APTA STANDARDS DEVELOPMENT PROGRAM
RECOMMENDED PRACTICE
American Public Transportation Association
1300 I Street, NW, Suite 1200 East, Washington, DC 20006

APTA SS-ECS-RP-001-14, Rev. 1
First Published: Oct. 17, 2014
First Revision: July 29, 2022

Enterprise Cyber Security Working Group

Cybersecurity Considerations for Public Transit

Abstract: This recommended practice establishes considerations for public transit chief information officers interested in developing cybersecurity strategies for their organizations. It details practices and standards that address vulnerability assessment and mitigation, system resilience and redundancy, and disaster recovery.

Keywords: advanced persistent attacks, cyber, cyber-assets, cybersecurity assessments, disaster recovery, enterprise cybersecurity, fallback, information security (INFOSEC), information and communication technology (ICT), information security, intrusion detection, redundancy, resilience, secure cloud, system penetration.

Summary: Cybersecurity is a growing concern for public transit managers, as control and management systems become increasingly dependent on information technology. These systems are vulnerable to increasingly sophisticated direct and indirect cyberattacks. The typical transit-based IT infrastructure comprises complex and interconnected components, subcomponents, and services. This complexity increases the exposure of these systems to threats. Given these increasing risks, the transit industry and its technology managers must take proper steps to ensure the security of their cybersystems. Working remotely has increased the risk of compromising electronic security perimeters. Transit organizations must prioritize cybersecurity control implementation and ongoing operations management.

Scope and purpose: This document provides information on and considerations for cybersecurity within the public transit industry and enterprise. This document is not a substitute for implementing a formal cybersecurity program or cybersecurity framework. Nothing in this document is intended to contradict mandatory local, state or federal governments' standards or guidelines.

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 system'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.

Table of Contents

Participants........iv
Introduction........iv

1. Overview........1
1.1 National cybersecurity strategy........1
1.2 Transportation systems sector cybersecurity strategy........2

2. Cyberthreat landscape........2
2.1 Target........2
2.2 Threats........4

3. Transportation information ecosystem........7
3.1 Operational systems........7
3.2 Enterprise information system........8
3.3 Cloud service providers........8
3.4 Managed service providers........8
3.5 Passenger information systems........9
3.6 Fare collection systems........9
3.7 Transit communications systems........10
3.8 Physical security systems........10

4. Pillars of cybersecurity........11
4.1 Governance........12
4.2 Infrastructure........12
4.3 Operations........13
4.4 People........14
4.5 Facilities........15

5. Managing information security risk........16
5.1 Cybersecurity risk management framework example........17

6. System contingency and resilience........26
6.1 Types of plans........26

7. Managing integrated cybersecurity risks........27
7.1 Systems development life cycle (SDLC)........28
7.2 Managed security service provider (MSSP)........30
7.3 Information security services and products........32

8. Standards, resources and tools........32
8.1 National Institute of Standards and Technology (NIST)........32
8.2 National Initiative for Cybersecurity Education (NICE)........33
8.3 International Organization for Standardization (ISO)........33
8.4 APTA standards and guidance........33
8.5 Federal Information Security Management Act (FISMA)........34
8.6 U.S. Computer Emergency Response Team (US-CERT)........34
8.7 Federal Information Processing Standard (FIPS)........34
8.8 SANS Institute........35
8.9 Academia and Stanford's Minimum-Security Standards........35

Related APTA standards.. 36
References.. 36
Definitions 38
Abbreviations and acronyms... 38
Summary of document changes 39
Document history 39

List of Figures and Tables

Figure 1 Information Security Diagram... 3
Figure 2 Transportation Information Ecosystem... 4
Figure 3 Threats to the Transit Sector Value Chain.................................... 6
Figure 4 NIST Cybersecurity Framework.. 12
Figure 5 Example of a Multilayered Network Security 13
Figure 6 Professional Development Ladder.. 15
Figure 7 Pillars of a Cybersecurity Risk Management Program 17
Figure 8 Identified and Unmanaged Risks.. 18
Figure 9 NIST 800-30 Reference for Cybersecurity Risk Qualification..... 19
Table 1 Assessing Likelihood of Occurrence 20
Table 2 Assessing Level of Impact.. 20
Figure 10 Statement of Cybersecurity Risk Example 21
Table 3 Identifying the Risk Decision-Maker 22
Table 4 Strategies for Managing Risk... 22
Figure 11 Risk Treatment Options Example... 23
Figure 12 Authorized Risk Management Decision Example 24
Table 5 KRI Reporting Example 25
Figure 13 Integration of Information Security in Risk Management.......... 26
Figure 14 System Life Cycle Processes.. 28
Figure 15 Supply Chain Complexity 29

Participants

The American Public Transportation Association greatly appreciates the contributions of the **Enterprise Cyber Security Working Group**, which provided the primary effort in the drafting of this document.

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

Julius Smith, Dallas Area Rapid Transit Chair Name, *Chair*

Lee Allen, *Transportation Security Administration*
Peter Anderson, *Greater Cleveland RTA*
Muneer Baig
Aldon Bordenave, *LACMTA*
Alesia Cain, Marine *Tiger Technologies*
Anthony Candarini, *AECOM*
Peter Cleveland
Timothy Coogan, *Colorado RTD*
Matthew Dimmick, *STV Incorporated*
Terry Follmer, *Cap Metro*
Ahmed Idrees, *Sound Transit*
Billie Johnson, *Regional Transit Authority*
Alan Jones, *Lextran*
Birus Kaganovich, *Hatch LTK*
Richard Lang, *TriMet*
Donald Luey, *Foothill Transit*
Clare Mueting, *TSA*
Leonard Shepherd, *Gannett Fleming*
John Sherman
Justin Smith, *Collins Aerospace*
William Tsuei, *Access Services*
Leigh Weber, *Cybersecurity Analysis*
Jeff Van Wingerden, *Sound Transit*

Project team
Austin Stombaugh, *American Public Transportation Association*
Rachel Deen, *Transit Safety & Security Solutions*

Introduction

This introduction is not part of APTA SS-ECS-RP-001-14, Rev. 1, "Cybersecurity Considerations for Public Transit."

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).

Cybersecurity Considerations for Public Transit

1. Overview

Cybersecurity is a growing concern recognized by all transit agencies where appropriate actions are urgent and required to reduce operational and financial risk. With the unprecedented pace and complexity of cyberattacks, a transit agency must be proactive in the strategic adoption of a holistic cybersecurity approach to protect critical information and fulfill its obligation to its customers. Cyber-vulnerabilities are exploited directly utilizing information technology, and the threat has grown in sophistication. A transit agency's cybersecurity strategy must be tightly woven into the organization's fabric at all levels. Eliminating all cyberthreats is impossible. However, transit agencies must take a full-spectrum risk-based approach. No longer is cybersecurity an IT department problem; it has manifested into an issue that requires involvement at the highest management level.

The American Public Transportation Association has developed several working groups to address the severe concern of cybersecurity. The mandate of these working groups is to produce guidance in maintaining adequate cybersecurity that all transit agencies, large or small, can utilize and implement. This document is a headway into a family of specific cybersecurity-related recommended practices. It is explicitly meant to provide transit agencies an overview of cybersecurity considerations. Other recommended practices that transit agencies can adopt and tailor for their immediate use are linked and referenced throughout.

1.1 National cybersecurity strategy

The nation's critical infrastructure, including transit, provides the essential services that underpin American society and serve as the backbone of its economy, security and health. The dependence on and seamless integration of technology into everyday activities and operations has brought about and exposed the critical need to address cybersecurity. APTA understands the real cyberthreats against transit infrastructure and agencies across the nation. Cyberthreats have become such an essential and sensitive concern that the current administration has identified cybersecurity as an important priority. The administration's cybersecurity strategy is twofold:

- **Improve resilience** to cyber-incidents by hardening digital infrastructure to be more resistant to penetration and disruption; improving the ability to defend against sophisticated and agile cyberthreats; and recovering quickly from incidents, whether caused by malicious activity, accident or natural disaster.
- **Reduce the cyberthreat** through working with allies on international norms of acceptable behavior in cyberspace, strengthening law enforcement capabilities against cybercrime, and deterring potential adversaries from taking advantage of remaining vulnerabilities.

The president's executive order on Improving the Nation's Cybersecurity (14028), issued on May 12, 2021, charges multiple agencies—including the National Institute of Standards and Technology (NIST)—to enhance the software security supply chain. To support and achieve the goals of the nation's cybersecurity strategy and aligning with the Department of Homeland Security (DHS), the Department of Transportation (DOT) and the Transportation Security Administration (TSA), APTA has broadly identified the following priorities for transit agencies to consider and at the minimum address concerning an agency's information and communications technology (ICT) infrastructure. The four priorities represent a broad-based, balanced information security program that addresses the management, operational and technical aspects of protecting federal information and information systems:

1. **Standards, policies, and procedures:** Transit agencies should develop, formalize and document specific standards, policies and procedures in protecting against cyberthreats and improving resilience to such incidents.
2. **Information system technology and infrastructure:** Transit agencies should ensure the capability, maintenance, serviceability and interoperability of the organization's ICT infrastructure. Transit agencies should implement a complete system development life cycle (SDLC) process that integrates risk management into the process.
3. **Awareness, training and education:** Transit agencies should focus on developing a general culture of awareness of cybersecurity. Further, transit agencies should identify specific individuals necessary to receive further training and education as part of their professional development and career progression, to enhance their internal capabilities against cyberthreats.
4. **Information security risk management integration:** Transit agencies should integrate information security into the organization's risk management strategy from the very top to align with the organization's strategy, mission and goals. Integrating information security into the risk management process will ensure proper identification and allocation of essential resources in enhancing the organization's ability to mitigate increased resilience against cyberattacks.

1.2 Transportation systems sector cybersecurity strategy

Our national security depends on an open, reliable and secure transportation system. The sector's cyber-infrastructure, which includes both business systems and physical automation systems, plays a critical role, as it enables increasingly complex and technologically sophisticated transportation operations. The sector's cyber-systems and physical automation require protection against malicious and inadvertent manipulation. Due to the numerous interdependencies within the industry, failure to protect these systems and automation may result in significant and adverse business, safety and security implications throughout the sector.

By maintaining continuous cybersecurity awareness, improving and expanding voluntary participation, defining the conceptual environment, enhancing intelligence and security information-sharing, and ensuring sustained coordination and strategic implementation, transit agencies should deter significant threats and help protect their systems. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning and resilient critical infrastructure—including assets, networks and procedures—vital to public confidence in transit, safety and well-being.

2. Cyberthreat landscape

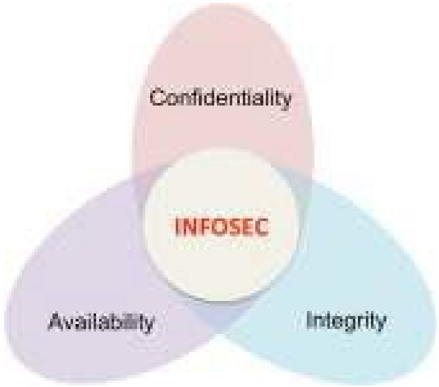
2.1 Target

The transit industry supports the movement of people and goods and includes the combination of vehicles, infrastructure and operations that enable these movements. The sector is increasingly digitalized and connected, relying on technology and interconnectivity for increased efficiency and improved functionality. With smart devices, onboard vehicle systems, Wi-Fi and next-generation GPS devices, the transit industry is experiencing significant changes thanks to transformative technologies and the internet of things (IoT). With the growing dependence on technology by governments, businesses, individuals and networks linking to the end users, cyberspace is increasingly becoming an attractive target.

An effective cyberattack against a transportation agency will seek to compromise the confidentiality, availability and/or integrity (see **Figure 1**) of the agency's information by exploiting the enterprise's ICT system:

- **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
- **Availability:** Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.
- **Integrity:** Guarding against improper information modification or destruction; this includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

FIGURE 1
Information Security Diagram

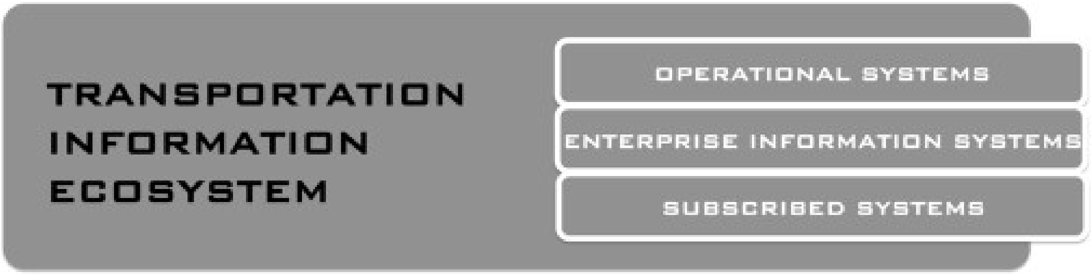


Modern transit systems are heavily dependent on various information technology systems and therefore are naturally at risk of a broad spectrum of cyberthreats. Cyberattacks can destroy a transit agency's physical systems, render them inoperable, hand over control of those systems to an outside entity, or jeopardize employee or customer data privacy.

Cyberattacks threaten every aspect of modern life that is touched— indirectly or directly—by information technology.

Typically, a transportation agency's IT infrastructure consists of three general layers (see **Figure 2**): operational systems, enterprise information systems and subscribed systems. These layers are integrated and implicitly dependent on one another for seamless operations. Each layer is critical to the operational integrity of the transit agency and—for this recommended practice—will be referred to as the transportation information ecosystem (TI ecosystem) as a whole. Systems within the TI ecosystem may share or depend upon data stored and processed within other layers.

FIGURE 2
Transportation Information Ecosystem


TRANSPORTATION INFORMATION ECOSYSTEM
OPERATIONAL SYSTEMS
ENTERPRISE INFORMATION SYSTEMS
SUBSCRIBED SYSTEMS

Cyberattacks may exploit and target specific system layers within the transit agency, including but not limited to the following:

- **Operational systems:** These systems integrate supervisory control and data acquisition (SCADA), original equipment manufacturer (OEM), and other critical component technologies responsible for the supervision, movement and monitoring of transportation equipment and services (i.e., train, track and signal control). Often such systems are interrelated into multimodal systems such as buses, ferries, paratransit and metro modes.
- **Enterprise information systems:** This describes the transit agency's information system, consisting of integrated layers of the operating system, applications systems and business system. Holistically, enterprise information systems encompass the entire range of internal and external information exchange and management.
- **Subscribed systems:** These consist of "managed" systems outside the transportation agency. Such systems may include internet service providers, hosted networks, the agency website, data storage, cloud services, etc.

2.2 Threats

Cyberspace is a unique ambiguous environment that easily allows governments, criminals, terrorists and even mischievous juveniles to mask their identity and remain anonymous. Cyberattacks directed against transportation organizations can be conducted in many ways, consisting of a single act or a combination of discrete steps threaded together. Such acts may be complicated exploitation of coding or the simple use of social engineering—the art of manipulating individuals' trust, behavior or identity—to reveal or gain access to confidential information. Once the targeted system is compromised, perpetrators might implement "backdoor" gates or install stealth code allowing data to be monitored or removed without detection. "Zero-day" switches can be implemented, which can be activated at a specified time or under a specified set of conditions, turning control of the operational or business systems over to the perpetrator.

Furthermore, cyberthreats may not all be software attacks. While cyberattacks in the form of software manipulation require a degree of expertise and technical knowledge, physical manipulation (intentional and unintentional) of the system is of genuine concern. Many attacks are known to exploit specific hardware linked to the TI ecosystem. Such examples may include manipulating infrared or laser signaling devices, jamming Wi-Fi signals, or even physically tapping or damaging critical communication cabling or nodes.

Successful cyberattacks rarely take the same form in consecutive or follow-on assaults against a targeted system. The digital environment is in its fastest form of evolution, with exponential advancements in technology and information sharing. Due to the "arms race" culture that exists in the initiating elements (criminal organizations, state actors, activists or "hacktivists") and the mitigating or responding components (government, industry and law enforcement), attacks are adapted in response to the level of success or failure with which they impact a target organization. Cyberattacks that are detected are usually contained and/or mitigated through some form of countermeasure or response. These countermeasures force the initiating elements to evolve their attack to circumvent the countermeasures. Many of the most threatening cyberattacks are now designed to hide in the system and evade detection, quarantine and/or removal by gaining control of the software that is implemented to capture the malicious software (called malware) in the first place. Additionally, such sophisticated malware is capable of regular self-updates, prolonging survivability and preventing detection. (e.g., Stuxnet).

In the transit industry, cybersecurity and technology professionals are faced with protecting their transportation information ecosystem from ransomware. Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand a ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. In recent years, ransomware incidents have become increasingly prevalent among the nation’s state, local, tribal and territorial government entities and critical infrastructure organizations. Malicious actors continue to adjust and evolve their ransomware tactics over time. The transit cybersecurity and technology community must remain vigilant in maintaining awareness of ransomware attacks and associated tactics, techniques and procedures across the country and around the world.

While many cyberattacks may be external, transit agencies, just like any other organization, are susceptible to internal attacks, such as from a disgruntled employee. An attack from an internal source has a higher probability of success and a more significant potential for damage, given the level of access and knowledge an insider may possess. Employees with minimal constraints or supervision can cause substantial damage and pose a severe threat to a transit agency.

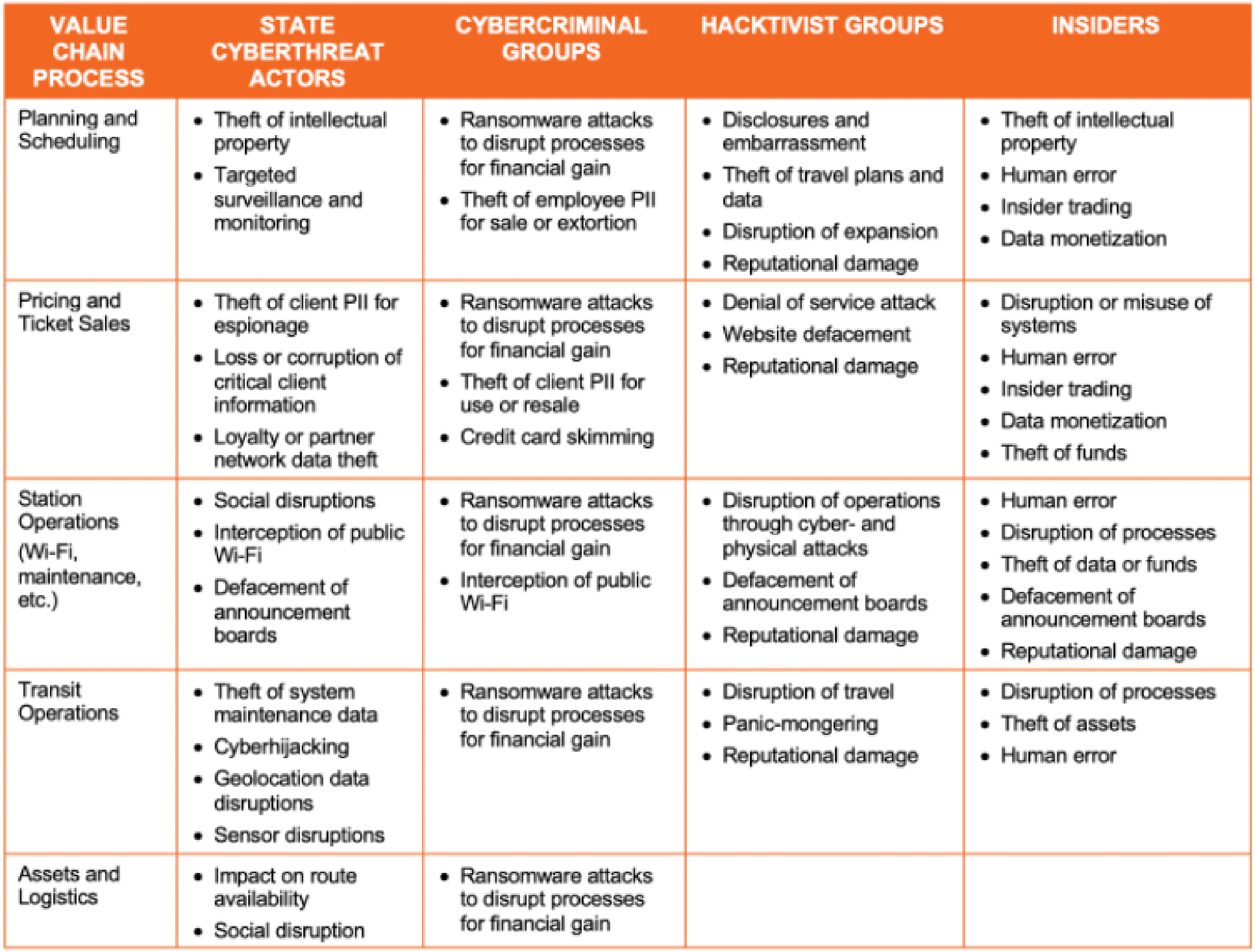
Cyberthreats and vulnerabilities of critical components of the transportation information ecosystem not only put the transit agency and the lives of passengers at risk but may also put the agency in noncompliance with many legal requirements, such as the Health Insurance Portability and Accountability Act (HIPAA), payment card industry security standards, and the Patriot Act. The compromise of the ICT systems puts confidentiality at risk and threatens the integrity and availability of the functions of the transit agency.

Cyberattacks pose a severe threat with detrimental consequences to any modern transit agency.

Cyberthreat actors institute disruptive and destructive attacks, particularly ransomware attacks; cyber–physical threats that could endanger people or property; supply chain risks; fraud; vulnerabilities associated with the integration of operational technologies (OT) and the internet of things (IoT); and cyber-enabled information operations that could discredit a transit organization or cause panic. Cyberthreats can affect all stages of the transit system value chain. As outlined in **Figure 3**, threats to the transit sector value chain are many.

FIGURE 3

Threats to the Transit Sector Value Chain



VALUE CHAIN PROCESS	STATE CYBERTHREAT ACTORS	CYBERCRIMINAL GROUPS	HACKTIVIST GROUPS	INSIDERS
Planning and Scheduling	• Theft of intellectual property • Targeted surveillance and monitoring	• Ransomware attacks to disrupt processes for financial gain • Theft of employee PII for sale or extortion	• Disclosures and embarrassment • Theft of travel plans and data • Disruption of expansion • Reputational damage	• Theft of intellectual property • Human error • Insider trading • Data monetization
Pricing and Ticket Sales	• Theft of client PII for espionage • Loss or corruption of critical client information • Loyalty or partner network data theft	• Ransomware attacks to disrupt processes for financial gain • Theft of client PII for use or resale • Credit card skimming	• Denial of service attack • Website defacement • Reputational damage	• Disruption or misuse of systems • Human error • Insider trading • Data monetization • Theft of funds
Station Operations (Wi-Fi, maintenance, etc.)	• Social disruptions • Interception of public Wi-Fi • Defacement of announcement boards	• Ransomware attacks to disrupt processes for financial gain • Interception of public Wi-Fi	• Disruption of operations through cyber- and physical attacks • Defacement of announcement boards • Reputational damage	• Human error • Disruption of processes • Theft of data or funds • Defacement of announcement boards • Reputational damage
Transit Operations	• Theft of system maintenance data • Cyberhijacking • Geolocation data disruptions • Sensor disruptions	• Ransomware attacks to disrupt processes for financial gain	• Disruption of travel • Panic-mongering • Reputational damage	• Disruption of processes • Theft of assets • Human error
Assets and Logistics	• Impact on route availability • Social disruption	• Ransomware attacks to disrupt processes for financial gain		

Many transit systems are critical infrastructure providers and, as such, could become targets for both politically and financially motivated cyberthreat activity. In fact, geopolitically motivated threat actors have targeted transportation systems as part of broader attempts to discredit or hobble a country or region. Transit agencies must be proactive and approach cybersecurity risks with a holistic solution that involves effective strategy addressing the three critical areas of IT infrastructure: operations, people and facilities. Criminals deploy tools and tactics such as commodity information stealers, bank Trojans and business email compromises to attempt to steal funds or exfiltrate personally identifiable information (PII), credit card data or other information they can monetize.

To help mitigate the growing cyberthreat against transit agencies, below is a list of recommended actions:

- Executive-level leadership involvement in the cybersecurity program
- Keeping operating systems, software and antivirus products up to date
- Disabling unnecessary remote desktop protocol (RDP) connections
- Training staff to protect themselves against phishing attacks
- Maintaining regular backups of system data
- Reviewing and enforcing policies on backups, patching, access controls, encryption and passwords

- Educating employees about the risks of disinformation, phishing and spear phishing
- Monitoring and protecting agency data
- Securing cross-domain connectivity and dispersed infrastructure
- Planning for the worst-case scenario and considering potential extortion scenarios
- Putting in place business continuity and disaster recovery plans
- Ensuring that incident response capabilities are readily available
- Having a clear media strategy
- Running regular exercises with all relevant stakeholders
- Obtaining a vulnerability assessment of the network environments

Additionally, transit agencies must rely on collaborative forums that enable knowledge sharing to promote awareness of new attacks, particularly industry-specific attacks. Raising awareness about the potential risks will improve the overall vigilance that an agency applies to these threats. Cyberthreats to transportation systems will only increase with time.

3. Transportation information ecosystem

The transportation information (TI) ecosystem is composed of layers of systems that perform various functions that allow the transit agency to deliver services to its customers (see **Figure 2**). These layers are interconnected, working in concert and sharing data among the layers. While each layer must be secured and protected, special attention is needed with interface and connectivity between layers. The links between layers often are the most vulnerable and easiest way to gain access into the TI ecosystem. (e.g., through the transit agency website to access stored data containing specific SCADA configurations.)

3.1 Operational systems

Operational technology (OT) systems in a transit agency are industrial control systems (ICS) that support operational services such as train control systems, traffic control systems, closed-loop passenger access systems and other operational services. Historically, OT/ICS systems were designed to be air-gapped and built on separate networks and controls; however, advancements in IT infrastructure and the evolution of the digital transformation and new business needs now require that the link between OT and enterprise systems be bridged.

Much attention has been placed on the vulnerabilities of ICS-based systems in recent times because of their ubiquitous implementation in multiple industries and the lengthy record of effective operations. Additionally, many of the early security designs utilize outdated digital and analog technology. Some ICS-based systems have been in operation since the 1970s, and many of the design documents and configuration standards of such systems are readily available online. ICS security controls are archaic, simple and poorly designed. Furthermore, methods to exploit security vulnerabilities and gaps of specific ICS systems are documented online by many underground hacking organizations or individuals.

Lately, ransomware attacks targeting critical infrastructure have demonstrated the rising threat of ransomware to OT assets and ICS. Given the importance of critical infrastructure to national security and America’s way of life, accessible OT assets are an attractive target for malicious actors seeking to disrupt critical infrastructure for profit or to further other objectives. As demonstrated by recent cyber incidents, intrusions affecting IT networks can also affect critical operational processes even if the intrusion does not directly impact an OT network.

3.2 Enterprise information system

The enterprise information system (EIS) is the entirety of an agency's information technology platform, which supports an organization's information and technology needs. EIS integrates core functions of the organization and can be broadly layered into three subcategories:

- **Infrastructure systems** are the core backbone of enterprise information technology and include networks, compute and storage, operating systems, and hypervisor technical services. They serve as the common platform to manage the complete hardware resources necessary for a specific applications system. Such resources include processor time, memory allocation, network communication, etc.
- **Application systems** primarily consist of user-interfaced software. Such software may be composed of proprietary software, third-party software or bundled software from the operating system. Application systems are often considered at the highest risk to cyberattacks, particularly networking-capable applications such as email and web browser applications.
- **Business enterprise systems** are specialized applications specifically responsible for managing the agency's confidential information and day-to-day business functions. Such systems include enterprise resource planning (ERP), customer relationship management (CRM), knowledge management system (KMS) and supply chain management (SCM).

3.3 Cloud service providers

A cloud service provider (CSP) is a company that offers components of cloud computing, such as infrastructure as a service (IaaS), software as a service (SaaS) or platform as a service (PaaS).

Cloud service providers use their own data centers and computing resources to host cloud computing-based infrastructure and platform services for customer organizations. Cloud services typically are priced using various pay-as-you-go subscription models. Customers are charged only for resources they consume, such as the amount of time a service is used, or the storage capacity or virtual machines used. For SaaS products, cloud service providers may either host and deliver their own managed services to users, or they can act as a third party, hosting the application of an independent software vendor.

Most enterprises, including public transportation agencies, are using CSPs to varying degrees, as it has become cost prohibitive in some cases to provide some technology services by internal IT teams. Many applications and service providers are now offering cloud-only solutions.

3.4 Managed service providers

Many transit agencies rely on third-party managed service providers (MSPs) to access and manage resources and data. Services provided by MSPs may include cybersecurity monitoring, detection and response; financial transactions; support systems maintenance; payroll; customer and employee data; and other critical operational functions.

Transit agencies must ensure that third-party vendors are compliant and meet specific information security requirements in order to provide or perform critical services. Furthermore, transit agencies must have a solid working relationship with each third-party vendor to ensure that processes and procedures are in place to facilitate cybersecurity identification, response and restoration. Such programs must be reviewed, exercised and updated regularly.

3.5 Passenger information systems

Passenger information systems are automated systems for supplying public transportation users with information about the nature and state of a public transportation service through visual, voice or other media. This can include several types of information, including the following:

- **Static or schedule information,** which changes only occasionally and is typically used for journey planning prior to departure.
- **Real-time information,** derived from automatic vehicle location systems, which changes continuously because of real-world events and is typically used during a journey (primarily how close the service is running to time and when it is due at a stop, but also incidents that affect service operations, platform changes, etc.).

Real-time information derived from automatic vehicle location systems changes continuously because of real-world events. Providing real-time information allows travelers to conduct their journey more confidently, including taking alternate steps in the event of delays. This helps to encourage greater use of public transportation.

Most transit operators now use technology to integrate passenger information systems, providing either schedule-based information through a journey planner application or schedule-based information in combination with real-time information.

Real-time information is provided to passengers in several ways, including platform-level signage, mobile phone applications, integration with existing third-party map applications, ridesharing applications, transit applications and automated public address systems. It may include both predictions about arrival and departure times and information about the nature and causes of disruptions.

3.6 Fare collection systems

Fare collection systems are the service created by integrating various technology components that automate the ticketing and ticket validation systems of a public transportation network. These individual components may include:

- fare media;
- devices to read/write media;
- depot/station computers;
- back-office systems;
- central clearinghouse applications;
- cloud presentation systems;
- mobile smartphone applications; and
- electronic payment systems.

Fare collection system implementations are now supporting integrated ticketing, which allows a person to make a journey that involves transfers within or between different transport modes with a single ticket that is valid for the complete journey (modes being buses, trains, subways, ferries, etc.). The purpose of integrated ticketing is to encourage people to use public transport by simplifying switching between transport modes and increasing the services' efficiency.

In most cases, integrated ticketing is made possible by modern electronic ticketing technologies such as magnetic stripe cards, contactless payment systems, smart cards, or mobile ticketing made possible by leveraging smartphones and current and integrated web services.

3.7 Transit communications systems

Transit communications systems are technologies that pass information from one user to another in a usable form via wire, wireless, radio, the internet or other links. Communications technologies facilitate interaction among drivers, dispatchers, emergency responders, and other personnel involved in transit and transportation operations. Typically, essential transit communications start with the conventional land mobile radio system, a wireless communications system used by transit organizations to communicate with field personnel. Communication is typically over digital and/or analog radio. Most current communications systems can transmit voice, text, data and video, while advanced communications systems are now enabling remote vehicle control. Both voice and text data can be transmitted over digital radio, the internet, cellular or other wireless networks. Preprogrammed text messages can be sent between drivers and dispatchers using a range of devices.

Examples of transit communications systems include the following:

- **Radio communications systems** consist of fixed and mobile radio equipment designed to serve an organization by allowing specific communication modes between dispatch and operators on a one-to-one or one-to-many basis. Standard radio communications systems use designated sites that can repeat and relay messages to nearby and remote sites as needed. Many frequency bands and modulation types are used for radio communications systems.
- **Wireless communications technologies** allow for electronic communications that do not utilize cables or wires. Radio frequencies are used to send messages from one device to another. The most common wireless communications technologies are short message service (SMS), general packet radio service (GPRS), 4G/LTE/5G mobile telephony, dedicated short-range communications (DSRC), Wi-Fi, WIMAX, and Bluetooth.
- **Telephony systems** are being upgraded. Traditional PBX systems and public switched telephone network (PSTN) lines between facilities upgraded with Voice over Internet Protocol (VoIP) systems for phone calls and other telephony services can reduce overall costs and provide higher reliability.
- **Mobile data terminals** (MDTs) are computerized devices used in public transit vehicles to communicate with a central dispatch office. MDTs provide two-way, text-based communications and the ability to upload data collected during a scheduled run.
- **Mobile digital computers** (MDCs) are mounted onboard transit vehicles and communicate with the dispatch office to transmit and receive real-time updates to the schedule, such as an added trip or missed passenger pickup. They also replace the driver’s paper records of activity on a shift.

3.8 Physical security systems

Physical security protects people, property and physical assets from actions and events that could cause damage or loss. This includes physical deterrence, detection of intruders and responding to those threats.

While some might consider cybersecurity and physical security to be distinct disciplines, they are in fact highly connected. The growing sophistication of physical security through technologies such as artificial intelligence and the IoT means IT and physical security are becoming more closely connected, and as a result, security teams need to be working together to secure both the physical and digital assets.

The technology systems that support these business services include but are not limited to the following:

- **Electronic access control systems** are becoming more prevalent in the physical protection of critical facilities, including those in critical infrastructure and public transportation systems. These systems use computers to solve the limitations of mechanical locks and keys. A wide range of credentials can be used to replace mechanical keys. An electronic access control system grants access based on the credential presented. When access is granted, the door is unlocked for a predetermined time, and the transaction is recorded. When an entry is refused, the door remains locked, and the attempted access is recorded. The system will also monitor the door and alarm if the door is forced open or held open too long after being unlocked.

- **Surveillance systems** include everything from proximity alarms and CCTV to sound and movement sensors and logs of who went where. Companies can deploy far more sophisticated detectors at more high-risk locations such as proximity, infrared, image, optical, temperature, smoke and pressure sensors to maintain a holistic view of their facilities. CCTV systems are becoming integrated with digital video recorders and network video recorders that can support archival and historical playback of video. Video analytics is a growing trend providing real-time alerts, smart alerts, watch lists and rules. These platforms drive exponential value from surveillance system investments by making video searchable, actionable and quantifiable.
- **Emergency response systems** facilitate reporting incidents and deployment of first responders to emergencies and include digital E911 systems and emergency dispatch communications systems.
- **Enterprise incident management systems** offer a holistic approach to the critical task of incident response. Advanced enterprise incident management technology enables mass transit and long-distance rail operators and infrastructure providers to improve the detection, recording and processing of incidents to significantly accelerate a response. This helps organizations minimize the impact of incidents, maintain punctuality, save cost, build passenger trust, and comply with regulations and external audits.

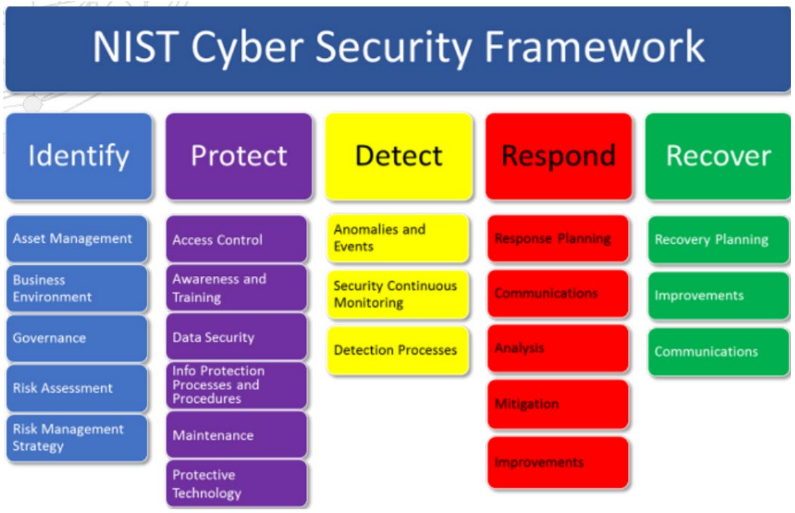
Enterprise incident management systems often integrate several disparate technology platforms, such as surveillance systems, access control systems, personal and vehicle location tracking, and integration with other communications and emergency response systems. This combination of information is then converted into a high degree of holistic situational awareness that guides operators in the control room through effective response and communication processes.

4. Pillars of cybersecurity

Cybersecurity domains include four critical domains for transportation organizations to consider when developing their information security (INFOSEC) strategies. They are cyber system infrastructure, operations, people and facilities. Addressing each domain is critical to maturing an agency’s cybersecurity capability and resilience. An appropriate INFOSEC strategy is designed to ensure and maintain confidentiality, preserve integrity, and sustain the availability of operationally critical data and information. Interdependencies and interactions between each domain must be understood so appropriate security levels can be identified and implemented. APTA has identified the NIST Cybersecurity Framework (NIST CSF) shown in **Figure 4** as a proper cybersecurity framework for transit agencies to consider for adoption and security risk management.

NIST CSF provides a common language for understanding, managing and expressing cybersecurity risk to internal and external stakeholders. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business and technological approaches to managing that risk. It can be used to manage cybersecurity risk across entire organizations, or it can be focused on the delivery of critical services within an organization.

FIGURE 4
NIST Cybersecurity Framework



4.1 Governance

Effective online and physical security is an enterprise objective and cannot be achieved through siloed management of business IT security or operational technology (OT) security. Information and cybersecurity governance requires active participation from senior managers across the organization, including risk management, finance, operations, business IT, legal, shared services, etc. Transit agencies must meet their obligations to safety and to protect, secure and control critical information.

Governance identifies the desired cybersecurity end state for the transit agency while ensuring that the agency's short- and long-term strategies are aligned and implemented. If a formalized security framework has not been selected and implemented, transit agencies should consider adopting and developing NIST CSF as an information security governance framework.

4.2 Infrastructure

System infrastructure is broadly divided into three codependent segments: hardware, software and configuration management. These are critical supporting elements of operational data and information exchange. In a multilayered cybersecurity approach (**Figure 5**), network security has dependencies on the relationship and management across hardware, software and configuration management disciplines.

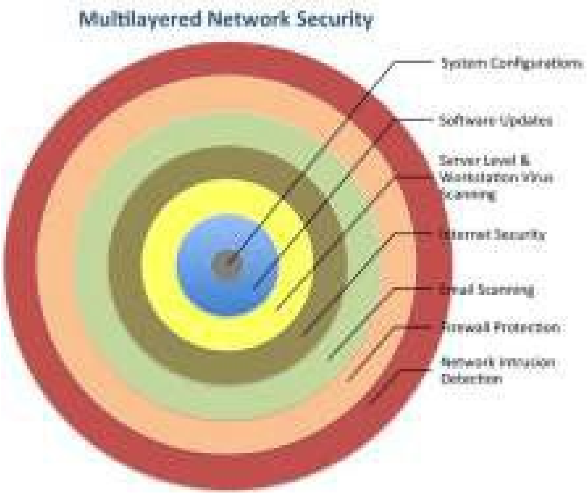
- **Hardware:** Cyber-system infrastructure includes operating systems and their associated cyber-assets, networks, physical hardware, and supporting facilities (e.g., HVAC, electricity, water). Supporting facilities include Operations Control Centers.[1] Hardware advancements are creating more innovative, faster, smaller and more secure equipment. It is essential for transit agencies to implement management strategies that address the acquisition and management of hardware to maximize the use and security of advanced technology. Acquisition lifespan management allows transit agencies to determine IT requirements, identify alternatives, select suitable solutions, integrate new solutions, maintain current operations and retire legacy systems at the appropriate time.
- **Software:** Business and operational platforms allow end-user integration and facilitate the control, processing and storage of sensitive or operationally critical data and information. Transit agencies must ensure that the latest software updates are reviewed and implemented to reduce risk by

[1] Refer to APTA-RT-OP-S-005-03, Rev. 3.

addressing specific security gaps as they are discovered. Security software and/or managed security services should be deployed as part of the transit agency's cybersecurity defense. This will include identifying potential issues, response to identified incidents, recovery and post-incident activities. One or more software packages or service providers may be deployed for the protection of the systems before a cybersecurity event being detected.

- **Configuration:** Baseline device or system configurations create a more secure operations environment. Baseline configurations allow tracking intentional changes to critical operational systems and then detecting nefarious changes made by bad actors (internal or external).

FIGURE 5
Example of a Multilayered Network Security


Multilayered Network Security
System Configurations
Software Updates
Server Level & Workstation Virus Scanning
Internet Security
Email Scanning
Firewall Protection
Network Intrusion Detection

A priority of cybersecurity needs is listed below:

- A complete, up-to-date inventory of all cyber systems and associated cyber assets used in critical operations and supporting functions. The organization must understand the cybersecurity risk to organizational operations (including mission, functions, image or reputation), organizational assets, and individuals.
- Baseline configurations of all cyber assets that make up a cyber system (i.e., SCADA) or support the IT/OT environment.
- Change management process or system that enables the tracking of each cyber-assets baseline configuration and intentional or unintentional changes made to that configuration.
- Logging, monitoring and alerting on baseline configurations tied to a Cybersecurity Incident Response Process (CSIRP) and Cybersecurity Incident Response Team (CSIRT) roles and responsibilities.

4.3 Operations

Operations manage the policies, procedures and processes in which transit agencies will implement, enforce and maintain cybersecurity practices. Policies, processes and procedures establish the necessary structure and boundaries for cybersecurity within the transit agency. A structured approach provides direction and guidance to transit agencies. Transit agencies must publish, communicate and enforce policies to enable the use of the pillars of cybersecurity and be proactive in handling cybersecurity-related threats. Established policies and processes minimize the risk of social engineering, information exploitation, internal threats, etc. Such plans must be reviewed, exercised and updated regularly.

Transit agencies should consider the following types of policies, processes and procedures to achieve the following:

- Define and prioritize the organization's mission, objectives, stakeholders and activities to establish cybersecurity roles and responsibilities, and refine risk-management decisions. Priorities for organizational mission, objectives and activities must be established and communicated.
- Develop policies, processes and procedures to manage and monitor the organization's regulatory, legal, risk, environmental and operational requirements to inform cybersecurity risk management. Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, must also be understood and managed. The organization's priorities, constraints, risk tolerances and assumptions are established and used to support operational risk decisions.
- Establish cybersecurity roles and responsibilities for the entire workforce, as well as third-party stakeholders (e.g., suppliers, customers and partners).
- Identify, establish, assess and manage cyber supply chain risk management processes to ensure agreement by organizational stakeholders. Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.
- Educate and train personnel and partners on applicable cybersecurity awareness to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures and agreements.
- Maintain security policies (that address purpose, scope, roles, responsibilities, management commitment and coordination among organizational entities), processes, and procedures that are used to manage the protection of information systems and assets.
- Manage technical security solutions to ensure the security and resilience of systems and assets, consistent with related policies, procedures and agreements.
- Execute and maintain response processes and procedures to ensure a response to detected cybersecurity incidents.
- Coordinate response activities with internal and external stakeholders (e.g., external support from law enforcement agencies).
- Execute and maintain recovery processes and procedures to ensure restoration of systems or assets affected by cybersecurity incidents.
- Coordinate restoration activities with internal and external parties (e.g., coordinating centers, ISPs, owners of attacking systems, victims, other CSIRTs and vendors).

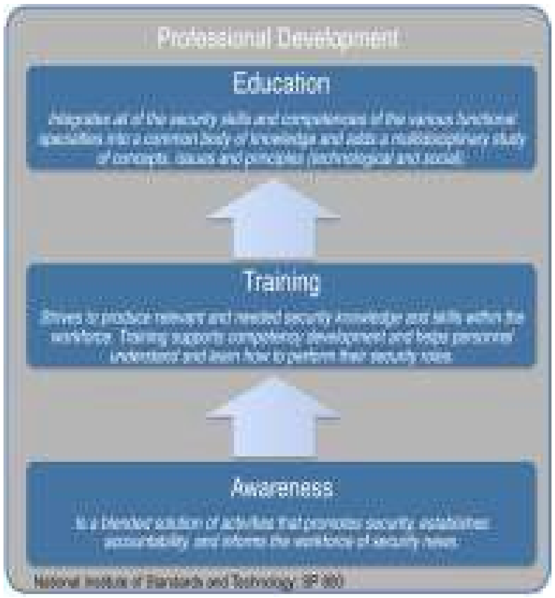
4.4 People

The human element remains the weakest link in any security program. However, transit agencies can build a culture of awareness within the organization, creating like-minded individuals to further support and be supported by the other pillars. Building a culture of awareness and further enhancing cybersecurity capabilities consists of three primary areas (**Figure 6**):

- **Education** integrates all the security skills and competencies of various functional specialties into a common body of knowledge and adds a multidisciplinary study of concepts, issues and principles. Information security education strives to produce information security specialists and professionals who are capable of vision and proactive responses.
- **Training** aims to produce relevant and needed security knowledge and skills within the workforce. Training supports professional development and assists personnel in performing their security roles, as outlined by their duties and responsibilities. The most important difference between training and awareness is that training seeks to teach skills that allow an individual to perform a specific function at a certain level of competency, while awareness seeks to focus an individual's attention on an issue or a set of issues. Awareness and training typically involve all the staff of a given organization.

- **Awareness** is a blended solution of activities that promote security, establish accountability and inform the workforce. An awareness program includes a variety of tools of communication, outreach and metrics development. Awareness programs continually push and reinforce security themes to users in a variety of formats and provide them security information. The first part of addressing awareness is to introduce concepts of responsibility, expectations, and accountability as a platform on which to develop the necessary skills.

FIGURE 6
Professional Development Ladder


Professional Development
Education
Integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge and adds a multidisciplinary study of concepts, issues and principles (technological and social).
Training
Strives to produce relevant and needed security knowledge and skills within the workforce. Training supports competency development and helps personnel understand and learn how to perform their security roles.
Awareness
Is a blended solution of activities that promote security, establishes accountability, and informs the workforce of security news.

National Institute of Standards and Technology: SP 800

Awareness and training programs should incorporate the mission, goals and objectives identified in the information security strategic planning process.

4.5 Facilities

Many attacks come in the form of compromising the physical hardware of an organization's IT/network infrastructure. There are six areas of physical and environmental security controls that should be assessed:

- **Access control:** Unauthorized access to a transit agency's information network or premises places the whole organization at risk. Physical access control should not be limited to physical hardware storage but needs to include the location of communication transmission wires, electric power sources, HVAC and any other resources possessing a link to ICT infrastructure.
- **Fire safety:** Building fires are a significant threat, and prevention is of high importance. Fires have the potential to take human life, as well as destroy hardware and data. Transit agencies must evaluate the fire safety of the physical environment and develop plans to mitigate potential losses in the event of a fire.
- **Supporting utilities:** Failures in heating and air conditioning systems and electrical services may cause service interruption and damage equipment. Transit agencies should identify and implement redundancies to ensure uninterrupted service.
- **Building structure:** Natural disasters may weaken and compromise the safety of the building. Transit agencies need to develop contingency plans to identify alternative locations for business operations and information security.

- **Interception of data:** Data may be intercepted, posing a significant risk to any transit agency. Data interception could occur through direct observation, interception of transmission or electromagnetic interception (i.e., Wi-Fi).
- **Portable media:** Viruses, worms and other malware used to exploit an information system may be carried on mobile media. Such portable media are easily concealed and pose a significant risk to any transit agency. Transit agencies should treat portable media as a controlled object and implement policies and procedures in authorizing the transportation and use of mobile media with their IT equipment.

An assessment will enable the transit agency to be resilient against ISP interruptions, physical damage, unauthorized disclosure/access, loss of system integrity and theft. Transit agencies must ensure compliance with all federal, state and local requirements concerning safety and security.

5. Managing information security risk

This section presents an overview of the significance of managing information security risk within the organization, based on key concepts and principles established by the National Institute of Standards and Technology (NIST).

- NIST 800-30, “Guide for Conducting Risk Assessments”: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
- NIST 800-39, “Managing Information Security Risk”: https://csrc.nist.gov/publications/detail/sp/800-39/final

ISO also publishes comprehensive and thorough risk management processes; see Section 8 for further reference.

An effective and robust information security program must implement a robust risk management process. In terms of organizational risk management, the primary goal of any organization is to protect the organization, continue operations and minimize unnecessary liabilities. However, information security often has been viewed as a technical process to be left out of the scope of the risk management process. Such practices often provided limited perspective and left the organization vulnerable because of inadequate resources allocated to information security. Therefore, the risk management process of information security must not be viewed as a technical task but must be an essential management function of the organization. Information security should be incorporated into the larger context of the risk-management strategy, achieving the organization’s strategy, mission and goals.

As defined by NIST, the objective of information security is the following:

- Ensure that senior leaders/executives recognize the importance of managing information security risk and establish appropriate governance structures for managing such risk.
- Ensure that the organization’s risk-management process is being effectively conducted across the three tiers of organization, mission/business processes and information systems.
- Foster an organizational climate where information security risk is considered within the context of the design of mission/business processes, the definition of an overarching enterprise architecture and system development life cycle processes.
- Help individuals with responsibilities for information system implementation or operation better understand how information security risk associated with their systems translates into organization-wide risk that may ultimately affect the mission/business success.

The successful implementation of information security objectives is heavily dependent on senior leadership, such that risk management must be a core function of the organization. Senior leadership must take ownership of the process to implement and manage an effective risk-management program. Effectively managing information security risk requires the following:

- Assigning risk management responsibilities to senior leaders/executives.
- Ensuring that senior leadership recognizes and understands information security risks to organizational operations and assets, individuals, and other organizations.
- Establishing the organizational tolerance for risk and communicating the risk tolerance throughout the organization, including guidance on how risk tolerance impacts ongoing decision-making activities.
- Accountability by senior leadership for their risk management decisions and for the implementing of effective, organization-wide risk management programs.

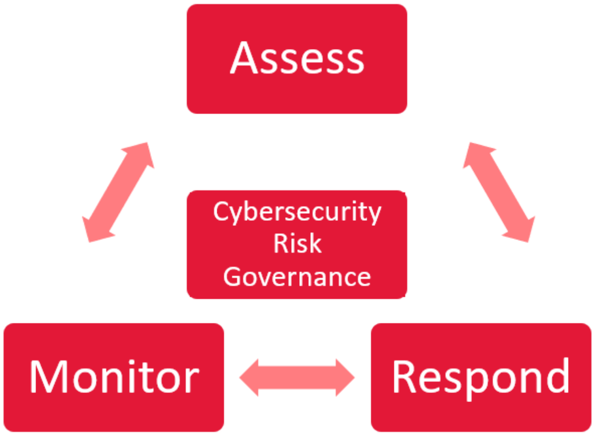
Section 5.1 represents an example of a successful risk management framework that has been put in place at a public transit organization, but risk management plans can vary among organizations and still be successful.

5.1 Cybersecurity risk management framework example

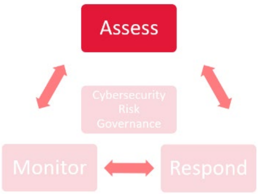
An agency's cybersecurity risk management framework should be composed of four pillars that form a cybersecurity risk management program (**Figure 7**).

1. **Risk governance:** Ensure that cybersecurity risk management practices are aligned to the agency's organizational risk appetite and that business stakeholders are aware of the cybersecurity risks they are accountable for. Risk governance occurs throughout the risk management life cycle.
2. **Assess risk:** Ensure that all identified cybersecurity risks collected are evaluated based on a standardized qualitative model.
3. **Respond to risk:** Ensure that all identified risks are managed and that risk decisions are made by appropriate and authorized risk owners.
4. **Monitor risk:** Communicate the status of the agency's cybersecurity risk via regular reporting of KRI (key risk indicators). Risk remediation activities are tracked according to an enforced reporting schedule.

FIGURE 7
Pillars of a Cybersecurity Risk Management Program



5.1.1 Assess risk



The Assess phase identifies, prioritizes and estimates risk resulting from the operation and use of information systems to organizational operations, organizational assets and the public. Risk assessments use the results of threat and vulnerability assessments to identify and evaluate risk in terms of likelihood of occurrence and potential adverse impact (i.e., magnitude of harm) to organizations, assets and individuals.

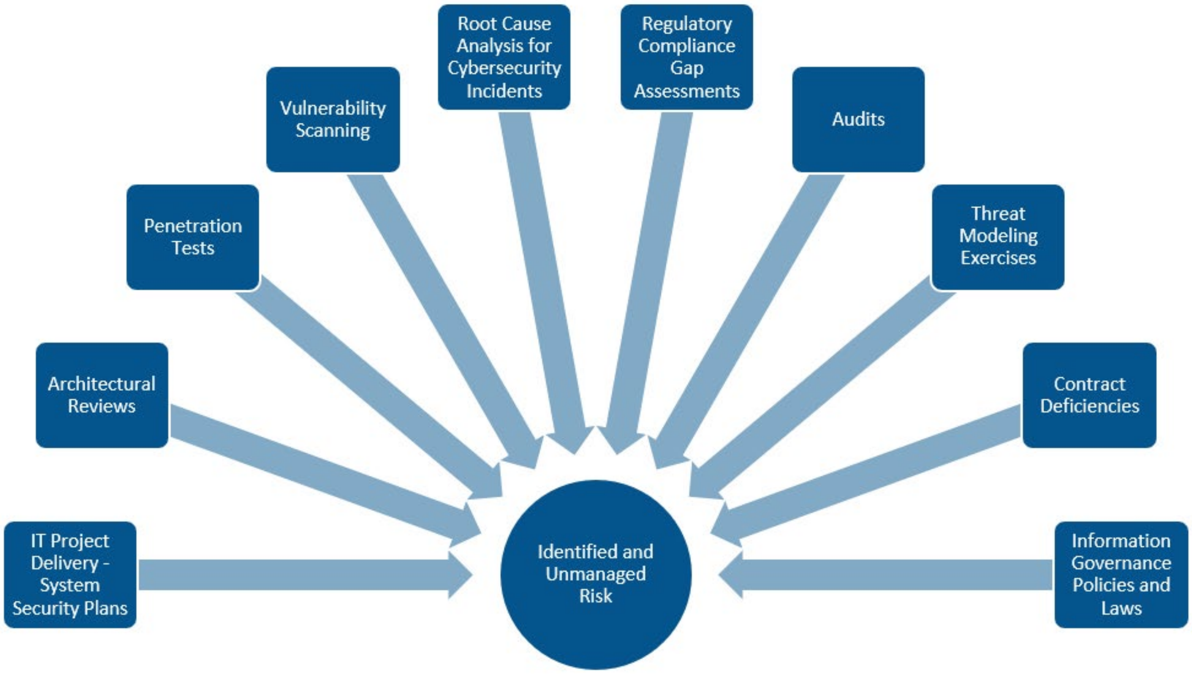
There are four primary components to the Assess phase:

1. Identifying risk
2. Cybersecurity Risk Management Working Group
3. Performing the risk assessment
4. Documenting the Statement of Cybersecurity Risk

5.1.1.1 Identifying risk

Risk identification is likely already occurring at agencies via in-place business processes. The results of these processes will be used as the input for scoring risk. These identified and unmanaged risks (**Figure 8**) should be stored in a risk management tracking and reporting tool until they can be reviewed by the agency's Cybersecurity Risk Management Working Group.

FIGURE 8
Identified and Unmanaged Risks


Root Cause Analysis for Cybersecurity Incidents
Regulatory Compliance Gap Assessments
Vulnerability Scanning
Audits
Penetration Tests
Threat Modeling Exercises
Architectural Reviews
Contract Deficiencies
IT Project Delivery - System Security Plans
Identified and Unmanaged Risk
Information Governance Policies and Laws

5.1.1.2 Cybersecurity Risk Management Working Group

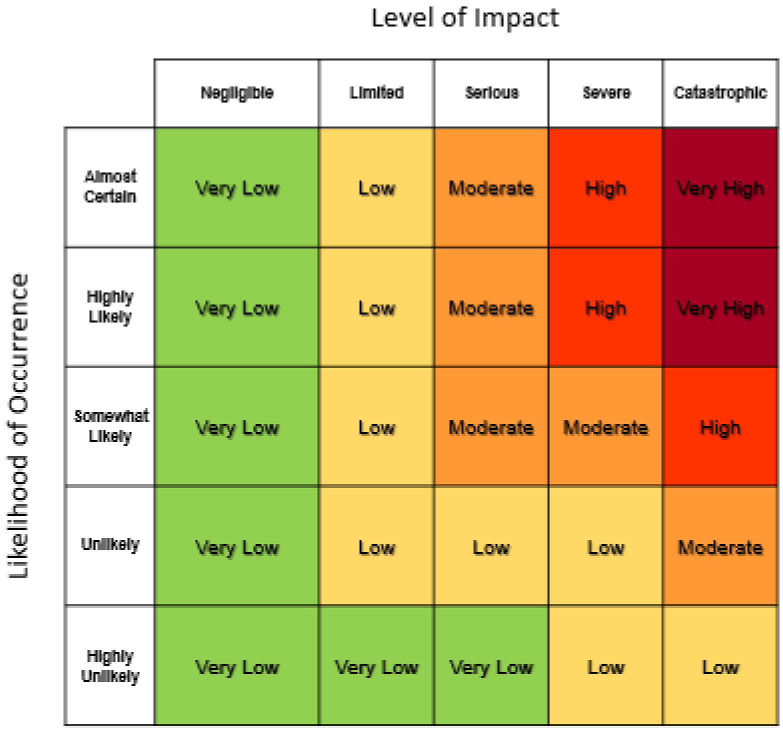
This group is a governing body that should be formed at the transit agency with the goal of performing consensus and standards-based risk scoring. It should be comprised of risk and technology stakeholders at the agency. For example, the group could consist of members from the following departments:

- Cybersecurity
- Information Technology
- Information Governance
- Risk Management
- General Council
- Rail Operations
- Bus Operations
- Public Safety

5.1.1.3 Performing the risk assessment

Measuring cybersecurity risk is the process of determining the likelihood of the threat being exercised against the vulnerability and the resulting impact from a successful compromise. Likelihood and impact are assessed on the system as it is operating at the time of the assessment. To ensure that risk assessments are consistent, it is important to utilize a standard definition on all risk assessments, such as the model in **Figure 9**.

FIGURE 9
NIST 800-30 Reference for Cybersecurity Risk Qualification


Level of Impact
Likelihood of Occurrence

	Negligible	Limited	Serious	Severe	Catastrophic
Almost Certain	Very Low	Low	Moderate	High	Very High
Highly Likely	Very Low	Low	Moderate	High	Very High
Somewhat Likely	Very Low	Low	Moderate	Moderate	High
Unlikely	Very Low	Low	Low	Low	Moderate
Highly Unlikely	Very Low	Very Low	Very Low	Low	Low

Defining likelihood of occurrence

The likelihood of occurrence is a weighted risk factor based on an analysis of the probability that a given threat can exploit a shared vulnerability. See **Table 1**.

TABLE 1
Assessing Likelihood of Occurrence

Likelihood	Likelihood Description
Almost Certain	Occurs often/weekly
Highly Likely	Could easily happen/monthly
Somewhat Likely	Could happen or have known it to happen/yearly
Unlikely	Hasn't happened yet but could/once every 10 years
Highly Unlikely	Conceivable/once every 100 years

Defining the level of impact

The level of impact from a threat event is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, loss of information or information system availability, etc. To ensure repeatability, the impact is best defined as meaningful, reusable and easily communicated across the organization. See **Table 2**.

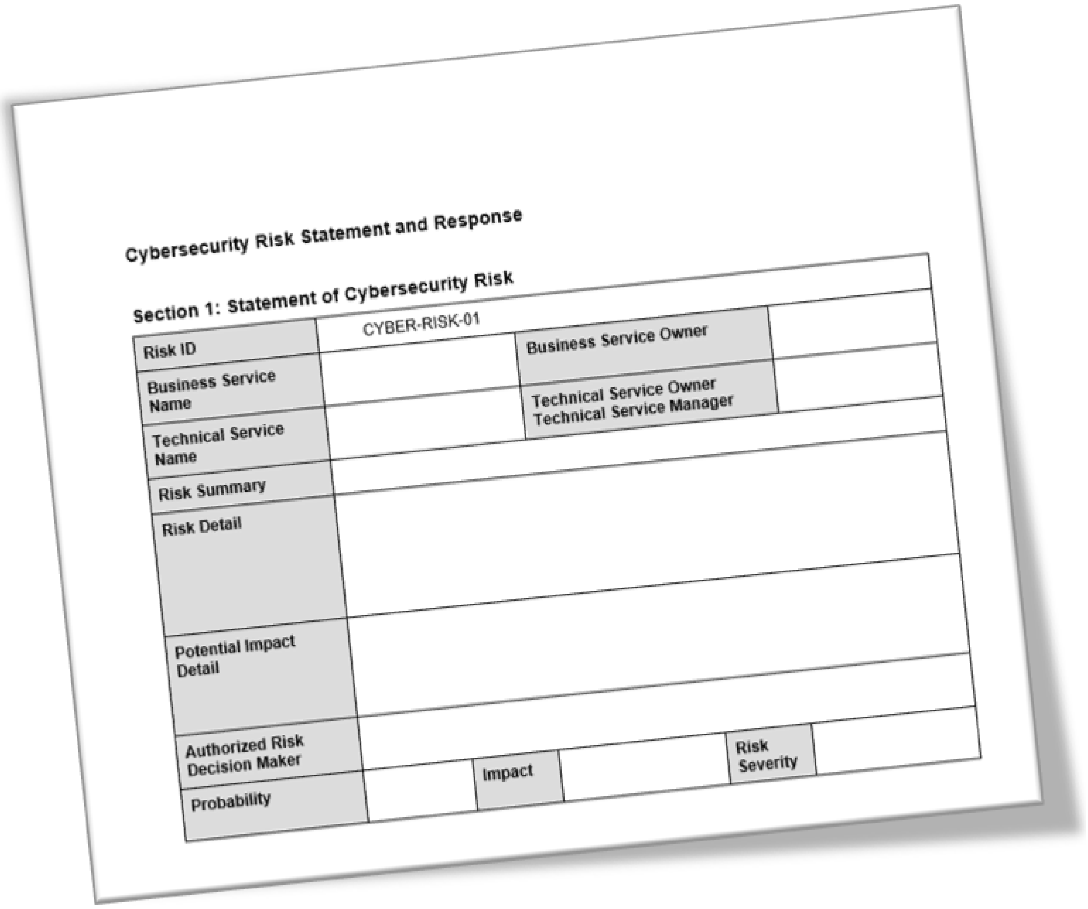
TABLE 2
Assessing Level of Impact

Impact	Impact Description
Catastrophic	A catastrophic threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, assets, individuals, other organizations or the nation.
Severe	A severe threat event might (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving serious life-threatening injuries.
Serious	A serious threat event might (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Limited	A limited threat event might (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but their effectiveness is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Negligible	A negligible threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, other organizations, individuals or the nation.

5.1.1.4 Documenting the Statement of Cybersecurity Risk

Once the level of risk has been determined, there is enough information to consider the risk assessment to be complete. This information, along with other details of the business service and technical service, should be compiled and finalized in the Statement of Cybersecurity Risk section of the Cybersecurity Risk Statement and Response (**Figure 10**).

FIGURE 10
Statement of Cybersecurity Risk Example

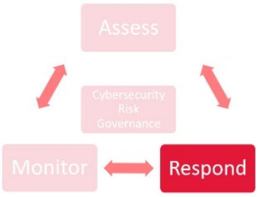


Cybersecurity Risk Statement and Response

Section 1: Statement of Cybersecurity Risk

Risk ID	CYBER-RISK-01		Business Service Owner		
Business Service Name			Technical Service Owner Technical Service Manager		
Technical Service Name					
Risk Summary					
Risk Detail					
Potential Impact Detail					
Authorized Risk Decision Maker					
Probability		Impact		Risk Severity	

5.1.2 Respond to risk



Risk response identifies, evaluates, decides on and implements appropriate risk management strategies designed to accept, avoid, mitigate or transfer cybersecurity risk that results from the operation and use of information systems.

The primary components to the Respond phase include the following:

1. Identify the authorized risk decision-maker
2. Risk management strategy
3. Proposal of risk treatment options
4. Finalize risk management decision

5.1.2.1 Identify the authorized risk decision-maker

The hierarchy of cybersecurity risk management accountability and decision-making should scale with the severity of the risk. The agency's senior leadership should have visibility and accountability for high-risk cybersecurity threats and vulnerabilities, but to maintain efficiency, responsible parties lower in the organization should be empowered to make risk management decisions as well. See **Table 3**.

TABLE 3
Identifying the Risk Decision-Maker

Severity of Risk	Authorized Official	Position Classification
Very High	Executive	General manager
High	Business service owner	Assistant general manager
Moderate	Business service owner	Assistant general manager OR senior manager
Low	Technical service owner	Senior manager OR manager
Very Low	Technical service manager	Manager

5.1.2.2 Risk management strategy

The purpose of assessing risk is to assist authorized risk decision-makers in prioritizing and managing the cybersecurity risk they are responsible for. For each identified risk, a management strategy must be devised that brings the risk to an acceptable level for an acceptable cost and in alignment with the risk tolerance of the organization. There are four basic strategies for managing risk, outlined in **Table 4**.

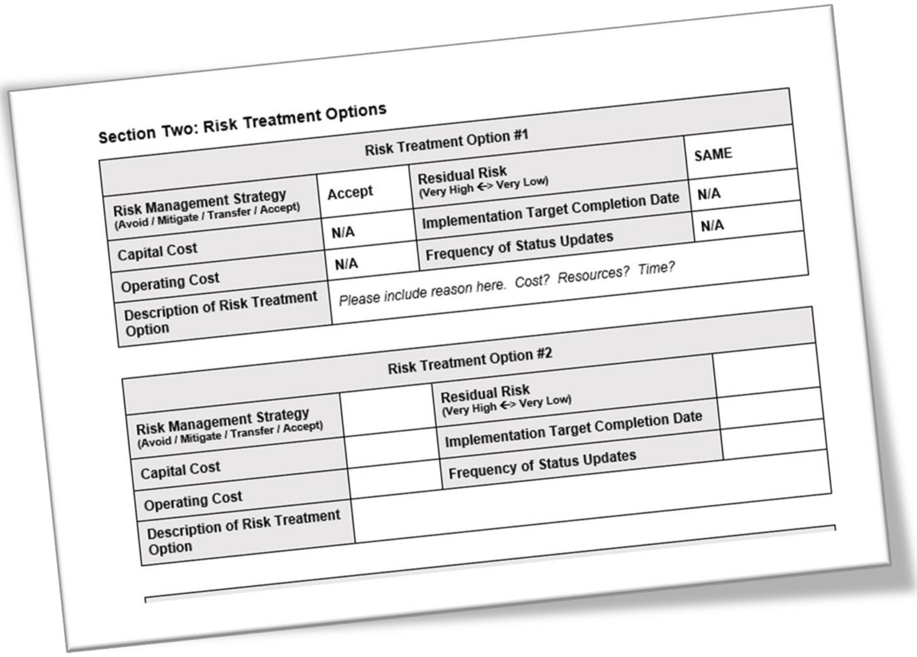
TABLE 4
Strategies for Managing Risk

Risk Management Strategy	Description
Avoid	Risk avoidance involves taking evasive maneuvers away from the risk event—for example, canceling a project or decommissioning a technology. Risk avoidance targets risk probability, decreasing the likelihood of the risk event occurring.
Mitigate	Risk mitigation actions are risk responses that reduce the probability and impact of the risk event. Risk mitigation actions can either be to implement new controls or enhance existing ones.
Transfer	Risk transfer is the exchange of uncertain future costs for fixed present costs. Often, the uncertain future cost of an IT risk event can be transferred to a third-party insurer who assumes the risk in exchange for insurance premiums, or to a third-party service provider who assumes the risk via a contract. Transferring the risk does not necessarily mean the risk has been removed, but it does transfer the ownership of the risk.
Accept	Accepting a risk means absorbing the expected cost of a risk event. It is a conscious and deliberate decision to retain the threat.

5.1.2.3 Proposal of risk treatment options

The Cybersecurity Risk Management Working Group, in addition to assessing the risk, should propose risk treatment options to inform the authorized risk decision-maker on potential solutions for managing risk. These risk treatment options should be formally documented in the Risk Treatment Options section of the Cybersecurity Risk Statement and Response (**Figure 11**) and should include information such as a description of the initiative(s), estimate of costs and timelines associated with completion. Once the risk treatment options are finalized, the Cybersecurity Statement of Risk and Response document is completed and needs to be delivered and communicated to the authorized risk decision-maker.

FIGURE 11
Risk Treatment Options Example



Section Two: Risk Treatment Options

Risk Treatment Option #1			
Risk Management Strategy (Avoid / Mitigate / Transfer / Accept)	Accept	Residual Risk (Very High <-> Very Low)	SAME
Capital Cost	N/A	Implementation Target Completion Date	N/A
Operating Cost	N/A	Frequency of Status Updates	N/A
Description of Risk Treatment Option	*Please include reason here. Cost? Resources? Time?*		

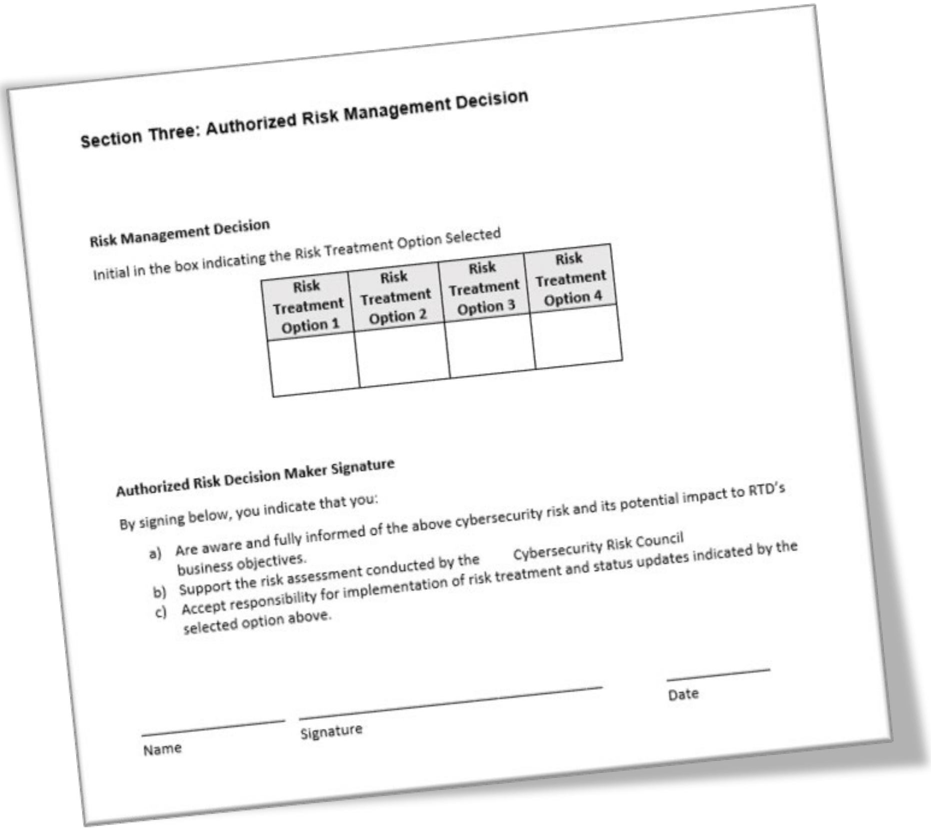
Risk Treatment Option #2			
Risk Management Strategy (Avoid / Mitigate / Transfer / Accept)		Residual Risk (Very High <-> Very Low)	
Capital Cost		Implementation Target Completion Date	
Operating Cost		Frequency of Status Updates	
Description of Risk Treatment Option			

5.1.2.4 Finalize the risk management decision

The authorized risk decision-maker is responsible for making an informed decision on the treatment of the identified cybersecurity risk. They can choose one or more of the risk treatment options proposed by the Cybersecurity Risk Management Working Group, or they may create and choose a different option.

In this step, the Authorized Risk Management Decision section of the Cybersecurity Statement of Risk and Response (**Figure 12**) needs to be completed and authorized via digital signature. If a risk management decision is not made by the authorized risk decision-maker within one month of receiving the risk treatment options from the Cybersecurity Risk Management Working Group, then the risk will be marked as "unmanaged" and will be monitored and reported as such. It is the responsibility of the authorized risk decision-maker to sponsor and fund risk treatment activities and to ensure that updates are provided to the Cybersecurity Risk Management Working Group on a regular basis.

FIGURE 12
Authorized Risk Management Decision Example



Section Three: Authorized Risk Management Decision

Risk Management Decision

Initial in the box indicating the Risk Treatment Option Selected

Risk Treatment Option 1	Risk Treatment Option 2	Risk Treatment Option 3	Risk Treatment Option 4

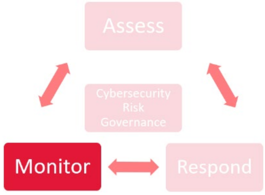
Authorized Risk Decision Maker Signature

By signing below, you indicate that you:

a) Are aware and fully informed of the above cybersecurity risk and its potential impact to RTD's business objectives.
b) Support the risk assessment conducted by the Cybersecurity Risk Council
c) Accept responsibility for implementation of risk treatment and status updates indicated by the selected option above.

Name　　Signature　　Date

5.1.3 Monitor risk



Risk monitoring provides agencies with the means to verify compliance of risk treatment activities and to identify risk-impacting changes to organizational information systems and environments of operation. It also allows agencies to report on the status of cybersecurity risk and inform organizational stakeholders, highlight the need to revisit other steps in the risk management process, and initiate new risk identification activities.

There are three key components to the Monitor phase:

1. Ensuring that risk treatment activities and status are up to date
2. Reporting of key risk indicators (KRIs) to the organization
3. Sponsoring new risk identification activities

5.1.3.1 Ensure that risk treatment activities and status are up to date

Authorized risk decision-makers are compelled to provide status updates for their risk treatment activities. This includes changes to implementation schedules, completion of risk treatment activities, and updates to original risk management decisions. If status updates for risk treatment activities are not provided by the authorized risk decision-maker, then the Cybersecurity Risk Management Working Group will actively solicit updates.

5.1.3.2 Reporting of key risk indicators (KRIs) to the organization

Keeping an agency's leadership and other stakeholders informed of cybersecurity risk is paramount. An enterprise-wide risk picture needs to be available to leadership for situational awareness, decision-making, funding and resource allocation. These risks will need to integrate with an agency's Enterprise Risk Management Program if one exists. If not, it is this reporting and feedback that will ensure that the agency's information systems and data are aligned with the risk tolerance of the organization.

Table 5 represents an example of what KRI reporting could look like at an agency.

TABLE 5
KRI Reporting Example

Agency Stakeholders	Frequency	Report Type
Board of directors	Biannually	• Level of inherent and residual risk • Serious risk that has been accepted • Number of new risks evaluated • Amount of risk reduced
Senior leadership team	Quarterly	• Level of inherent and residual risk • Serious risk that has been accepted • Number of new risks evaluated • Amount of risk reduced • Amount of risk "unmanaged"
Risk owners (AGMs)	Monthly	• Current level risk for respective business services • Number of new risks evaluated for respective business services • Amount of risk "unmanaged" for respective business services • Risk that has been accepted
Authorized risk decision-maker	Monthly	• Request status updates for risk treatment plans • Current risk status for all accountable risk

5.1.3.3 Sponsoring new risk identification activities

Monitoring organizational cybersecurity risk also entails ensuring that risk assessments are being completed for critical and important IT services; the risk cannot be managed if it has not been identified. As outlined in the "Assess risk" section of this plan, there are already many risk identification activities being performed as part of an agency's business processes, but the Cybersecurity Risk Management Working Group should also provide sponsorship for assessments if gaps in identified risk exist, or if there is a need to validate the effectiveness of in-place security controls.

These gaps can be identified by:

- Analyzing business impact analysis reports
- Performing cyberthreat modeling activities
- Leveraging institutional knowledge

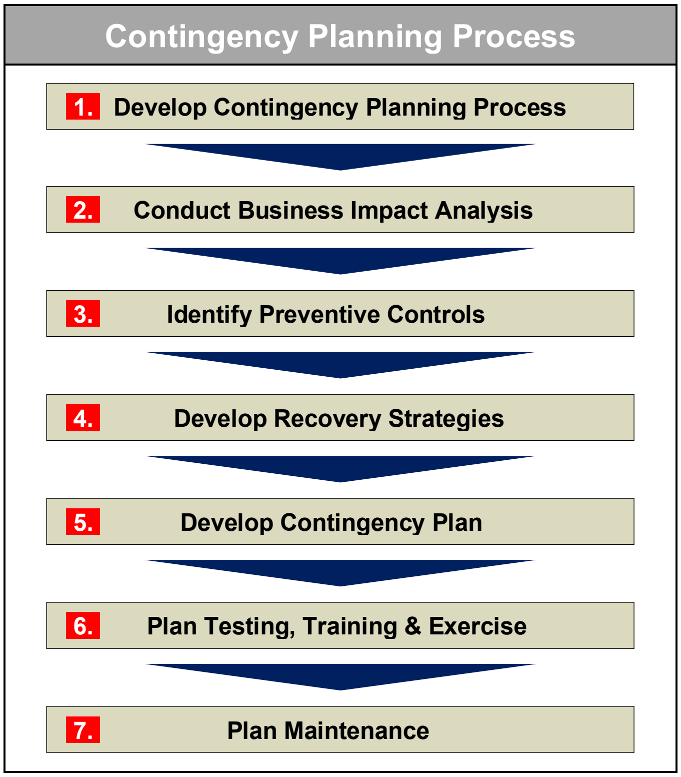
The performance of risk identification and control validation activities, such as risk assessments, penetration testing, and architecture and configuration reviews may be performed by any of the following:

- Internal resources
- External third-party private sector partners
- Department of Homeland Security

6. System contingency and resilience

System resilience is directly tied in with the transit agency's business continuity plan. It is essential for a transit agency, which thousands of customers are dependent on to provide uninterrupted service as expected. Resilience is the ability of a transit agency to mitigate disruptive services and quickly return to its original state after an incident. Transit agencies must identify and prioritize their vital services in all operating conditions through a thorough business impact analysis. Effective contingency planning includes incorporating security controls early in developing an information system and maintaining these controls on an ongoing basis. By following a simple seven-step process as outlined in NIST 800-100, "Seven-Step IT Contingency Planning Process" (summarized in **Figure 13**), transit agencies will have the ability to quickly identify a security incident and take appropriate steps to recover from such an incident.

FIGURE 13
Integration of Information Security in Risk Management


Contingency Planning Process
1. Develop Contingency Planning Process
2. Conduct Business Impact Analysis
3. Identify Preventive Controls
4. Develop Recovery Strategies
5. Develop Contingency Plan
6. Plan Testing, Training & Exercise
7. Plan Maintenance

Resilience, as defined by DHS, is the ability to quickly adapt and recover from any known or unknown changes to the environment. The goal of a resilient organization is to always continue mission-essential functions during any type of disruption. Resilient organizations continually work to adapt to changes and risks that can affect their ability to continue critical operations. Risk management, contingency and continuity planning are individual security and emergency management activities that can also be implemented holistically across an organization as components of a resilience program.

6.1 Types of plans

Information system contingency planning represents a broad scope of activities designed to sustain and recover critical system services following an emergency event. Information system contingency planning fits into a much more comprehensive security and emergency management effort that includes organizational and business process continuity, disaster recovery planning, and incident management. Ultimately, an organization would use a suite of plans to properly prepare response, recovery and continuity activities for disruptions affecting the organization's information systems, mission/business processes, personnel and facility. The following plans support the organization's contingency and resilience planning activities and should be considered in developing in an overall effort of creating a resilient organization against cybersecurity incidents:

- **Incident Response Plan:** This addresses the ability to proactively detect, contain, eradicate and recover from a security breach, such as malware or an active network penetration leaking a transit agency's confidential information. The Federal Information Security Management Act (FISMA) explicitly directs all federal agencies to develop and implement procedures for detecting, reporting and responding to security incidents. This practice will be helpful for all transit agencies at the state and local level to consider. The robustness of a transit agency's incident response will vary depending on its budget, size and capability. However, smaller transit agencies can implement basic practices while working with other agencies to foster a synergy of information sharing. All transit agencies should have some form of incident response.
- **Business Continuity Plan:** The BCP focuses on sustaining an organization's mission/business processes during and after a disruption. An example of a mission/business process may be an organization's payroll process or its customer service process. A BCP may be written for mission/business processes within a single business unit or may address the entire organization's processes. The BCP may also be scoped to address only the functions deemed to be priorities. A BCP may be used for long-term recovery in conjunction with the Continuity of Operations Plan, allowing for additional functions to come online as resources or time allow. Because mission/business processes use information systems, the business continuity planner must coordinate with information system owners to ensure that the BCP expectations and information system capabilities are matched.
- **Continuity of Operations Plan:** The COOP focuses on restoring an organization's mission-essential functions at an alternate site and performing those functions for up to 30 days before returning to normal operations. Additional functions, or those at a field office level, may be addressed by a BCP. Minor threats or disruptions that do not require relocation to an alternate site typically are not discussed in a COOP.
- **Crisis Communications Plan:** Organizations should document standard procedures for internal and external communications in the event of a disruption using a crisis communications plan. A crisis communications plan is often developed by the organization responsible for public outreach. The plan provides various formats for communications appropriate to the incident. The crisis communications plan typically designates specific individuals as the only authority for answering questions from or providing information to the public regarding emergency response. The plan may also include procedures for disseminating reports to personnel on the status of the incident and templates for public press releases.
- **Disaster Recovery Plan:** The DRP applies to major, usually physical disruptions to service that deny access to the primary facility infrastructure for an extended period. A DRP is an information system–focused plan designed to restore operability of the target system, application or computer facility infrastructure at an alternate site after an emergency. The DRP may be supported by multiple information system contingency plans to address the recovery of impacted individual systems once the alternate facility has been established. A DRP may support a BCP or a COOP by recovering supporting systems for mission/business processes or mission-essential functions at an alternate location. The DRP addresses only information system disruptions that require relocation.

7. Managing integrated cybersecurity risks

Organizations are increasingly concerned about the risks associated with IT products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the cyber supply chain. These risks are associated with an enterprise's decreased visibility into, and understanding of, how the technology they acquire is developed, integrated and deployed, as well as the processes, procedures and practices used to ensure the security, resilience, reliability, safety, integrity and quality of the products and services.

With fast-paced advancement of ICT technology, an organizational capability of identifying, developing, implementing and retiring ICT equipment will be vital to achieve the most current and highest level of security protection. A critical function of a transit agency's IT security is the acquisition process. The acquisition process is not only about the procurement of information technology equipment to fulfill the direct immediate needs of the organization, but it also must encompass security throughout the whole process.

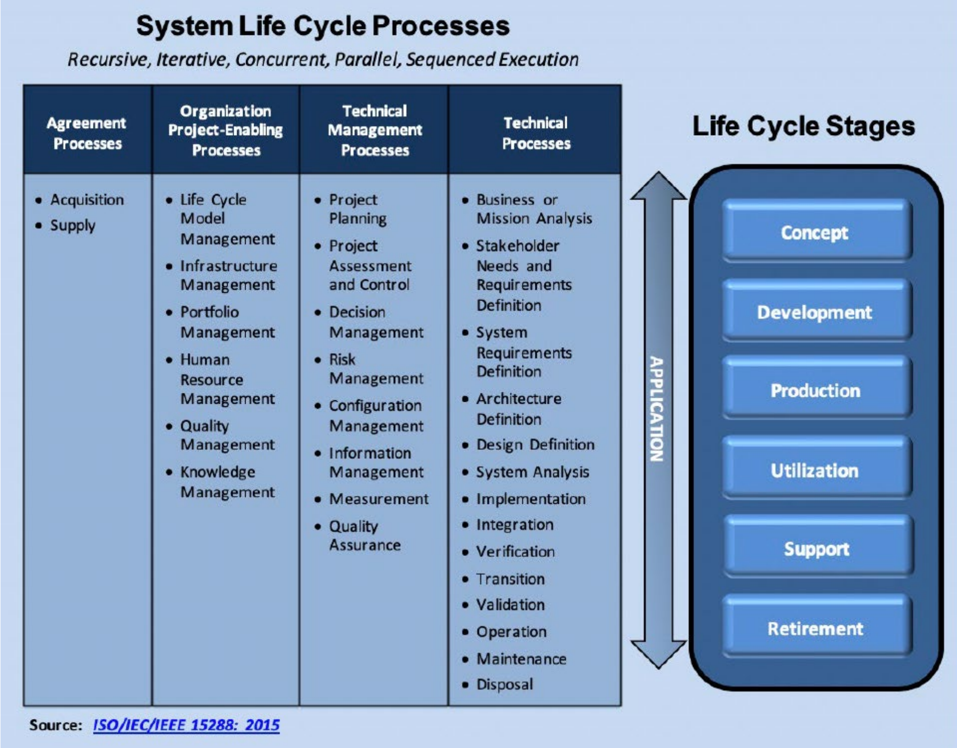
Every phase of procurement needs to meet and be vetted through a set of minimal security requirements defined by the agency and complying with any federal, state and local mandates.

The overall resilience of a transit agency's information systems (i.e., how well systems operate while under stress) is a key factor and performance measure in determining the potential survivability of missions/business functions. The use of certain information technologies may introduce inherent vulnerabilities into these information systems, resulting in risk that may have to be mitigated by reengineering the current mission/business processes. The wise use of information technologies during the design, development and implementation of organizational information systems is of paramount importance in managing risk.

7.1 Systems development life cycle (SDLC)

Security by design should be built into the SDLC and should cover every stage from cradle to grave of the IT systems and services. This holistic SCLC approach helps ensure that appropriate cybersecurity considerations are built into each life stage. **Figure 14**, from NIST SP 800-160 in Volume 2, shows this model.

FIGURE 14
System Life Cycle Processes

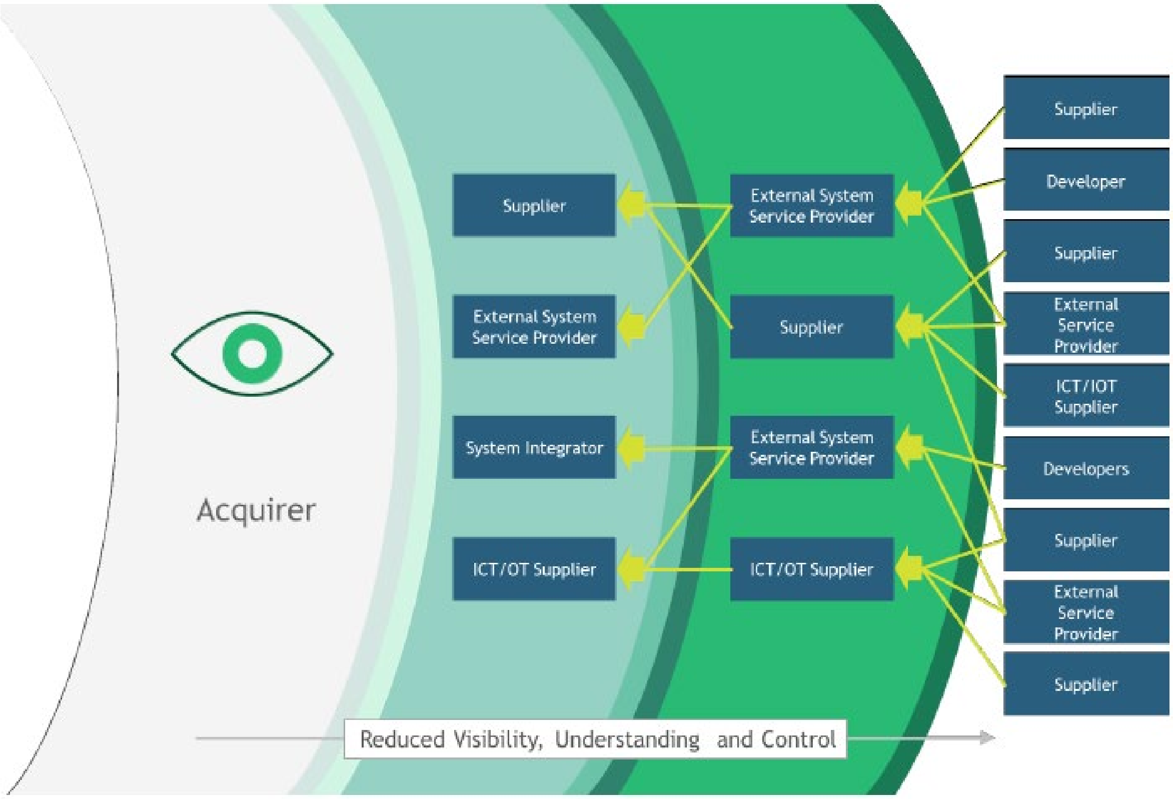

System Life Cycle Processes
Recursive, Iterative, Concurrent, Parallel, Sequenced Execution

Agreement Processes	Organization Project-Enabling Processes	Technical Management Processes	Technical Processes
• Acquisition • Supply	• Life Cycle Model Management • Infrastructure Management • Portfolio Management • Human Resource Management • Quality Management • Knowledge Management	• Project Planning • Project Assessment and Control • Decision Management • Risk Management • Configuration Management • Information Management • Measurement • Quality Assurance	• Business or Mission Analysis • Stakeholder Needs and Requirements Definition • System Requirements Definition • Architecture Definition • Design Definition • System Analysis • Implementation • Integration • Verification • Transition • Validation • Operation • Maintenance • Disposal

Source: ISO/IEC/IEEE 15288: 2015

An organization's visibility, understanding and control of its cyber supply chain is critical to properly manage the cybersecurity risks. The complexity of the supply chain and related cybersecurity is best captured by **Figure 15**, taken from NIST SP 800-161, which is viewed from the perspective of the "acquirer" with many downstream risks related to suppliers and developers of the IT systems and services that may be several layers deeper than the party the agency is contracting with.

FIGURE 15
Supply Chain Complexity


Acquirer
Supplier
External System Service Provider
System Integrator
ICT/OT Supplier
External System Service Provider
Supplier
External System Service Provider
ICT/OT Supplier
Supplier
Developer
Supplier
External Service Provider
ICT/IOT Supplier
Developers
Supplier
External Service Provider
Supplier
Reduced Visibility, Understanding and Control

By utilizing the SDLC process, transit agencies can more effectively manage their ICT systems. Many SDLC models have been developed, but they generally cover five major phases: initiation, development/acquisition, implementation, operations/maintenance and disposal. With the goal of maintaining information security through maintaining confidentiality, preserving integrity and sustaining availability, transit agencies must integrate security in each phases of the SDLC. Utilizing security activities outlined within each phase developed by NIST SP 800-100, transit agencies will have a broad understanding of the security activities necessary within the SDLC process. The following are the key security activities for each phase:

1. **Initiation**
    - Initial delineation of business requirements in terms of confidentiality, integrity and availability.
    - Determination of information categorization and identification of known special handling requirements to transmit, store or create information such as personally identifiable information.
    - Determination of any privacy requirements.

2. **Development/acquisition**
    - Conduct the risk assessment and use the results to supplement the baseline security controls.
    - Analyze security requirements.
    - Perform functional and security testing.
    - Prepare initial documents for system certification and accreditation.
    - Design security architecture.
3. **Implementation**
    - Integrate the information system into its environment.
    - Plan and conduct system certification activities in synchronization with testing of security controls.
    - Complete system accreditation activities.
4. **Operations/maintenance**
    - Conduct an operational readiness review.
    - Manage the configuration of the system.
    - Institute processes and procedures to ensure operations and continuous monitoring of the information system's security controls.
    - Perform reauthorization as required.
5. **Disposal**
    - Build and execute a disposal/transition plan.
    - Archive critical information.
    - Sanitize media.
    - Dispose of hardware and software.

7.2 Managed security service provider (MSSP)[2]

A managed security service provider (MSSP) provides outsourced monitoring and management of security devices and systems. Common services include managed firewall, intrusion detection, virtual private network, vulnerability scanning and antiviral services. MSSPs use high-availability security operation centers (either from their own facilities or from other data center providers) to provide 24/7 services designed to reduce the number of operational security personnel an enterprise needs to hire, train and retain to maintain an acceptable security posture.

The following sections describe some of the benefits of using an MSSP in detail.[3]

7.2.1 Minimize costs and maximize efficiency

An MSSP offers a team of seasoned security experts that will work for an agency at a fraction of the cost of building a security team in-house.

7.2.2 Extend a team

A global MSSP offers a unique advantage. With a global footprint, an agency will be better positioned for continued operations wherever or whenever it needs it through an MSSP's global security operation centers. These SOCs offer the latest threat intelligence and visibility into advanced threats where a smaller or regional provider cannot.

[2] https://www.gartner.com/en/information-technology/glossary/mssp-managed-security-service-provider
[3] Adapted from https://cipher.com/blog/10-managed-security-services-benefits-to-know/

7.2.3 Become a threat-hunting organization

An MSSP offers advanced monitoring, analysis and investigation of malicious code and callbacks, detecting attempted or successful security breaches. The SOC ensures best-in-class defense, real-time incident response and operational optimization. An MSSP uses threat monitoring to go beyond the network to become a threat-hunting organization and stop threats before they even hit the network.

7.2.4 Rapid incident response and event investigation

An MSSP can provide incident response and event investigation services, as well as experience in handling enterprise security incidents. This prevents further harm to the organization, ranging from single-system compromises to enterprise-wide intrusions by advanced attack groups. An MSSP's incident response team will quickly assess the challenges the agency faces and recommend specific actions using digital forensics.

7.2.5 SIEM and log management insights

An enterprise generates relevant data about its security posture across multiple locations. An MSSP can analyze all the data from a single point of view. This makes it easier to identify trends and patterns that are out of the ordinary. That is the job of a security information and event management system. An MSSP will use the SIEM system to collect logs and other security-related documentation for analysis on a single platform. It can use this information to correlate an agency's data against a database of threat intelligence feeds and proactively identify any malicious activity.

7.2.6 Security asset management relief

Organizations often purchase new IT security solutions, only to let them sit on the shelf due to lack of skilled staff or project priority. An MSSP partner can offer the necessary skills and technical resources a team needs to manage and administer these new security assets. The MSSP will take a holistic view of a security environment and understand the specific requirements of how to integrate the new security assets with the latest patches, configuration changes and security policy changes.

7.2.7 Closely monitor advanced threats

Small and midsized enterprise organizations face an increasing complexity and sophistication of cyberthreats, such as advanced persistent threats, advanced malware (Trojans, viruses, and worms), and other malicious attacks. An MSSP partner can provide sophisticated security technologies and the latest threat intelligence to provide monitoring and detecting against these serious, growing threats. An MSSP can get an active threat protection program up and running quickly while minimizing costs and maximizing security.

7.2.8 Automate vulnerability risk management

Ongoing vulnerability scans are a critical element for a successful security posture. An MSSP partner can provide accurate internal and external scans across the IT and IT/OT environment, network assets, hosts, web applications and databases. Vulnerability scans by an MSSP will reduce the resource needs through a structured distributed deployment. This reduces IT operational cost. If appropriate and approved, the MSSP can offer configuration changes, patches, vulnerabilities, hardening and policy compliance of IT assets, devices and applications, with interactive dashboards and informative reports.

7.2.9 Properly manage risk and compliance

It's critical to monitor an agency's cybersecurity maturity compliance level for regulatory purposes. A highly certified MSSP will extend its risk management and compliance expertise and certification to an organization and ensure its assets are protected. A benefit of using an MSSP is having the expertise of its risk management and compliance programs.

7.2.10 Obtain best-in-class intelligence

The best MSSPs offer real-time threat intelligence technology to identify advanced malware attacks, persistent threats and malicious attacks. MSSPs invest millions of dollars into detecting and analyzing global threats using threat intelligence inside a real intelligence laboratory. Adding an MSSP partner allows an agency's security personnel to focus on strategic security projects while the MSSP focuses on the tactical threat hunting and monitoring capabilities.

7.3 Information security services and products

Information security services and products are essential elements of any organization's information security program. Many products and services to support an agency's information security program for information systems are widely available in the marketplace today.

Security products and services should be selected, used and integrated into a transit agency's information security program to manage, develop and protect information, and to maintain information security infrastructure. The acquisition process of security services and products should include risk management activities to identify and mitigate specific risks associated with such acquisition.

Transit agencies should weigh savings gained by outsourcing specific services against the risks connected to placing data and transactions outside their control and management. The importance of systematically managing the process for the acquisition of information security services cannot be underestimated because of the potential impact associated with those risks.

Before selecting specific services, organizations should review the status of their security programs and the security controls that are either planned or in place to protect information systems and data.

Agencies should use the risk management process to identify a compelling mix of management, operational and technical security controls that will mitigate risk to an acceptable level. The number and type of appropriate security controls and related information security services may vary throughout a particular system's services life cycle.

8. Standards, resources and tools

APTA has identified industry standards, resources and tools for transit agencies to utilize and reference in developing specific information security programs tailored to individual agencies. These references are not exhaustive and are meant only to serve as a guide.

8.1 National Institute of Standards and Technology (NIST)

NIST is a non-regulatory U.S. federal agency responsible for developing standards and guidelines, including minimum requirements, and for providing adequate information security for all agency operations and assets. The SP 800 series provides guidance, description, details and standards in establishing and implementing information security programs. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life.

In 2014, NIST released Version 1.0 of the Cybersecurity Framework (https://www.nist.gov/cyberframework) to help organizations charged with providing the nation's financial, energy, healthcare and other critical systems better protect their information and physical assets from cyberattack. The framework provides a structure that organizations, regulators and customers can use to create, guide, assess or improve comprehensive cybersecurity programs.

Additionally, transit agencies should consider utilizing the Cyber Security Evaluation Tool (CSET®) from the Department of Homeland Security. It is a tool that assists organizations in protecting their key cyber assets. This tool provides a systematic and repeatable approach for assessing the security posture of digital systems and networks. It includes both high-level and detailed questions related to all industrial control and IT systems.

8.2 National Initiative for Cybersecurity Education (NICE)

NICE has evolved from the Comprehensive National Cybersecurity Initiative and extends its scope beyond the federal workplace to include civilians and students in kindergarten through postgraduate school. The goal of NICE is to establish an operational, sustainable and continually improving cybersecurity education program encouraging sound cybersecurity practices that will enhance the nation's security. NICE will be represented by four components:

- **Component 1:** National Cybersecurity Awareness. Lead: DHS
- **Component 2:** Formal Cybersecurity Education. Co-Leads: Department of Education and National Science Foundation
- **Component 3:** Cybersecurity Workforce Structure. Lead: DHS, supported by the Office of Personnel Management
- **Component 4:** Cybersecurity Workforce Training and Professional Development. Tri-Leads: Department of Defense, Office of the Director of National Intelligence and DHS.

8.3 International Organization for Standardization (ISO)

ISO is the world's largest developer of voluntary international standards. International standards give state-of-the-art specifications for products, services and good practice, helping to make industry more efficient and effective. Developed through global consensus, they help to break down barriers to international trade.

The following standards apply to cybersecurity:

- **ISO/IEC 13335:** Information Technology Guidelines for the Management of IT Security
- **ISO/IEC 17799:** Code of Practice for Information Security Management
- **ISO/IEC 27001:** Information Security Management Systems – Requirements
- **ISO/IEC 27005:** Information Security Risk Management
- **ISO/IEC 31000:** Risk Management Principles and Guidelines
- **ISO/IEC 31010:** Risk Management Risk Assessment Techniques
- **ISO/IEC 15408:** Common Criteria for Information Technology Security Evaluation

8.4 APTA standards and guidance

The Control and Communications Cyber Security Work Group develops APTA standards for rail system control and communications security. The Control and Communications Security Work Group that began its work in 2007 published Part I of the APTA recommended practice "Securing Control and Communications Systems in Transit Environments" in 2010 (APTA-SS-CCS-RP-001-10). Part I is an introductory guide for transit agency cybersecurity and is focused on general principles such as describing transit system networks, organizing a cybersecurity program and performing a cybersecurity risk assessment. Part I is limited in its cybersecurity scope, and it does not address the specific use of cybersecurity technologies for prevention of attacks once cybersecurity risks are identified. Part II (APTA-SS-CCS-RP-002-13) focuses on defining and applying security controls applied to high-risk/consequence and vital systems (safety-critical signaling systems, etc.) and medium-risk/consequence systems (SCADA such as traction power systems, etc.), while laying out these security controls in the context of a transit agency security plan.

Additional guidance is available from "Ten Basic Cybersecurity Measures, Public Transportation Industry, Reducing Exploitable Weaknesses and Attacks in Communication and Control," which provides transportation cybersecurity officials, transportation agency general managers and other related stakeholder groups basic guidance and proactive steps for reducing vulnerability to a cyberattack. This document is available on HSIN-PT and on APTA's Safety & Security Resource page as an excellent resource for beginners and experts in cybersecurity.

8.5 Federal Information Security Management Act (FISMA)

FISMA is a U.S. federal law that recognizes the importance of information security to the economic and national security interests of the United States. FISMA has brought attention within the federal government to cybersecurity and emphasized a "risk-based policy for cost-effective security." FISMA requires agency program officials to conduct annual reviews of the agency's information security program and report the results to the Office of Management and Budget. The OMB uses this data to assist in its oversight responsibilities and to prepare its annual report to Congress on agency compliance with the act.

8.6 U.S. Computer Emergency Response Team (US-CERT)

The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) leads efforts to improve the nation's cybersecurity posture, coordinate information sharing, and proactively manage threats to the nation while protecting the constitutional rights of Americans. US-CERT strives to be a trusted global leader in cybersecurity: collaborative, agile and responsive in a dynamic and complex environment. US-CERT provides the following tools and resources:

- **National Vulnerability Database:** The NVD is the U.S. government repository of standards- based vulnerability management data represented using the Security Content Automation Protocol. This data enables automation of vulnerability management, security measurement and compliance.
- **Vulnerability Notes:** Vulnerability Notes contain information about vulnerabilities and include summaries, technical details, remediation information and lists of affected vendors.
- **Vulnerability Card Catalog:** Authorized users can log into the Vulnerability Card Catalog to access information regarding emerging vulnerabilities reported to the CERT Coordination Center.
- **US-CERT Portal:** The US-CERT Portal provides a secure, web-based, collaborative system to share sensitive, cybersecurity-related information and news with participants in the public and private sector, including GFIRST, the CISO Forum, NCRCG, ISAC members, and various other working groups. Authorized users can visit the US-CERT Portal.
- **US-CERT Einstein Program:** This program provides an automated process for collecting, correlating, analyzing and sharing computer security information across the federal government to improve national situational awareness.
- **Security Configuration Benchmarks and Scoring Tools:** The Center for Internet Security (CIS) has security configuration benchmarks and scoring tools, many of which can be downloaded free of charge.

8.7 Federal Information Processing Standard (FIPS)

A Federal Information Processing Standard is a publicly announced standardization developed by the U.S. federal government for use in computer systems by all non-military government agencies and by government contractors, when properly invoked and tailored on a contract. Many FIPS pronouncements are modified versions of standards used in the technical communities, such as the American National Standards Institute, the Institute of Electrical and Electronics Engineers, and the International Organization for Standardization (ISO).

8.8 SANS Institute

The SANS Institute was established as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world. A ranges of individuals, from auditors and network administrators to chief information security officers, are sharing the lessons they learn and are jointly finding solutions to the challenges they face. At the heart of SANS are the many security practitioners in varied global organizations from corporations to universities working together to help the entire information security community.

SANS has developed the Top 20 CIS Critical Security Controls for effective cyberdefense. The CIS Critical Security Controls are a recommended set of actions for cyberdefense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks. A principal benefit of the controls is that they prioritize and focus a smaller number of actions with high-payoff results.

8.9 Academia and Stanford's Minimum-Security Standards

Academia is a great source of free and practical guidance on how to improve cybersecurity, and organizations typically disclose which software solutions/tools and methodologies they are using to secure their systems. Stanford University is one of the leaders that provides excellent resources and guidance on how to protect IT assets. One of its thought leadership pieces is the development of what's called the Minimum Security Standards that all devices that connect to its networks must meet. These standards are intended to reflect the minimum level of care necessary for Stanford's sensitive data and are not intended to relieve Stanford or its employees, partners, consultants or vendors of further obligations that may be imposed by law, regulation or contract.

Other valuable resources from government and academia are as follows:

- CISA Cybersecurity Resources: https://www.cisa.gov/cisa-cybersecurity-resources
- EDUCAUSE Cybersecurity Program: https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program

Related APTA standards

APTA-SS-CCS-RP-001-10, "Securing Control and Communications Systems in Transit Environments, Part I"

APTA-SS-CCS-RP-002-13, "Securing Control and Communications Systems in Transit Environments, Part II"

References

Accenture. "All aboard! How hackers are moving in on the transit sector." June 2020. https://www.accenture.com/us-en/blogs/cyber-defense/hackers-moving-in-on-transit-sector

Cybersecurity & Infrastructure Security Agency. "Ransomware Guidance and Resources." https://www.cisa.gov/ransomware

Cybersecurity & Infrastructure Security Agency. "Ransomware Guide," September 2020. https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

Department of Homeland Security, "Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise," November 2011. https://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf

Executive Office of the President National Science and Technology Council, "Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program," December 2011. https://www.nitrd.gov/pubs/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf

International Organization for Standardization, ISO/IEC 13335:2004, Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management.

International Organization for Standardization, ISO/IEC TR 13335-3:1998, Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security outlines techniques and procedures to assist in IT security management and implementation.

International Organization for Standardization, ISO/IEC TR 13335-4:2000, Information technology – Guidelines for the management of IT Security – Part 4: Selection of safeguards provides guidance on selecting safeguards that consider organization-specific needs and concerns.

International Organization for Standardization, ISO/IEC TR 13335-5:2001, Information technology – Guidelines for the management of IT Security – Part 5: Management guidance on network security helps to identify and analyze communications-related factors when establishing network security requirements.

International Organization for Standardization, ISO/IEC 17799, Information technology – Code of Practice for Information Security Management.

International Organization for Standardization, ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements, is a certification standard intended to be used with ISO/IEC 17799.

National Institute of Standards and Technology, Information Technology Laboratory. Software Supply Chain. "Improving the Nation's Cybersecurity: NIST's Responsibilities under the Executive Order." https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity

National Institute of Standards and Technology, Special Publication 800 Series. http://csrc.nist.gov/publications/PubsSPs.html:
SP 800-30, "Risk Management Guide for Information Technology Systems," July 2002.
SP 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems," May 2004.
SP 800-64, "Security Considerations in the Information System Development Life Cycle," October 2003.
SP 800-18, Revision 1, "Guide for Developing Security Plans for Federal Information Systems," February 2006.
SP 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," February 2010.
SP 800-39, "Managing Information Security Risk: Organization, Mission, and Information System View," March 2011.
SP 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations," August 2009.
SP 800-53A, Revision 1, "Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans," June 2010.
SP 800-59, "Guideline for Identifying an Information System as a National Security System," August 2003.
SP 800-60, Revision 1, "Guide for Mapping Types of Information and Information Systems to Security Categories," August 2008.
SP 800-39, "Managing Risk from Information Systems: An Organizational Perspective," April 2008.
SP 800-70, Revision 2, "National Checklist Program for IT Products – Guidelines for Checklist Users and Developers," February 2011.
SP 800-137 (Initial Public Draft), "Information Security Continuous Monitoring for Federal Information Systems and Organizations," December 2010.
SP 800-55, "Security Metrics Guide for Information Technology Systems," July 2003.

NIST Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004.

NIST Federal Information Processing Standards Publication 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006.

NIST ITL Bulletin: Selecting Information Technology Security Products, April 2004. http://csrc.nist.gov/publications/nistbul/04-2004.pdf

NIST ITL Bulletin: "Information Technology Security Services; How to Select, Implement, and Manage," June 2004. http://csrc.nist.gov/publications/nistbul/b-06-04.pdf

SANS Institute, "8 Simple Rules for Securing your Internal Network," September 2003. https://sansorg.egnyte.com/dl/e75uF2TVm6

SANS Institute, "The Internal Threat to Security Or Users Can Really Mess Things Up," September 2003. https://sansorg.egnyte.com/dl/Rm2nDJ9ogg

SANS Institute, "Federal Information Technology Management and Security," September 2003. www.sans.org/reading_room/whitepapers/bestprac/federal-information-technology-management-security_1190

SANS Institute, "A Guide to Government Security Mandates," December 2002. https://sansorg.egnyte.com/dl/4KJOvJ3DoS

US-CERT, "Recovering from a Trojan Horse or Virus," 2008. https://us-cert.cisa.gov/sites/default/files/publications/trojan-recovery.pdf

US-CERT, "Introduction to Information Security," 2008. https://us-cert.cisa.gov/sites/default/files/publications/infosecuritybasics.pdf

US-CERT, Technical Information Paper-TIP-11-075-01, "System Integrity Best Practices," March 2011. http://cryptome.org/0003/rsa-apt-wand.pdf

U.S. Department of Transportation, Enterprise Architecture and Business Transformation Office, "Enterprise Transition Plan," June 2009. www.dot.gov/cio/docs/ETS_FY2009.pdf

U.S. Government Accountability Office (GAO), "National Cybersecurity Strategy: Key Improvements are Needed to Strengthen the Nation's Posture," testimony before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives, March 2009. https://www.gao.gov/products/gao-09-432t

Definitions

enterprise cybersecurity: The body of technologies, processes and practices designed to protect business and IT networks, computers, programs and data from threats, attacks, damage or unauthorized access.

information security (INFOSEC): The protection of information assets to achieve confidentiality, integrity and availability.

intrusion detection monitoring: Network or system activities to detect unauthorized or malicious activities or policy violations.

penetration testing (or pen testing): A method of testing, measuring and enhancing established security measures on information systems and support areas. Pen testing is part of the overall IT security assessment.

secure cloud: The set of procedures, processes and standards designed to provide information security assurance in a cloud computing environment.

Abbreviations and acronyms

BCP	Business Continuity Plan
CIS	Center for Internet Security
CISO	chief information security officer
CIO	chief information officer
COOP	Continuity of Operations Plan
CSIRT	Cybersecurity Incident Response Team
CSP	cloud service provider
DHS	Department of Homeland Security
DOD	Department of Defense

DOE	Department of Education
DOT	Department of Transportation
DRP	Disaster Recovery Plan
EIS	enterprise information system
FIPS	Federal Information Processing Standard
GAO	Government Accountability Office
FISMA	Federal Information Security Management Act
GFIRST	Government Forum of Incident Response and Security Teams
GUI	graphical user interface
HVAC	heating, ventilation, air conditioning
ICT	information and communications technology
IEC	International Electrotechnical Commission
INFOSEC	information security
ISAC	Information Sharing & Analysis Center
IT	information technology
ITL	Information Technology Laboratory (NIST)
ISO	International Organization for Standardization
MSP	managed service provider
NCRCG	National Cyber Response Coordination Group
NSF	National Science Foundation
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OEM	original equipment manufacturer
PBX	Private Branch Exchange
SANS	Sys Admin, Audit, Networking and Security
SCADA	supervisory control and data acquisition
SDLC	system development life cycle
SSL	secure socket layer
SP	(NIST) Special Publication
TI	transportation information
TSA	Transportation Security Administration
US-CERT	United States Computer Emergency Readiness Team

Summary of document changes

- Bullet points xx

Document history

Document Version	Working Group Vote	Public Comment/ Technical Oversight	Rail CEO Approval	Policy & Planning Approval	Publish Date
First published	—	—	—	—	Oct. 17, 2014
First revision	Aug. 27, 2021	Jan. 7, 2022	Mar. 4, 2022	June 22, 2022	July 29, 2022