/ISASecure/PDFs/Miscellaneous%20PDFs/Documents-Articles-and-Technical-Papers/ISAGCA-Security-Lifecycles-whitepaper.pdf?hsLang=en>
- MITRE Corporation, “Finding Cyber Threats with ATT&CK™-Based Analytics,” 2017.
<https://www.mitre.org/publications/technical-papers/finding-cyber-threats-with-attck-based-analytics>
- National Institute of Standards and Technology (NIST), “Approaches for Federal Agencies to Use the Cybersecurity Framework,” NISTIR 8170, March 2020.
<https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8170-upd.pdf>
- National Institute of Standards and Technology (NIST), “Assessing Security and Privacy Controls in Information Systems and Organizations,” NIST Special Publication 800-53A Rev. 5, January 2020.
<https://doi.org/10.6028/NIST.SP.800-53Ar5>
- National Institute of Standards and Technology (NIST), “Automation Support for Security Control Assessments,” NISTIR 8011, June 2017. <https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8011-1.pdf>
- National Institute of Standards and Technology (NIST), “Cybersecurity Framework Version 1.1 Manufacturing Profile,” NISTIR 8183, 2020. <https://doi.org/10.6028/NIST.IR.8183r1>
- National Institute of Standards and Technology (NIST), “Developing Cyber-Resilient Systems: A Systems Security Engineering Approach Publication,” December 2021.
<https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final>
- National Institute of Standards and Technology (NIST), 2024. “The NIST Cybersecurity Framework (CSF) 2.0,” Version 2.0, February 26, 2024. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>
- National Institute of Standards and Technology (NIST), “Guide for Conducting Risk Assessments,” NIST Special Publication 800-30, September 2012.
<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>

APTA SS-TCS-RP-003-26
Operational Technology Cybersecurity Maturity Framework

- National Institute of Standards and Technology (NIST), “Guide to Cyber Threat Information Sharing,” NIST Special Publication 800-150, October 2016. <http://dx.doi.org/10.6028/NIST.SP.800-150>
- National Institute of Standards and Technology (NIST), “Guide to Industrial Control Systems (ICS) Security,” SP 800-82, Rev. 3, September 2023. <https://csrc.nist.gov/pubs/sp/800/82/r3/final>
- National Institute of Standards and Technology (NIST), “NIST Risk Management Framework Overview.” https://www.nist.gov/system/files/documents/2018/03/28/vickie_nist_risk_management_framework_overview-hpc.pdf
- National Institute of Standards and Technology (NIST), “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations,” NIST Special Publication 800-171 Rev. 3, May 2024. <https://doi.org/10.6028/NIST.SP.800-171r3>
- Santos, O., “Cisco CyberOps Associate, CBROPS 200-201, Official Cert Guide,” 2021. <https://www.ciscopress.com/store/cisco-cyberops-associate-cbrops-200-201-official-cert-9780136807834>
- U.S. Department of Energy, Cybersecurity Capability Maturity Model (C2M2), September 2021. <https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0>
- U.S. Department of Homeland Security CISA, “Transportation Systems Sector Cybersecurity Framework Implementation Guidance,” June 2015. https://www.cisa.gov/sites/default/files/publications/tss-cybersecurity-framework-implementation-guide-2016-508v2_0.pdf
- U.S. Department of Homeland Security CISA, “Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies,” September 2016. https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf
- U.S. Department of Homeland Security National Cyber Security Division, “Public Safety Communications Resiliency,” July 2017. https://www.cisa.gov/sites/default/files/publications/07202017_10_Keys_to_Public_Safety_Network_Resiliency_010418_FINAL508C.pdf

Definitions

automatic train protection (ATP): A wayside and/or onboard train system to apply emergency brakes if a signal is missed by the train operator.

automatic train supervision (ATS): Provides advanced functionalities of train control, typically including advanced automatic routing and automatic train regulation.

CISA: The Cybersecurity and Infrastructure Security Agency is a component of the U.S. Department of Homeland Security that leads the national effort to understand, manage and reduce risk to the country's cyber and physical infrastructure.

Cybersecurity Capability Maturity Model (C2M2): A tool for evaluating and improving cybersecurity. It was developed in 2012 by the U.S. energy sector and the Department of Energy. The C2M2 is managed by the DOE's Office of Cybersecurity, Energy Security, and Emergency Response, Cybersecurity for Energy Delivery Systems division.

communications-based train control (CBTC): A continuous, automatic train control system that relies on wayside data communications and/or GPS for position sensing and uses the "moving block" principle for safe train separation rather than fixed blocks with track circuits.

configuration management: A practice and process of handling hardware, software and firmware changes systematically so a device or system maintains its integrity over time.

cybersecurity: The field of protecting digital computers and networks from accidental or malicious modifications.

defense-in-depth: A layered approach to information security that uses multiple computer security techniques to help mitigate the risk of one component of the defense being compromised or circumvented.

electronic security perimeter: Adapted from NERC-CIP electric power regulations, a logical perimeter drawn around electronic assets in a security zone to separate them from other zones.

emergency cutoff (blue light) system: A safety system installed at passenger stations that cuts off traction power and notifies the control center that power has been cut at this location.

fail-safe: A device that fails in a manner that protects the safety of personnel and equipment.

interlocking: An arrangement of railway signals and signal appliances so interconnected that their movements must succeed one another in proper sequence.

IPSec: A suite of protocols for securing Internet Protocol communications that authenticates and encrypts each IP packet in a communication session.

malware: Short for malicious software. Such software is created and used by people, usually with bad intentions, to disrupt computer operations or obtain confidential information without consent.

NIST SP 800-53: NIST Special Publication 800-53, titled "Recommended Security Controls for Federal Information Systems and Organizations" (see References). Rev. 5, dated January 2020, was used in preparing this document.

APTA SS-TCS-RP-003-26
Operational Technology Cybersecurity Maturity Framework

NIST SP 800-82: NIST Special Publication 800-82, titled “Guide to Industrial Control Systems (ICS) Security” (see References). The May 2015 final version was used in preparing this document.

Operations Control Center (OCC): A central location that monitors, and in some cases controls, some portion of a transportation system. It may handle just one system or many systems simultaneously.

Operationally Critical Security Zone: A security zone containing systems necessary for proper operation of rail transit, such as SCADA, dispatch and ATS.

patch management: A regular, coordinated method for equipment vendors to update software and firmware fixes for their digital equipment at transit agencies in a timely and responsible manner.

programmable logic controller (PLC): An industrial computer used for automation of mechanical processes.

risk: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of the adverse impacts that would arise if the circumstance or event occurs and the likelihood of occurrence.

risk management: The process of identifying risk, assessing risk and taking steps to reduce risk to an acceptable level.

SCADA: A control system involving a master terminal unit and remote terminal units, used for supervisory control and data acquisition.

track circuit: An electrical circuit designed to indicate the presence or absence of a train in a specific section of track.

traction power: A network supplying power to electrically powered railways.

trusted (network): Network of an organization that is within the organization’s ability to control or manage. Further, it is known that the network’s integrity is intact and that no intruder is present.

vital: A term applied within rail safety to denote fail-safe operation. (Derived from IEEE Standard 1483, 2000 glossary, “vital function: A function in a safety-critical system that is required to be implemented in a fail-safe manner.”)

vital programmable logic controller (vital PLC): A PLC with fail-safe functions intended for safety-critical signaling and interlocking applications in rail transit.

vital signaling: The portion of a railway signaling network that contains vital equipment.

virtual private network (VPN): A computer network in which some of the connections are virtual circuits instead of direct connections via physical wires within some larger network, such as the internet. A VPN in and of itself is not necessarily secure.

whitelisting: Describes a list or register of entities that are granted certain privileges, services, mobility, access or recognition.

Abbreviations and acronyms

AI	artificial intelligence
APTA	American Public Transportation Association
ATP	automatic train protection
BAS	building automation system
CAN	controller area network
CAP	corrective action plan
CBTC	communications-based train control
CCSWG	Control and Communications Security Working Group
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CISO	chief information security officer
CMF	Cybersecurity Maturity Framework
CSET	Cyber Security Evaluation Tool
CSF	NIST Cybersecurity Framework
CSO	chief security officer
DCS	distributed control system
DHS	Department of Homeland Security
DMZ	demilitarized zone (in Purdue zoning)
ESCSWG	Energy Sector Control Systems Working Group
FIPS	Federal Information Processing Standard
FTA	Federal Transit Administration
HVAC	heating, ventilation and air conditioning
IEC	International Electrotechnical Commission
ICS	industrial control system
ICS-CERT	Industrial Control Systems Computer Emergency Response Team
IEEE	Institute of Electrical and Electronics Engineers (commonly just IEEE)
IPFIX	Internet Protocol Flow Information Export
IPSec	Internet Protocol Security
IR	incident response
ISA	International Society of Automation
IT	information technology
KPI	key performance indicator
KRI	key risk indicator
NERC-CIP	North American Electric Reliability Corporation – Critical Infrastructure Protection
NIST	National Institute of Standards and Technology
OCC	Operations Control Center
OT	operational technology
OT-CMF	Operational Technology Cybersecurity Maturity Framework
PLC	programmable logic controller
PTC	positive train control
RACI	responsible, accountable, consulted and informed
ROI	return on investment
SCADA	supervisory control and data acquisition
SDLC	system development life cycle
SIEM	security information and event management
SDOC	Standards Program’s Standards Development Oversight Council (APTA)
SOC	Security Operations Center
SOC 2	Systems and Organization Controls 2

APTA SS-TCS-RP-003-26
Operational Technology Cybersecurity Maturity Framework

ST-ISAC Surface Transportation Information Sharing and Analysis Center
TCP/IP Transmission Control Protocol/Internet Protocol
TSA Transportation Security Administration
VLAN virtual local area network
VPN virtual private network

Document history

Document Version	Working Group Vote	Public Comment/ Technical Oversight	CEO Approval	Policy & Planning Approval	Publish Date
First published	July 3, 2026	August 5, 2026	August 28, 2026	Sep. 25, 2026	Sep. 28, 2026

Appendix A: CISA recommended practices

This appendix provides links existing recommended practices from CISA. Additional supporting documents detailing a wide variety of control systems topics associated with cybersecurity vulnerabilities and their mitigation have been developed and vetted by control system SMEs. These documents will be updated, and topics added, to address additional content and emerging issues.

- “Updating Antivirus in an Industrial Control System”
 - [Full document](#)
- “Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies”
 - [Full document](#)
- “Creating Cyber Forensics Plans for Control Systems”
 - [Full document](#)
- “Developing an Industrial Control Systems Cybersecurity Incident Response Capability”
 - [Full document](#)
- “Good Practice Guide: Firewall Deployment for SCADA and Process Control Networks”
 - [Full document](#)
- “Case Study: Cross-Site Scripting”
 - [Full document](#)
- “Patch Management of Control Systems”
 - [Full document](#)
- “Securing Control System Modems”
 - [Full document](#)
- “Configuring and Managing Remote Access for Industrial Control Systems”
 - [Full document](#)

Supporting documents:

- Cybersecurity procurement language guidance:
 - [Cybersecurity Procurement Language for Energy Delivery \(ESCSWG 2014\)](#)
 - [Cyber Security Procurement Language for Control Systems \(DHS 2009\)](#)
- Mitigations for vulnerabilities in control systems networks:
 - [Mitigations for Security Vulnerabilities Found in Control System Networks](#)
- Securing control systems modems:
 - [An Undirected Attack Against Critical Infrastructure](#)
- Protecting network perimeters:
 - [Backdoors and Holes in Network Perimeters](#)
- SQL attack methodology:
 - [SQL Attack Methodology Analysis](#) (HSIN portal membership required)
- Integration Objects OPC UA Server Toolkit (Update A) :
 - Deploying Secure OPC
- Hardening OPC hosts:
 - [Hardening OPC Hosts](#)
- Security implications of OPC/OLE/DCOM/RPC:
 - [Security Implications of OPC, OLE, DCOM, and RPC in Control Systems](#)
 - [Abstract](#)
- Securing control systems:
 - [DHS Bulletin: Securing Control Systems](#)

Appendix B: OT-CMF maturity levels – implementation reference

Maturity Level	Level Objective	Key Characteristics and Activities
Level 0, Baseline (On-Ramp)	Establish minimum conditions to begin an OT cybersecurity program	- Executive leadership issues a documented cybersecurity policy and commitment - A security champion is identified with authority to advance the program - OT assets are identified and documented - Tier 1 OT-CMF controls are identified and implementation planning begins - Cybersecurity hygiene and threat awareness activities are initiated - An initial OT cybersecurity self-assessment is performed
Level 1, Initiated	Formalize adoption and begin coordinated execution	- Executive leadership formally adopts the OT-CMF - Security liaisons are appointed across business units - Purpose and ownership of OT assets are defined - Core cybersecurity procedures and processes are documented and communicated - Cybersecurity awareness activities are implemented organization-wide - OT-CMF self-assessment is performed on an annual basis
Level 2, Planned	Establish governance, policy alignment, and risk management	- Cybersecurity Governance Committee is chartered and operational - Agency-specific policies, procedures, and procurement standards are developed - OT risk management is aligned with the enterprise risk management (ERM) program - KPIs and KRIs are defined - OT safety and security zone architecture is documented - Level 2 controls are implemented; Level 3 controls are evaluated - Internal or third-party cybersecurity assessments are conducted
Level 3, Operationalized	Demonstrate consistent, measurable cybersecurity operations	- OT security monitoring and continuous improvement programs are established - Policies and procedures are enhanced, approved and enforced organization-wide - Defined reporting processes support senior leadership and system owners - Role-based OT cybersecurity training is implemented - Risk classification and impact assessment standards are applied - Level 3 OT-CMF controls are implemented - Annual independent audits are performed
Level 4, Managed	Standardize, integrate and optimize cybersecurity capabilities	- Board-level cybersecurity oversight is established - Cyber-intelligence capabilities support proactive threat awareness - Policies and procedures are standardized and optimized - Network segmentation and secure-by-design principles are enforced - Security orchestration, automation and response (SOAR) and SIEM capabilities are integrated with OT monitoring - Vulnerability remediation is automated and governed by SLAs/OLAs - Annual third-party audits continue
Level 5, Optimized	Achieve adaptive, intelligence-driven cyber resilience	- Advanced threat hunting and zero-day detection capabilities are in place - Automated, adaptive protection and response mechanisms are operational - Continuous optimization of OT cybersecurity controls is achieved - Real-time risk and threat reporting informs senior leadership - Independent audits validate continuous monitoring and automated response

Notes:

- Levels are *sequential and cumulative*; each level builds on the previous.
- Controls should be implemented *by tier* and aligned to organizational capacity.
- Agencies should avoid skipping levels or relying on ad hoc control adoption.

Appendix C: Facility risk assessment template

Identify, evaluate and mitigate combined physical and cyber risks to operational technology facilities.

Cyber Risks (e.g., malware, network access)	Existing Controls	Recommended Improvements	Facility/Location	OT Assets Present	Physical Risks (e.g., theft, vandalism, intrusion)

Instructions:

1. List each facility and the OT assets within it.
2. Identify **physical risks** and **cyber risks** separately.
3. Record **existing controls** (e.g., locks, cameras, firewalls, MFA).
4. Recommend **improvements** and assign each a priority.
5. Assign an **overall risk level** for tracking.

Appendix D: Shared log integration workflow

Purpose: Correlate physical access records with cyber system logs for anomaly detection.

Workflow steps:

1. **Collect** daily badge/access control logs from physical security systems.
2. **Export** OT/IT system log-in and activity logs from the SIEM or log management tool.
3. **Match** badge activity to log-in activity:
 - Flag log-ins **without matching physical access records**.
 - Flag physical access **without corresponding system log-ins**.
4. **Review** anomalies jointly with the physical security lead and OT security lead.
5. **Document** findings and corrective actions.

Date	Person	Badge Swipe Time	Log-In Time	Anomaly Detected?	Notes/Actions

APTA SS-TCS-RP-003-26
Operational Technology Cybersecurity Maturity Framework

Appendix E: OT-CMF quick-start visual progress tracker

Phase	Action/Control	Owner	Due Date	Status)
Foundation	Executive endorsement of OT-CMF	General Manager		☐ Not Started ☐ In Progress ☐ Complete
Foundation	Assign a security champion	OT Lead		☐ Not Started ☐ In Progress ☐ Complete
Foundation	Inventory critical OT assets	Maintenance Lead		☐ Not Started ☐ In Progress ☐ Complete
Foundation	Post cybersecurity awareness posters	HR/Safety		☐ Not Started ☐ In Progress ☐ Complete
Implementation	CM-8 Asset Inventory	OT Engineer		☐ Not Started ☐ In Progress ☐ Complete
Implementation	AC-2 Account Management	IT Security		☐ Not Started ☐ In Progress ☐ Complete
Implementation	IR-1 Incident Response Procedure	Cyber Champion		☐ Not Started ☐ In Progress ☐ Complete
Implementation	AU-12 Log Management	System Admin		☐ Not Started ☐ In Progress ☐ Complete
Implementation	SI-3 Malware Protection	IT Admin		☐ Not Started ☐ In Progress ☐ Complete
Governance	Governance Roles Matrix	Cyber Champion		☐ Not Started ☐ In Progress ☐ Complete
Governance	Cybersecurity Policy Memo	CISO		☐ Not Started ☐ In Progress ☐ Complete
Governance	Monthly Checkpoint Review	OT/IT Coordinator		☐ Not Started ☐ In Progress ☐ Complete

Appendix F: Small agency toolkit

This appendix provides simplified resources and practical guidance for small transit agencies with limited staff and budget. The goal is to make the OT-CMF framework actionable and achievable even in resource-constrained environments.

F.1 Quick-start priorities

Small agencies should begin with a few high-impact, low-cost actions:

- Maintain a basic asset inventory (Excel or Google Sheets is sufficient).
- Enforce strong password policies (length, complexity, expiration).
- Conduct quarterly access reviews for privileged accounts.
- Keep OT system software patched whenever possible.
- Create a simple incident response contact list (internal and external support).

F.2 Role consolidation template

In smaller agencies, roles may need to be combined. Responsibilities can be assigned as follows:

- **IT manager/OT supervisor** → Serves as cybersecurity lead
- **Operations lead** → Coordinates incident response
- **Finance/administration** → Tracks budget and compliance records
- **External vendor/managed service provider (MSP)** → Provides specialized cybersecurity services such as penetration testing or monitoring

F.3 Budget and resource planning

Use a phased approach to align investments with agency capacity:

- **Phase 1 (low cost):** Leverage existing staff, free/open-source tools and starter policies (levels 1 and 2).
- **Phase 2 (moderate cost):** Add basic monitoring tools, endpoint protection and staff training (levels 2 and 3).
- **Phase 3 (higher investment):** Engage managed security services, advanced monitoring, and automation for level 4 and 5 readiness.

F.4 Lightweight tools and templates

- **Asset inventory template:** Spreadsheet fields for asset name, location, function, criticality and update status.
- **Monthly security checklist:** One-page list of recurring tasks (e.g., password changes, patch reviews, backup verification).
- **Policy starter pack:** One- to two-page documents covering:
 - access control;
 - patch management; and
 - incident response.
- **Dashboard starter:** KPI tracker in Excel (green/yellow/red status for updates, access reviews, training and incidents).

F.5 Small agency callouts

When implementing the OT-CMF, small agencies should remember the following:

- **Keep it simple.** Policies can start as single-page documents.
- **Use existing resources.** Repurpose IT tools and staff for OT security.
- **Leverage partnerships.** Collaborate with regional peers, ISACs or trusted vendors.
- **Grow incrementally.** Reaching levels 1 and 2 quickly is a meaningful milestone; higher levels can be targeted later.

F.6 Minimal viable level roadmap

- **Level 1:** Asset inventory + password policy + contact list
- **Level 2:** Quarterly access reviews + patching routine
- **Level 3:** Incident response drill + KPI reporting (Excel log)

Appendix G: Mature agency toolkit

This appendix provides advanced guidance for mature transit agencies that have achieved a high level of OT-CMF maturity (Level 4 or higher). It is designed to help agencies optimize, innovate and sustain their cybersecurity posture in dynamic operational environments.

G.1 Optimization priorities

Mature agencies should focus on continuous improvement through the following:

- **Automation of security processes** (e.g., patch deployment, log analysis, compliance tracking).
- **Integration of threat intelligence** into OT monitoring and decision-making.
- **Advanced metrics** such as mean time to detect (MTTD), mean time to respond (MTTR) and predictive risk modeling.
- **Continuous workforce development** with role-based training and scenario-based exercises.

G.2 Continuous improvement framework

Agencies at this stage should establish feedback loops to sustain maturity:

- **Regular gap assessments:** Conduct biannual reviews to identify evolving risks and adjust controls.
- **Metrics calibration:** Update KPIs to focus on proactive indicators (e.g., percentage of automated responses).
- **Governance reviews:** Senior leadership conducts quarterly reviews of OT governance performance and alignment with organizational objectives.

G.3 Emerging technology integration

Mature agencies should prepare for and integrate new capabilities:

- **Industrial IoT (IIoT) and smart infrastructure:** Secure device onboarding and life cycle management.
- **Artificial intelligence and machine learning:** Apply to anomaly detection, predictive maintenance and incident triage.
- **Cloud and edge OT services:** Establish secure architectures, strong identity management and monitoring for distributed systems.

G.4 Peer collaboration and sector leadership

Agencies at levels 4 and 5 should play a leadership role in the sector by doing the following:

- **Participating in industry working groups** and ISACs to share threat intelligence and lessons learned.
- **Contributing to standards development** and pilot programs for emerging OT security practices.
- **Hosting peer exchanges** to support smaller agencies in their maturity journey.

G.5 Advanced toolkit elements

- **Automated compliance dashboard:** Real-time view of control status, incidents and performance metrics.
- **Predictive analytics models:** Identify trends that may indicate emerging vulnerabilities.
- **Red Team/Blue Team exercises:** Formal adversarial testing to validate readiness.
- **Resilience planning:** Incorporate cyber resilience into business continuity and disaster recovery programs.

G.6 Sustaining Level 5 (Optimized)

To maintain peak maturity:

- Embed cybersecurity into enterprise risk management and strategic planning.
- Establish a culture of cybersecurity-informed engineering for all OT system designs.
- Continuously adapt governance and processes to address evolving threats and technology.

Appendix H: Sample Change Control Request Form template

Change Control Form	
ID: _____	Title: _____
System/Asset: _____	
Change Type: ☐ Standard ☐ Normal ☐ Emergency	
Description and Rationale: _____ _____ _____	
Risk and Impact: ☐ Safety ☐ Reliability ☐ Cybersecurity	
Affected Controls: _____ _____ _____	
Rollback/Contingency Plan: _____ _____ _____	
Test Plan: _____ _____ _____	
Implementation Window: _____	
Post-Change Validation and Sign-Off:	
Signature: _____	Date: _____
Signature: _____	Date: _____

Appendix I: How Tier 3 is used in practice

Below is the Tier 3 (Priority 3) control set in the APTA Operational Technology Cybersecurity Maturity Framework (OT-CMF). Tier 3 represents advanced, operationalized controls that move an organization from foundational compliance into measurable, resilient and repeatable cyber operations across OT environments.

I.1 How Tier 3 is used in practice

- **Audience:** CISO, OT security leadership, operations leadership
- **Purpose:** Move from having controls to proving effectiveness
- **Outcome:**
 - Measurable reduction in cyber risk
 - Faster detection and response
 - Clear ownership and accountability
 - Defensible posture for TSA, auditors and boards

These 38 controls are typically implemented after Tier 1 (Foundational) and Tier 2 (Core) controls are in place and functioning.

I.2 Tier 3 (Priority 3) OT-CMF controls

Governance, Risk and Oversight (6)

1. Formal OT cybersecurity performance metrics and KPIs defined and tracked
2. Regular executive-level reporting on OT cyber risk posture
3. OT cyber risk incorporated into enterprise risk management
4. Documented risk acceptance and exception management process
5. Formal third-party OT cybersecurity governance process
6. Periodic independent reviews or audits of OT cybersecurity controls

Asset, Network and System Management (6)

7. Automated OT asset discovery integrated with inventory management
8. Network architecture documentation maintained and validated regularly
9. OT network segmentation enforced with policy-based controls
10. Secure configuration baselines defined for OT systems
11. Configuration drift detection implemented for critical OT assets
12. Life cycle management process for OT assets (deploy → maintain → retire)

Identity, Access and Privilege Management (5)

13. Role-based access control (RBAC) implemented for OT systems
14. Privileged access management (PAM) applied to OT administrative accounts
15. Formal user access review and recertification process
16. Remote access to OT systems controlled, logged and monitored
17. Vendor and contractor access governed by time-bound authorization

Vulnerability and Patch Management (5)

18. OT-specific vulnerability identification and classification process
19. Risk-based vulnerability prioritization tied to operational impact
20. Documented patch testing and deployment procedures for OT
21. Compensating controls defined when patches cannot be applied
22. Vulnerability remediation tracked to closure with accountability

Monitoring, Detection and Logging (6)

- 23. Centralized collection of OT logs and telemetry
- 24. Defined OT security monitoring use cases and alert thresholds
- 25. Integration of OT monitoring with SOC or monitoring function
- 26. Formal alert triage and escalation procedures
- 27. Correlation of OT alerts with safety and operational indicators
- 28. Retention and protection of OT security logs

Incident Response and Recovery (5)

- 29. OT-specific incident response plan developed and maintained
- 30. OT incident response roles and responsibilities defined
- 31. Regular OT cyber incident tabletop or functional exercises
- 32. Coordination procedures with safety, operations and communications teams
- 33. Lessons learned and corrective actions tracked post-incident

Training, Awareness and Sustainment (5)

- 34. Role-based OT cybersecurity training for engineers and operators
- 35. Executive and leadership cybersecurity awareness focused on OT risk
- 36. Incident response and recovery training for OT personnel
- 37. Contractor and vendor cybersecurity awareness requirements
- 38. Continuous improvement process based on incidents, exercises and metrics

Appendix J: Joint response plan sample

Purpose: Provide a coordinated playbook for handling incidents involving both physical and cyber domains.

Incident Type: _____

Date: _____

Reported By: _____

Step	Action	Responsible Role	Time Frame
1	Detect and validate incident (physical or cyber trigger)	SOC Analyst/Physical Security Operator	Immediate
2	Notify cross-domain response team	Incident Response Coordinator	< 15 minutes
3	Secure affected systems or areas	OT Security Lead/Physical Security Lead	< 30 minutes
4	Contain threat to prevent escalation	OT Engineer/Safety Manager	< 1 hour
5	Investigate root cause	OT Security Lead/Safety Manager	1–4 hours
6	Restore normal operations	OT Operations/Maintenance	Variable
7	Conduct post-incident review and update procedures	All Leads	Within 7 days

Appendix K: Out-of-scope item discussion

This appendix gives guidance for three topics that are out of scope for this recommended practice but are of interest to transit agencies and vendors.

K.1 How to approach security retrofits for legacy systems

Retrofitting security upgrades for legacy equipment presents special issues for transit agencies. Using the defense-in-depth model, mitigating security controls may be put in effect, including the following:

- protection around the perimeter of these devices, such as insulating them from external connections
- increased use of personnel or physical security measures as compensating or mitigating controls

K.2 Security control: How to provide isolation

Transit agencies may be able to use the application layer of the Ethernet/TCP/IP (internet) stack for communication isolation. Some security controls affecting the application layer are listed in this document, such as configuration management, detecting unauthorized software, and use of antivirus or whitelisting software.

However, there are a host of techniques that are generally more sophisticated and require more technical knowledge to research, develop, design and implement. They include the following:

- **A secure software plan by the vendors.** At the application layer, techniques that eliminate buffer overflow, format string vulnerabilities and other coding vulnerabilities may be introduced.
- **Deep packet inspection firewalls.** Depending on the protocol used, there may be application layer firewalls that look at every application layer packet to separate out illegal or unauthorized commands to networked equipment.

K.3 Upgrading legacy equipment

Upgrading legacy systems does have some additional challenges, but none that are insurmountable or prohibitively costly. The proper maturity planning will allow an organization to secure the legacy OT network as it is matured across the organization.

Areas for potential upgrade for legacy systems include the following:

- risk assessment: data and network analysis
- network segregation with next-generation firewall and protocol filtering
- monitoring both networks and devices for anomalies
- autonomous response, which is optional
- secure access control both on-vehicle and over the air
- log aggregation and reporting
- SIEM integration