

Cybersecurity Resilience Assessment Tool to Enhance Public Confidence in Transit

PREPARED BY

Michael Echols
Max Cybersecurity

Brandon Thomas, Kathryn Seckman,
Scott Belcher
Grayline Group

On behalf of Rock Island County Metropolitan
Mass Transit District (MetroLINK)



U.S. Department of Transportation
Federal Transit Administration



AUGUST

20
23

COVER PHOTO

Courtesy of Sawyer Bengtson, unsplash.com

DISCLAIMER

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof. The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report. The opinions and/or recommendations expressed herein do not necessarily reflect those of the U.S. Department of Transportation.

Cybersecurity Resilience Assessment Tool to Enhance Public Confidence in Transit

AUGUST 2023

FTA Report No. 0250

PREPARED BY

Michael Echols
Max Cybersecurity
1875 K Street NW, Suite 400
Washington, DC 20006

Brandon Thomas, Kathryn Seckman, Scott Belcher
Grayline Group
P.O. Box 160314
Austin, TX 78716

On behalf of Rock Island County Metropolitan
Mass Transit District (MetroLINK)

SPONSORED BY

Federal Transit Administration
Office of Research, Demonstration and Innovation
U.S. Department of Transportation
1200 New Jersey Avenue, SE
Washington, DC 20590

AVAILABLE ONLINE

<https://www.transit.dot.gov/about/research-innovation>

Metric Conversion Table

SYMBOL	WHEN YOU KNOW	MULTIPLY BY	TO FIND	SYMBOL
LENGTH				
in	inches	25.4	millimeters	mm
ft	feet	0.305	meters	m
yd	yards	0.914	meters	m
mi	miles	1.61	kilometers	km
VOLUME				
fl oz	fluid ounces	29.57	milliliters	mL
gal	gallons	3.785	liters	L
ft³	cubic feet	0.028	cubic meters	m ³
yd³	cubic yards	0.765	cubic meters	m ³
NOTE: volumes greater than 1000 L shall be shown in m ³				
MASS				
oz	ounces	28.35	grams	g
lb	pounds	0.454	kilograms	kg
T	short tons (2000 lb)	0.907	megagrams (or "metric ton")	Mg (or "t")
TEMPERATURE (exact degrees)				
°F	Fahrenheit	5 (F-32)/9 or (F-32)/1.8	Celsius	°C

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE August 2023		2. REPORT TYPE Final		3. DATES COVERED June 2021 – June 2022	
4. TITLE AND SUBTITLE Cybersecurity Resilience Assessment Tool to Enhance Public Confidence in Transit				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Michael Echols (Max Cybersecurity), Brandon Thomas (Grayline Group), Kathryn Seckman, (Grayline Group), Scott Belcher (Grayline Group)				5d. PROGRAM NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Max Cybersecurity 1875 K Street NW, Suite 400, Washington, DC 20006 Grayline Group P.O. Box 160314, Austin, TX 78716 Rock Island County Metropolitan Mass Transit District (MetroLINK)				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Department of Transportation Federal Transit Administration Office of Research, Demonstration and Innovation 1200 New Jersey Avenue, SE, Washington, DC 20590				10. SPONSOR/MONITOR'S ACRONYM(S) FTA	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S) FTA Report No. 0250	
12. DISTRIBUTION/AVAILABILITY STATEMENT Available from: National Technical Information Service (NTIS), Springfield, VA 22161; (703) 605-6000, Fax (703) 605-6900, email [orders@ntis.gov]; Distribution Code TRI-30					
13. SUPPLEMENTARY NOTES [www.transit.dot.gov/research-innovation/fta-reports-and-publications] [https://www.transit.dot.gov/about/research-innovation] [https://doi.org/10.21949/1527663] Suggested citation: Federal Transit Administration. Cybersecurity Resilience Assessment Tool to Enhance Public Confidence in Transit. Washington, D.C.: United States Department of Transportation, 2023. https://doi.org/10.21949/1527663 .					
14. ABSTRACT In 2021, the Federal Transit Administration (FTA) awarded the Rock Island County Metropolitan Mass Transit District (MetroLINK) a grant to develop a cybersecurity assessment tool to assess its cyber posture as part of FTA's Public Transportation COVID-19 Research Demonstration Grant Program. The Cybersecurity Assessment Tool for Transit (CATT) and supporting documents were developed to assist MetroLINK and other small and mid-sized transit agencies in assessing their cyber preparedness and resilience. CATT is designed specifically for the cybersecurity needs of small to mid-sized public transit agencies. The goal of the tool is to onboard public transit organizations to develop and strengthen their cybersecurity program to identify risks and prioritize activities to mitigate them. The COVID-19 pandemic forced agencies to change how they operated, bringing in new technologies to manage critical operations and to facilitate remote work, many of which exponentially increased the number of threat vectors. In parallel, cyberattacks and network intrusions continue to proliferate. Recent incidents demonstrate that even small and mid-sized transit agencies are vulnerable to system disruptions due to cyberattacks. Prior to this project, no cybersecurity assessment tools had been developed specifically for the unique context and conditions faced by transit agencies.					
15. SUBJECT TERMS Cybersecurity, Assessment, COVID-19					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Unlimited	18. NUMBER OF PAGES 106	19a. NAME OF RESPONSIBLE PERSON
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER

TABLE OF CONTENTS

1	Executive Summary
5	Section 1 Introduction
17	Section 2 The Transit Cyber Environment
24	Section 3 Assessment Best Practices
40	Section 4 Gap Analysis
46	Section 5 Cybersecurity Resilience Review
49	Section 6 Enhancing the CRR
58	Section 7 Summary and Findings
59	Appendix A Understanding the NIST System
61	Appendix B Cyber Resources for Transit
63	Appendix C Set of Cyber Assessment Tools Reviewed
64	Appendix D Cybersecurity Assessment Tool for Transit (CATT) Security Assessment Report <i>Note: Certain figures in Appendix D reference “STAAT”, an early acronym used by the project team to reference the CATT tool. When used in figures, STAAT is also a reference to CATT.</i>
94	Appendix E Cybersecurity Assessment Tool for Transit (CATT) Project Team Response to the Independent Evaluation

LIST OF FIGURES

- 21 **Figure 2-1** Comparison of IT and ICS
- 30 **Figure 3-1** NIST System Development Life Cycle
- 48 **Figure 5-1** Cyber assessment: Cyber Resilience Review (CRR) domains

LIST OF TABLES

- 33 **Table 3-1** Potential Impact Definitions for Security Objectives

Forward



Transit Leaders -

Security and safety are always top of mind for all of us as we deliver on our mission. For decades, we have effectively invested in resources, operations, and talent to reduce the physical risks faced by operations. However, as we employ advances in technology, the means by which we go about reducing risks to our ridership and our team is evolving. Technology is no longer a support function; it has become a critical component of our operations. In parallel to the advance of technology, cybersecurity has been moved front and center to ensuring our operations are secure.

The above was exacerbated by the pandemic, as we all moved to remote operations within weeks. Our operations were stressed by the need to quickly and securely implement remote access to our systems and software. Decisions were made to ensure operations persisted, but no doubt new risks were introduced.

Some transit agencies have invested more than others in developing their cybersecurity programs. Services and tools abound from public and private organizations to assist. As a smaller agency, however, we have struggled with the breadth and complexity of resources available. It has been difficult to figure out where to start, or what to do next.

To help address this shift in risk with a focus on small and mid-sized agencies, MetroLINK, in cooperation with Max Cybersecurity and the Grayline Group, secured funds from the Federal Transit Administration's COVID-19 Research Demonstration Grant Program to address this challenge. We have developed a self-assessment tool that reduces the complexity and is focused on the needs of small and mid-sized public transit agencies. The tool is approachable, understandable, and immediately usable to assess and help map out where we go from here to improve our cybersecurity posture.

I am excited for the future of public transit. Technology is enabling us to make our operations better, more effective, and more efficient. Ensuring we also secure our systems given these new technologies is critical. I am pleased to offer this tool to the industry to support the continued investment in technology to further deliver on the mission of public transit. Thank you.

Jeff Nelson
CEO, MetroLINK
Chairman, American Public Transportation Association, 2022

Acknowledgments

The project team would like to thank the MetroLINK team for their incredible support through this process, in particular Jeff N lson and Chelsey Waterman. In addition, the project team would like to thank:

Polly Hanson
American Public Transportation Association (APTA)

David Schneider
Federal Transit Administration (FTA)

Cara Marcus
National Rural Transit Assistance Program (NRTAP)

Nancy Pomerleau
Cybersecurity and Infrastructure Security Agency (CISA)

Carnegie Mellon University

Marcela Moreno
National Center for Applied Transit Technology (N-CATT)

Greg Meldrum
MetroLINK

Anthony Candarini
AECOM

Tim Coogan
RTD Denver

Abstract

In 2021, the Federal Transit Administration (FTA) awarded the Rock Island County Metropolitan Mass Transit District (MetroLINK) a grant to develop a cybersecurity assessment tool to assess its cyber posture as part of FTA's Public Transportation COVID-19 Research Demonstration Grant Program. The Cybersecurity Assessment Tool for Transit (CATT) and supporting documents were developed to assist MetroLINK and other small and mid-sized transit agencies in assessing their cyber preparedness and resilience. CATT is designed specifically for the cybersecurity needs of small to mid-sized public transit agencies. The goal of the tool is to support and encourage public transit organizations to develop and strengthen their cybersecurity program to identify risks and prioritize activities to mitigate them.

The COVID-19 pandemic forced agencies to change how they operate, bringing in new technologies to manage critical operations and to facilitate remote work, many of which exponentially increased the number of threat vectors. In parallel, cyberattacks and network intrusions continued to proliferate. Recent incidents demonstrate that transit agencies of all sizes, including small and mid-sized transit agencies, are vulnerable to system disruptions due to cyberattacks. Prior to this project, no cybersecurity assessment tools had been developed specifically for the unique context and conditions faced by transit agencies.

Executive Summary

In 2020, the Mineta Transportation Institute (MTI) released an important cybersecurity study, *Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness*.¹ After surveying more than a third of the American Public Transportation Association's (APTA) public transit members, the researchers concluded that the industry is not prepared for the growing cyber threat. The MTI study found that most transit agencies do not have the basic policies or personnel in place to respond to a cyber incident.

Since the study's publication, the situation has only increased in complexity. Several large-scale incidents have occurred among public transit agencies. In parallel, new technologies and capabilities have been deployed, both improving the delivery of transit services while also introducing additional security risks. The emergence of the Coronavirus Disease 2019 (COVID-19) highlighted these vulnerabilities and exacerbated the cyber security challenges with which transit agencies had to deal.

The COVID-19 pandemic forced transit entities to quickly adapt to meet operational challenges including the security of cyber assets, systems, and networks. As system upgrades and agency operations continued remotely, information and operational technology risks increased exponentially, further aggravating challenged cybersecurity operations.

The project is designed to provide a cybersecurity assessment tool to transit agencies that caters to their current risk posture and threat environment. Originally intended for small to medium-sized transit agencies, the project is intended to help public transit agencies quickly understand gaps that may exist in their current cyber risk posture, and to deliver tailored resources to remediate those that are identified.

Research Process

The project team began by surveying existing cybersecurity assessment tools and resources that are available to public transit agencies (see Appendix C for a list of assessment tools reviewed for this project). Though many are free or inexpensive to use, all require a deep grasp of the language and structure for how cybersecurity is done. Using them effectively requires a level of understanding of the language and underlying concepts that many transit agencies simply do not have among their current team. To effectively use an existing tool, agencies that do leverage them most often engage with outside consulting firms to ensure the necessary knowledge and understanding is brought to bear.

¹ Belcher, Scott, Terri Belcher, Eric Greenwald, and Brandon Thomas. 2020. *Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness*. Mineta Transportation Institute Report 20-36, San Jose State University. <https://transweb.sjsu.edu/sites/default/files/1939-Belcher-Transit-Industry-Cyber-Preparedness.pdf>.

Using this survey of existing tools as a foundation, the project team identified the existing Cyber Resilience Review (CRR) developed by the U.S. Department of Homeland Security’s Cyber and Infrastructure Security Agency (CISA) as an optimal tool to assess the cybersecurity readiness of a public transit agency because of its focus on resiliency for critical infrastructure. The CRR leverages the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) as the basis. NIST is an arm of the U.S. government charged with developing standards and measurements across many areas of U.S. society and responding to the need for research of emerging topics affecting critical infrastructure. For cybersecurity subjects, NIST provides the foundation for all of U.S. policy. Using NIST-based products will help a transit agency understand cybersecurity best practices, manage cyber risks, and approach network assessments and monitoring in a systematic way. More on NIST can be found in Appendix A.

Using the principles of NIST and the CRR assessment tool, the team performed a cyber resilience assessment of the project’s sponsor, MetroLINK of Moline, Illinois, to observe first-hand the effort, expertise and other resources required to deliver an effective assessment.

When going through the assessment process with MetroLINK, the project team identified several opportunities to improve the experience of using the CRR for the transit context.

1. **Question Clarity:** The project team identified opportunities to streamline the questions to make them more understandable to the transit audience, adding terms and phrases well known among public transit executives as well as embedding definitions directly among the questions to assist with understanding.
2. **Response Clarity:** The CRR requires responses of “Yes”, “No”, or “Incomplete”. Selecting among them for each question was difficult as the definition of each response option was different for each question. The project team opted to reorganize the questions so that responders only had to choose the response that “best fit” their situation and context, enabling an easier selection.
3. **Industry-Specific Resources:** The project team added industry-specific resources to the existing resource guides from the CRR. These resources provide direct links to resources targeted directly to the public transit industry from CISA, APTA and others. See Appendix B for an overview of cyber resources for transit agencies.

The result of this work is the Cybersecurity Assessment Tool for Transit (CATT), an efficient, streamlined resource for public transit agencies to assess their existing cyber posture, with directed resources to assist in maturing their cybersecurity programs.

Overview and Scope of the CATT

The primary goal of the CATT is to develop an understanding and qualitative measurement of essential cybersecurity capabilities. Participants are asked to choose descriptions of practices that best describe the organization's current practices. The descriptions help participants to articulate evidence regarding both performances of cybersecurity practices as well as sustainment of those practices over time among a set of ten domains.

The domains examined are:

1. Asset Management
2. Controls Management
3. Configuration and Change Management
4. Vulnerability Management
5. Incident Management
6. Service Continuity Management
7. Risk Management
8. External Dependencies Management
9. Training and Awareness
10. Situational Awareness

As per assessment best practices, the CATT should be completed in a group setting, with leadership from each of the agency's key departments represented. It should not be completed solely by the technology team, as cybersecurity is a whole-of-organization endeavor. The discussions the assessment induces is a key value of the exercise, as it helps the organization understand and align on its current status with regard to cyber risk. A facilitator may be needed to ensure a quality discussion.

The tool is designed to be understandable by those not well versed in the language of cybersecurity. Definitions are provided for key words to ensure the broad group at the table is clear on the intent of the question. The CATT will take approximately a full day to complete, given the discussions that occur.

Once the CATT is completed, it is also important to provide time with the same group to review the findings and guidance of the resulting report. An outcome of this discussion should be an action plan documenting the next steps the organization plans to take to address any identified shortcomings. This too should facilitate productive and useful discussion among the team as to how to move forward on filling any gaps identified.

CATT Review Scoring

The CATT is an interview-based assessment. It is understood that participants often do not have complete knowledge of an organization's operations. For each question set, participants are asked to select the description that most aptly applies to their organization. There is no “right” or “wrong” answer. The intent is to document the current state of your cybersecurity program so that the CATT can assist in identifying gaps and help the organization in remediating areas where limited or no aspects of the program have yet been created. The discussion that this decision prompts is often as valuable as the selection itself.

For each question set, five descriptions of a practice are provided that accomplish the Goal, starting with “the practice is not performed”.

A Goal is considered “Red” if it is not consistently performed. A Goal is considered “Yellow” if it is consistently performed, but not yet consistently measured and managed. A Goal is considered “Green” if it is consistently performed and both measured and managed.

1. Practice is not performed (RED)
2. Practice is starting to be performed, but it is not yet consistently performed (YELLOW)
3. Practice is consistently performed, but not measured and managed (YELLOW)
4. Practice is performed and is starting to be measured and managed (GREEN)
5. Practice is performed and both measured and managed (GREEN)

The intent of the understanding provided by the CATT is to assist in prioritizing the work needed to better secure the public transit agency, and ensure it is resilient if an incident is to occur. Included within the CATT Self-Assessment Package are resource guides that provide step-by-step guidance for what to do to address opportunities for improvement as identified.

An independent review of the CATT is provided in Appendix D.

The CATT is available to all transit agencies via download on the Federal Transit Administration's [page for cybersecurity](#).

Section 1

Introduction

Transportation systems are quickly becoming multifaceted environments composed of numerous components that were not designed with cybersecurity in mind, from the internet-connected garage door to the driver display unit on the bus and everything in between. The wide range of threats and new threat vectors makes it difficult for organizations and those charged to protect them to keep up with evolving risks that target such systems. In parallel, a growing number of sophisticated attackers are driving new levels of creativity to access and disrupt the critical functions of transit organizations. Managing digital security in parallel to physical security is critical to assuring the free flow of transit systems, as well as the safety of passengers, employees, and stakeholders.

Resilience is the ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture consistent with an organization's needs.²

Cybersecurity assessment is the foundation for building resilience across a transit agency. Performing cybersecurity assessments is a method of understanding the security mechanisms, practices, and policies supporting an organization's resilience. The outcome of a cybersecurity assessment helps an organization identify vulnerabilities, prioritize needs, and understand where critical systems are not adequately protected. Assessments are not one-off exercises; they must be performed periodically over time to ensure a continuous understanding of an organization's security posture. Building a systematic approach to understanding the environment and reviewing opportunities for risk reduction will set the transit agency on a journey that supports best practices for cybersecurity management.

This modernized approach to risk management is critical in a time of widening technology implementation. The scope and complexity of digital technology, the expansion of digital networks, and the proliferation of multimedia communication channels greatly increase the opportunity for systemwide failure. For transit agencies, the use of digital technologies has moved beyond the back office, extending onboard passenger trainsets and railcars, on ferries and buses, and in stations.

² Computer Security Resource Center. "Glossary." National Institute of Standards and Technology, U.S. Department of Commerce. Accessed October 25, 2021. <https://csrc.nist.gov/glossary/term/resilience>.

Networking technologies such as cloud computing and fifth generation (5G) cellular technologies allow transit agencies to:

- More affordably manage their fleet
- Provide a rich array of new services to passengers
- Improve passenger safety and security through advanced monitoring
- Enhance control applications for operations, onboard security, and throughout the back office (e.g., positive train control)

Cloud Computing – A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.³

5G – 5G enables a new kind of network that is designed to connect virtually everyone and everything together including machines, objects, and devices. 5G wireless technology is meant to deliver higher multi-Gbps (Giga bits per sec) peak data speeds, ultra-low latency, more reliability, massive network capacity, increased availability, and a more uniform user experience to more users. Higher performance and improved efficiency empower new user experiences and connects new industries.⁴

The growth of IT implementations, digital component integrations, and data projects has increased dramatically in recent years. The level of cybersecurity for these digital systems, however, has not kept pace. Transit organizations are the end users, but do not build equipment. They rely on an array of suppliers to provide hardware, software, and services, interconnected and aligned to support the agency's mission and vision. Risk is diffused through these often-complex systems of vendors; however, the burden and liability always rest with the agency. Therefore, understanding the digital and physical risks across the environment begins with a proper assessment.

The practice of cybersecurity follows a formula; the high-level concepts are static across industries and organizations. As an assessor moves from the high-level to the tactical, they must have a keen awareness of both the physical and the technical environments. The assessment toolset utilized must be honed to produce data that allow risk managers and leadership to make the most effective decision about how to lower identified risk.

³ Computer Security Resource Center. "Glossary." National Institute of Standards and Technology, U.S. Department of Commerce. Accessed October 28, 2021. https://csrc.nist.gov/glossary/term/cloud_computing.

⁴ Qualcomm. "Everything you need to know about 5G." What is 5G? Accessed November 2, 2021. <https://www.qualcomm.com/5g/what-is-5g>.

An assessor must be aware of the transit operator environment. There are critical realities that must be understood given the history and development of public transit as it exists today. One of those realities is transit equipment manufacturers have been slow to build security into network components and conveyances. Worse, older components are unable to update or upgrade firmware or software. Many assets are built to enable efficient transportation management. Adding security after-the-fact can create new vulnerabilities, such as:

- Systems are deployed without the ability to perform patch management
- Networks are often left “open” and have poor or nonexistent access control
- Historically, software and/or firmware solutions are developed with redundant network services that are open and “listening”
- There is a “hard shell” mentality that assumes all attacks are stopped at the perimeter
- Vendors often transfer all cybersecurity liability onto the customer (i.e., the vendor will not be responsible for the external access controls to the systems)
- Compromised assets often do not provide alerts that identify a breach

Internet of Things (IoT)

IoT describes Internet-connected devices that enable seamless connections among people, networks, and physical services. The developments in IoT technologies have presented new types of cyber risk that are difficult to assess with the existing cyber risk approaches. IoT technologies need to be supported with a supply chain process to update the list of assets that are added to the network across periods of time. This will assist in preventing modified IoT components from enabling a disruption in the system. Although the U.S. government is trying to work with manufacturers to integrate better security in the use of IoT technologies across industries, many of the devices are still susceptible to successful attack.

The Internet of Things Cybersecurity Improvement Act of 2020 sought to address security given these advances.⁵ Although the new IoT cybersecurity law focuses primarily on the procurement of IoT technology and products by the federal government, it has the potential to ultimately create a more uniform IoT security standard across the private sector.

⁵ Internet of Things Cybersecurity Improvement Act of 2020, H.R. 1668, 116th Cong. (2019-2020). <https://www.congress.gov/bill/116th-congress/house-bill/1668>.

Digital Transformation

An important transformation occurring across the transit environment is the expanded interaction of networks within and among systems, as well as the introduction of software control capabilities. Systems that were once segmented from the Internet have become dependent on Internet-based connections to other systems. Software is blurring the lines between and among systems.

“Software is eating the world,” so coined Marc Andreessen, famed Silicon Valley venture capitalist.⁶ The basic idea behind this statement is that many activities are moving from physical to digital. This trend is now encroaching on public transit, as agencies are moving to more advanced digital practices such as mobile ticketing, upgraded data and analytics capabilities, and digital tools that enhance operations. With this paradigm shift comes the opportunity to rethink and redesign the way operations are executed. This transformation, however, also creates a new series of digital risks that are different from risks in the physical realm.

Public transit agencies are not alone—this trend is disrupting most industries. Consider how people now access music, shop, meet with work colleagues, or look for transportation options. These are just a few examples of industries that have been completely disrupted by the digital revolution.

As additional industries become disrupted and activities move from physical to digital, consumer behavior and expectations evolve. For example, it is no longer tenable to run a business on a cash basis alone; credit cards and, increasingly, digital mobile wallets are accepted, if not required. Similarly, providing paper-based schedules serve some, but many prefer digital options for finding their way. For many industries, this disruption has been met with accelerated innovation. As public transit progresses along its disruption journey, this “move fast and break things” mentality is not feasible, as “breaking things” can severely impact livelihoods and, where safety is concerned, people’s lives. Moreover, the public sector is not as accommodating of failure as the private. In the private sector, failure is accepted and even welcomed in many cases, in particular within the software sector with mantras such as “fail fast, fail often.” In the public sector, where public servants are using taxpayer dollars, risk taking is not as welcomed.

As software eats through industry by industry and organization by organization, how operations are executed is not the only disruption. The role of leadership is also impacted. Effective leadership is driven by leveraging assets while mitigating risks. Great leaders know how to manage risk. Digital risk requires

⁶ Andreessen, Marc. “Why Software Is Eating the World.” Andreessen Horowitz, August 20, 2011. <https://a16z.com/2011/08/20/why-software-is-eating-the-world/>.

particular consideration, as more digital technologies encroach into operations. The impact of digital risk on the overall risk landscape of an organization is increasing, necessitating leaders to incorporate new and different risks into their threat calculus.

As more riders depend on digital schedules to know when and where to catch the bus, train, or ferry, protecting the digital scheduling software is becoming critical to ensure effective service delivery. As operators move to digital or contactless payment systems, the ability to protect customers' financial and personally identifiable information (PII) is similarly critical. In many cases, legal and/or regulatory requirements influence how an agency must protect certain types of information. Understanding digital risk is an essential component of understanding the overall security of an organization.

Our Cyber World

Security of systems has long been an essential part of design, build, and operation processes. With the rise of the Internet, pathways to access systems from afar have become feasible. The ability of cyber interference to disrupt organizational operations has not gone unnoticed by nefarious actors. Digital vulnerabilities are being discovered and exploited at an increasing rate. Major attacks such as SolarWinds, Microsoft, Colonial Pipeline, and Kaseya have caused major interruptions and cost the global economy hundreds of millions of dollars in losses. The transit industry has also experienced a number of high-profile attacks involving the Metropolitan Transportation Authority (MTA) in New York, Martha's Vineyard Ferry in Massachusetts, Southeastern Pennsylvania Transportation Authority in Pennsylvania (SEPTA), and TransLink in Vancouver, Canada.

Cybersecurity is not just a security issue for organizations, but also a national security issue. Therefore, to protect critical infrastructure, the U.S. government designated transportation as one of 16 industries defined as critical infrastructure for the United States. The Department of Homeland Security (DHS) oversees the reduction of risks across these sectors, working with sector specific agencies that hold responsibility for public-private partnerships to assure sector resilience. This designation recognizes sectors that, if hit with a debilitating attack, will impact the economic security of the nation. With this designation comes a host of free U.S. government resources, but also scrutiny of transit agency cybersecurity practices.

Each transit organization, no matter the size, is responsible for the cybersecurity of its environment and the safety of its riders. From new mobile applications to new methods to schedule operator shifts, the digital footprint of the typical transit agency is broad. As this footprint grows, so too do the cyber vulnerabilities that can be exploited. As the broader threat landscape expands with the prominence and economic role public transit agencies play within

communities, these vulnerabilities are likely to be exploited by bad actors. Each new Internet-connected software, tool, or service adds vulnerability through which the system may be breached.

The public transit industry is not alone in dealing with cyber risk. Many industries have been dealing with such risk for decades. Resources exist at the federal, state, local, and industry levels to assist in building out an effective program. The National Institute of Standards and Technology (NIST) serves as the clearinghouse for documentation on how best to effectively manage cybersecurity systems. Oversight for operationalizing these frameworks, tactics, and techniques for national security falls to DHS's Cybersecurity and Infrastructure Security Agency (CISA). The American Public Transportation Association (APTA), the American Association of State Highway Transportation Officials (AASHTO), and other transit organizations also have resources available.

Cyber in Transit

In 2020, the Mineta Transportation Institute (MTI) released an important cybersecurity study, *Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness*.⁷ After surveying more than a third of APTA's public transit members, the researchers concluded that the industry is not prepared for the growing cyber threat. The MTI study found that most transit agencies do not have the basic policies or personnel in place to respond to a cyber incident. The study included several recommendations for the Federal Transit Administration (FTA), APTA, and public transit operators.

Agencies are beginning to take steps to protect themselves from cyberattacks, including conducting regular cyber assessments, seeking technical leadership from outside the transit industry, and contracting out the management of PII. Among the reasons for not implementing adequate cybersecurity practices is a reoccurring theme of scarce resources. The scarcity of financial and human resources will always be an impediment to the total application of cybersecurity best practices. However, by using the methodologies being created by the many collaboration efforts of the U.S. government, private sector, and academia, the cost of security planning and management is decreasing.

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 ransom in exchange for decryption.⁸

⁷ Belcher et al., *op cit*.

⁸ Cybersecurity and Infrastructure Security Agency. "Ransomware 101." Resources, Stop Ransomware. Accessed November 14, 2021. <https://www.cisa.gov/stopransomware/ransomware-101>.

Transit agencies that implement tested cybersecurity strategies will lower their organizational risks. COVID requirements and operational distraction have amplified cyber threats to transit agencies. Both DHS and the Federal Bureau of Investigation (FBI) have seen an increase in COVID-related attack types by malicious actors since the COVID outbreak in 2020.⁹ Taking a strategic approach to risk reduction and necessary steps toward good cyber hygiene will help organizations withstand and recover from many attack techniques. Implementing practices that identify, protect, detect, respond, and recover from cyber events will enhance the transit agency's ability to securely operate no matter what conditions it faces.

All agencies can take basic steps to minimize cyber risks, beginning with an assessment of the agency's cyber posture. Whereas most organizations have some tools and resources in-house that help to protect their assets, systems, and networks, it is hard for them to gauge the vulnerabilities or capabilities against certain attack methods. Even when they have a formal cybersecurity program, the absence of a systematic approach to identify and reduce cyber risk creates uncertainty. This negates the ability to ever quantify enterprise risk.

Although the capabilities that come standard with Microsoft and other business software or technologies such as firewalls are a great start, they often fall short in protecting the transit enterprise. To be competitive with a growing legion of smart and agile hackers requires a deliberate security management approach that leverages broader cybersecurity best practices and supports the organization's resilience.

How COVID-19 Changed Transit

The COVID-19 pandemic forced transit entities to quickly adapt to meet operational challenges, including securing assets, systems, and networks while maintaining quality of service. As system upgrades and agency operations continued remotely, information and operational technology risks increased exponentially.

Early in the COVID pandemic, transit organizations found themselves in a challenging situation—balancing the needs of essential workers who relied on public transit to travel to and from work with the impact of reduced ridership due to changing work and gathering restrictions. Transit leaders had to adapt quickly and adhere to new regulations and the evolving service needs of the community. Routes were changed or cancelled, fares were reduced or eliminated, and pre-pandemic public transit service was dramatically reduced.

⁹ Federal Bureau of Investigation. "FBI Releases the Internet Crime Complaint Center 2020 Internet Crime Report, Including COVID-19 Scam Statistics." National Press Office, March 17, 2021. <https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics>.

COVID caused a large segment of the workforce to move from working in an office to working from home. This transition forced organizations to rapidly adapt their digital support infrastructure. Meetings and teleconferences moved to digital meeting venues such as Zoom or Microsoft Teams. On-premise systems had to be accessed by a newly remote workforce. IT staffs had to ensure existing services remained available and that these new, now-critical services were integrated into the organization's infrastructure, often in a matter of days. Protection of these systems frequently took a back seat to ensuring the team had what it needed, compounding digital risk exposure.

Further, as teams got their home-based operations up and running, new vulnerabilities were introduced. The home wireless network of each team member, the home computer used to access that internal system, and even the remote learning system accessed on the work computer to facilitate home schooling for children all introduced risk to the organization's cybersecurity posture. Connecting computers to minimally protected home and public Wi-Fi introduced the possibility of device compromise. Networks and systems may not have been visually inspected since work from home policies were implemented. Cybersecurity practices may have been relaxed to maintain or accommodate employee and contractor remote connectivity given urgent needs.

Most transit agencies are prepared to manage unforeseen circumstances because many agencies play a critical role in municipal emergency response. Digital risk and response, however, have not necessarily been accounted for in many systems. These must now be added to the playbook to ensure that all employees and stakeholders are working to minimize cyber risks.

Now more than ever, it is critical that public transit agencies secure their remote worker systems. In the age of COVID, the remote worker environment has been stretched, tested, and deployed to a degree that was likely unplanned. Hybrid and remote work opportunities that may not have existed prior to the pandemic are also increasing, which reinforces the need to create sustainable cybersecurity policies and practices for individuals accessing key systems from off site.

Endpoints

Allowing employees to seamlessly connect to corporate networks is essential for them to fulfill their roles, but every device that connects to the network presents its own inherent risk. When employees work from home, they sit outside the reach of the corporate firewall that can monitor and block incoming and outgoing communications to endpoint devices. Many organizations insist that employees connect to a virtual private network (VPN) and while this can offer some protection, ensuring all employees do so regularly can be challenging.

Endpoint devices have become an attractive target for cybercriminals. They often have unpatched software vulnerabilities and (via the user) remain susceptible to phishing, the most common attack vector used to target endpoints.

Cyberattacks are increasingly designed to target endpoints, seeking to install malware and gain unauthorized access to networks. The proliferation of endpoint devices in recent years has increased the opportunities for adversaries to launch these attacks, and the shift to cloud hosting and software as a service (SaaS) only complicates this issue further. The average cost per breach resulting from an attack on endpoints is more than twice the average cost of a general data breach.¹⁰

The significant damage and disruption that endpoint breaches can cause make incident response essential. An assessment must consider the ability to respond in the context of limiting attacks occurring at an endpoint. Positive impacts of this focus include reducing incident response times by disrupting and containing attacks earlier in the attack chain process.

Culture of Cybersecurity

Security and safety have long been organization-encompassing issues for public transit agencies. The team is defined, accountability is instilled, and policies and procedures are disseminated throughout the organization, from the board and CEO to the bus inspector. Cyber risk, as an element of organizational safety and security, should be incorporated into the culture of accountability and policy communication. The resources required to make this happen—the investment of time and money—generally come from an agency’s leadership. As such, transit organization leaders need to invest their own time to ensure that cybersecurity is a recognized priority and a responsibility embraced throughout

¹⁰ RevBits. “The Growing Importance of Endpoint Security.” December 7, 2020. <https://www.revbits.com/blogs/the-growing-importance-of-endpoint-security>.

the ranks of their organization. Leadership emphasis on the subject reminds employees and stakeholders that cybersecurity tools and the IT department alone will never make a transit agency secure.

A culture of cybersecurity is an environment where employees have been trained to effectively use good cyber hygiene and recognize opportunities to reduce individual and organizational risk. An example would be to ensure that each new employee has specific role-based cyber threat training. Employee training is one of the most important security breach prevention methods an organization can implement. Promoting documented processes and robust training will contribute to employees' ability and dedication to detect attacks.

Employees are the foundation of the operation and play an outsized role in mitigating such vulnerabilities. Training that supports cybersecurity best practices and agency procedures will provide a foundational layer of security. Cybersecurity programs support business best practices. Examples of security controls include ensuring IT services are shut off at employee termination and documenting all IT assets. They help limit an organization's liability, better manage system oversight, and inform financial decisions. Assessors should review practices across transit agencies to determine where cyber education will assist in identifying cyber exploits and quickly manage consequences to limit cascading effects.

Through a robust assessment, information about the alignment of functions, programs, and initiatives should deliver a perspective on points of intersection, overlap, and possible leverage where informed employees can impact attacks against the organization. Questions as simple as understanding if employees are trained on certain threats and why specific response approaches are used can reduce cyber risks. Therefore, it is important that an assessor understands if formalized, improved, multidirectional information exchanges that are top-down, bottom-up, and between offices are part of the organization's culture. Ultimately, these activities are key to reducing the cost of cybersecurity.

Training is just one of many domains that must be monitored and continuously improved upon to reach accepted levels of risk for a transit organization. The assessment process is the mechanism to understand if goals are being met across all of them and what investments must be prioritized to reach the acceptable level of risk. As important as training is, transit agencies must regularly examine the value and effectiveness of all security domains through a robust cybersecurity assessment process to understand opportunities for reducing enterprise risks.

Cybersecurity Leadership

Is it an “IT” thing? Given its technical roots, many are inclined to assign cyber risk management to the IT team. While this may work for some organizations, many IT teams will struggle with ensuring cyber risk management is a whole of organization approach. As the tools of cybersecurity gain in importance, policies, procedures, and the role of individual responsibility often do not get the attention they deserve. Agencies that house cyber risk management under IT must ensure that IT leadership has the authority and breadth to manage across departments.

Is it a “Security” thing? Other organizations add cyber risk management under existing safety and security departments. However, those departments often lack the technical knowledge and domain expertise to effectively lead cyber risk management. Agencies that house cyber risk management under security must bring in the correct technical leadership to effectively manage the technical risks and opportunities.

Is it a “C-Suite” thing? The CEO and the executive leadership team are forced to balance and act on an array of ever-changing risks with limited and often insufficient resources. Cybersecurity risks should be regularly included on the executive and board agendas to ensure risk management decisions are made with the full risk landscape in mind.

Resiliency

Every organization determines acceptable risk to a function or service differently, respective of its risk tolerance. Comprehension of the risk, however, is only a segment of the work. Management and mitigation of the accepted risks—the process of building and maintaining resilience—is a long-term process.

Cyber resiliency is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.¹¹ Cyber resiliency focuses on capabilities supporting the key organizational mission. It maximizes an organization’s ability to complete critical functions despite an adversary present in its systems and infrastructure. Although an organization may not know that a specific attack will occur, it can anticipate the potential outcomes of such an attack and maintain operations.

¹¹ Computer Security Resource Center. “Glossary.” National Institute of Standards and Technology, U.S. Department of Commerce. Accessed October 23, 2021. https://csrc.nist.gov/glossary/term/cyber_resiliency.

With this knowledge, the organization can plan to protect against the attack and put mechanisms in place to respond if systems are breached. The planning process can identify existing gaps, which will inform decisions around resource investments and risk prioritization. Organizations manage risk in a variety of ways, including accepting the risk, seeking to remove it, buying it down, transferring it, or avoiding it. To compensate for uncertainty, organizations can take various approaches to determine the likelihood of events, ranging from a worst-case, imminent event to an unobserved, highly unlikely event.

By performing cyber assessments and using the results as input into a cyber resiliency plan, an organization can plan around potential uncertainty. Information derived from previous attacks, exercises, and anecdotal data can assist in planning for potential attacks and provide a baseline for cyber risk. This information can be accessed through cyber threat information sharing arrangements, even if it has not been observed at the transit agency being assessed.

Section 2

The Transit Cyber Environment

Transit operations manage large numbers of control and communications systems that must safely interoperate to provide seamless service to the public. Transit agencies interconnect systems to incorporate new technologies, delivering innovations that increase operational efficiencies, improve safety, and enable data sharing and reporting with other groups internal and external to the organization. This activity provides real-time information for key stakeholders, bolstering physical and operational security and enhancing system performance. Many of these interconnected systems, however, were never designed or envisioned to be connected as an enterprise system. Additionally, they were never meant to be accessible, either directly or indirectly, via the Internet.

Historically, physical systems were segregated so that a breach of one in no way could impair another. The bus, the door to the garage, and the gate to the parking lot were separate systems, well segregated from one another. These operational technology (OT) systems included firmware and even software, but for a long time they remained segregated from other systems. The expansion of information technology (IT) in many cases altered the working environment for OT.

Operational technology (OT) is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes, and events.

Information technology (IT) is the common term for the entire spectrum of technologies for information processing, including software, hardware, communications technologies, and related services. In general, IT does not include embedded technologies that do not generate data for enterprise use.¹²

IT systems are designed to be connected. The more connected an IT system, the more useful and valuable it becomes. A computer on the desk is almost useless unless it is connected to the Internet. In most transit agencies, connection to the outside world and various business systems is inevitable, if not already a requirement of the architecture. Agencies are facing increasing pressure to obtain, analyze, and share data to improve service and performance.

Connectivity to partners and data-sharing systems creates new efficiencies. Web-enabled public information systems and remote business partner

¹² Gartner. "Gartner Glossary." Accessed November 1, 2021. <https://www.gartner.com/en/information-technology/glossary>.

interfaces are a growing trend. Lines between government and private-sector partners are blurring. This includes internally between IT and OT, as well as externally between government agencies and vendors. Connected, electric, and autonomous vehicle systems and the addition of new transportation modes will exacerbate this situation. Transit operators are evolving into mobility or communication hubs.

With the rise of Internet-enabled systems, the traditional physical segregation is becoming less feasible given the demands of the organization. Once an Internet-connected device or technology is introduced to any of these systems, the entire system becomes vulnerable to that potential access point. Enabling closed circuit television (CCTV) on a bus effectively exposes the bus to any Internet-connected device because often other operating systems share the same hub those CCTV devices use to supply the security team with video. Even physical systems like garage doors and parking lot gates are increasingly tethered to the Internet in some way, if only through the operations monitoring software that many agencies use to manage and oversee access.

These standard OT systems were not built to be revised, refined, upgraded, patched, or otherwise iterated. They were built to do one thing, do it well, and do it in isolation from any other system. The firmware and software involved was not designed to be tinkered with, let alone integrated with other systems. As OT and IT systems are merged, the resulting system takes on the security profile of the IT system. The risk introduced by adding IT capabilities to OT systems must be understood and managed effectively.

Key Considerations

The following are key considerations for cybersecurity assessments in a public transit environment.

Information Technology

Much of cybersecurity vulnerability relies on remote access—nefarious access to data or systems using the communication channels of the Internet. Referred to more broadly as IT, this arena encompasses the storing, retrieving, and sending of information, most often in the form of data. When we think of modern, disrupting technologies, most think first of the computer and the mobile phone. These are forms of IT.

Fortunately, the public transit industry is not alone in needing secure IT infrastructure. A vast array of tools and resources already exist, many built into existing software and systems. For example, most enterprise office software typically comes equipped with useful tools and resources that can be configured to further secure a transit operator's implementation of that network.

Transit agencies are facing many of the same issues observed across other industries related to IT. Managing the cybersecurity elements of any expansion can be challenging. Transit agencies must implement systematic approaches to integrate change and control risk within their enterprise, especially as they evolve and iterate with new technologies. For example, organizations are now forced to manage the challenges associated with improving and rearchitecting existing technology to bustling systems without service disruption.

Operational Technology

The predecessor to IT is OT. Think of this as the technology that predates the Internet—the garage door, the tools, and the infrastructure used to manage the bus yard and beyond. These are the systems critical to running operations. A subset of OT are industrial control systems (ICS), the systems used to monitor and control industrial processes—mission-critical operations. Examples of ICS in the transit environment are the systems that manage garage access or the HVAC system.

Many industrial control systems are managed by a supervisory control and data acquisition (SCADA) system. SCADAs provide a graphical interface and alerting mechanisms so that an operator can know and understand the current state of the system over time. Examples of SCADAs in the transit environment are the software that manages building access or the tools used to oversee the fueling of buses. These systems have been attacked all over the world. In many cases, transit operators use equipment and systems provided by the same vendors. As such, a vulnerability at one transit agency most likely exists at others.

The Cybersecurity and Infrastructure Security Agency (CISA) has produced a series of recommendations on best practices to secure industrial control systems. According to CISA:

Industrial Control Systems are important to supporting U.S. critical infrastructure and maintaining national security. ICS owners and operators face threats from a variety of adversaries whose intentions include gathering intelligence and disrupting National Critical Functions.¹³

Key recommendations from CISA on how to protect ICS infrastructure include:

- Check, prioritize, test, and implement ICS security patches.
- Backup system data and configurations.
- Identify, minimize, and secure all network connections to ICS.

¹³ Cybersecurity and Infrastructure Security Agency. “CISA Industrial Control Systems Security Offerings.” Publications Library. Accessed December 2, 2021. <https://www.cisa.gov/publication/ics-security-offerings>.

- Continually monitor and assess the security of ICS, networks, and interconnections.
- Disable unnecessary services, ports, and protocols.
- Enable available security features and implement robust configuration management practices.
- Leverage both application whitelisting and antivirus software.
- Provide ICS cybersecurity training for all operators and administrators.
- Maintain and test an incident response plan.
- Implement a risk-based defense-in-depth approach to securing ICS hosts and networks.¹⁴

Integration of OT and IT

The risks of OT and IT as stand-alone systems are well understood by security professionals. However, with transformations underway in mobility writ large, and among public transit systems specifically, the line between OT and IT is blurring. It is increasingly difficult to keep OT systems segregated, introducing a host of new risks and vulnerabilities.

Due to the nature of their design and intended independent operating environment as a siloed system, this infrastructure was not designed with an organized set of cybersecurity criteria in mind. Common design practices were to keep the ICS isolated from the enterprise and other networks; hence cybersecurity was never baked into the system architecture. ICS designs were based on system functionality, reliability, and availability. But with the current needs of data sharing and system accessibility, industrial control systems are being connected to the outside world—in effect corrupted from their intended design. The ever-increasing digitization of the transit environment and the need for information gathering increase opportunities for cyber-related incidents and network infiltration.

To understand risk around ICS, transit agencies should consider the following questions:

- Can a computer or mobile device be used to collect intelligence and monitor the operational network(s)?
- Can an outsider use the network to take control of the system(s)?
- What can a disgruntled insider do to degrade the network (systems, assets)?
- How can policies, lines of responsibility, training, and compliance audits help secure the agency's assets?

¹⁴ Cybersecurity and Infrastructure Security Agency. "Recommended Cybersecurity Practices for Industrial Control Systems." Accessed November 13, 2021. https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf.

- How can software change management lessen the chances of software configuration problems?
- How can the system be returned to normal operation after an attack?
- What is the physical response from cyber disruption? Is there a disaster recovery plan for the ICS in case of attacks? Is the plan current?

Figure 2-1 shows a comparison of how security topics are handled differently by information technology and industrial control systems.

SECURITY TOPIC	INFORMATION TECHNOLOGY (IT)	CONTROL SYSTEMS (ICS)
Antivirus and Mobile Code	Very common; easily deployed and updated	Can be very difficult due to impact on ICS; legacy systems cannot be fixed
Patch Management	Easily defined; enterprise wide remote and automated	Very long runway to successful patch install; OEM specific; may impact performance
Technology Support Lifetime (Outsourcing)	2-3 years; multiple vendors; ubiquitous upgrades	10-20 years; same vendor
Cyber security Testing and Audit (Methods)	Use modern methods	Testing has to be tuned to system; modern methods inappropriate for ICS; fragile equipment breaks
Change Management	Regular and scheduled; aligned with minimum-use periods	Strategic scheduling; non trivial process due to impact
Asset Classification	Common practice and done annually; results drive cyber security expenditure	Only performed when obligated; critical asset protection associated with budget costs
Incident Response and Forensics	Easily developed and deployed; some regulatory requirements; embedded in technology	Uncommon beyond system resumption activities; no forensics beyond event re-creation
Physical and Environmental Security	Poor (office systems) to excellent (critical operations systems)	Excellent (operations centers; guards, gates, guns)
Secure Systems Development	Integral part of development process	Usually not an integral part of systems development
Security Compliance	Limited regulatory oversight	Specific regulatory guidance (some sectors)

Figure 2-1 Comparison of IT and ICS¹⁵

¹⁵ American Public Transportation Association. 2013. *Securing Control and Communications Systems in Rail Transit Environments, Part II: Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones*. APTA-SS-CCS-RP-002-13. https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-002-13.pdf.

Integration of Digital with Physical

Beyond the integration of OT with IT technologies, digital and physical systems are integrating across many key aspects of operations. Even physical security relies on a series of digital tools and resources. In many transit organizations, the head of security owns the assessment of risk for the organization. However, digital risk is the purview of the IT team—often a wholly discrete endeavor. Integrating digital risk into the overall risk assessment of the organization is becoming more critical as digital technologies play a larger role in the organization.

Transit agencies are the ultimate cyber-physical environment. In a resource-constrained environment, considerations must be made to determine where and when to implement prescribed controls so that system owners can identify cyber issues. By modeling the entire environment, the assessment approach can allow planners to determine the optimal time and place to intervene when required. The goal should be to enable organizations to quickly discover and prioritize cyber threats by creating a model that integrates all available organizational data. The assessment should produce data that aid organization-wide support and engagement. The expectation is that hackers will exploit the cyber-physical connection where possible.

System Architecture

All public transit agencies execute their mission through a complex set of systems that include vehicle and operator management, fare management, traditional back-office systems such as the general ledger and e-mail and file management, among others. For the most critical systems, referred to as “high value assets” (HVAs) in CISA’s documentation, network segmentation is required to ensure its data flows are uncorrupted.¹⁶ Network data flow to and from an HVA, and the flows within it must be isolated from other flows. In addition, these data flows must be encrypted so that if (or when) they are exposed, the data within remain secure.

The cyber assessment will assist in identifying cybersecurity linkages and interdependencies. Safety functions often ride the same conduits and digital systems, and so digital risk must be considered when designing and assessing the effectiveness of safety systems. The assessment may also reveal a host of unrelated vulnerabilities that may be addressed by altering the system architecture.

¹⁶ Computer Security Resource Center. “Glossary.” National Institute of Standards and Technology, U.S. Department of Commerce. Accessed November 2, 2021. https://csrc.nist.gov/glossary/term/high_value_asset.

NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations

This specification provides examples of data flow restrictions:

- Blocking outside application, or network-layer traffic claiming to be from within the organization (e.g., inbound e-mail claiming to originate from an internal e-mail address)
- Blocking web requests to external websites that are not from the HVA's web proxy server
- Restricting information transfers between the HVA and external organizations based on analysis of data structures and content¹⁷

As systems that include HVAs are identified, it is important to further define the “security zone”—the set of security requirements for the portion of the network that includes this system and/or an HVA. This form of documentation and policy places the necessary focus and attention on managing the network given the role the system plays in ensuring safe and successful operations.

As the design and architecture of the complex set of systems matures, “zero trust architecture” should become part of the conversation and risk management goals. The 2021 Presidential Executive Order on Improving the Nation’s Cybersecurity instructed federal departments and agencies to move closer to a zero trust architecture.¹⁸ The idea is that the design of the system precludes the need to trust any one entity or individual in ensuring the security of the system.¹⁹ This is an ambitious goal—one that few, if any, transit systems have successfully reached.

¹⁷ National Institute of Standards and Technology. 2020. *Security and Privacy Controls for Information Systems and Organizations*. NIST Special Publication 800-53 Revision 5. U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>.

¹⁸ National Institute of Standards and Technology. “Improving the Nation’s Cybersecurity: NIST’s Responsibilities Under the May 2021 Executive Order.” Accessed October 27, 2021. <https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity>.

¹⁹ Computer Security Resource Center. “Glossary.” National Institute of Standards and Technology, U.S. Department of Commerce. Accessed October 24, 2021. https://csrc.nist.gov/glossary/term/zero_trust_architecture.

Assessment Best Practices

Cybersecurity assessments have become fundamental components of an organizational risk management program.²⁰ Organizations from across the world use these assessments to identify, estimate, and prioritize cyber risks to organizational operations. Transit agencies can use the cybersecurity assessment process to address ongoing threats to operations, assets, passengers, and stakeholders from adversaries looking to disrupt service.

Organizations conduct risk assessments to determine risks that are common to the organization. Risk is “a measure of the extent to which an entity is threatened by a potential circumstance or event and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.”²¹ A good cybersecurity assessment incorporates these tenants and overlays accountability to assist transit agencies in planning. The first step in performing an assessment is identifying the team that will execute the process.

Key Roles

A successful assessment is predicated on inclusion and requires the active participation of members of the organization who serve in various roles. In its Self-Assessment Guide for the Cyber Resilience Review tool, CISA defines the key roles involved in an assessment process.²²

The **sponsor** should ideally be the chief executive or another senior executive in the organization and should have a broad understanding of the importance and purpose of completing an assessment. General responsibilities include:

- Deciding whether the organization should conduct an assessment
- Selecting an individual to serve as the facilitator
- Ensuring that the resources necessary for the assessment are available
- Communicating the organization’s support for the assessment

The **facilitator** is identified and assigned by the sponsor to have overall responsibility for preparing the organization and conducting the assessment. General responsibilities include:

²⁰ National Institute of Standards and Technology. 2011. *Managing Information Security Risk: Organization, Mission, and Information System View*. NIST Special Publication 800-39. U.S. Department of Commerce. <https://csrc.nist.gov/publications/detail/sp/800-39/final>.

²¹ Computer Security Resource Center. “Glossary.” National Institute of Standards and Technology, U.S. Department of Commerce. Accessed October 21, 2021. <https://csrc.nist.gov/glossary/term/risk>.

²² Cybersecurity and Infrastructure Security Agency. 2020. “*Cyber Resilience Review (CRR): Method Description and Self-Assessment User Guide*.” Cybersecurity and Infrastructure Security Agency, April 2020. U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/publications/2_CRR%204.0_Self-Assessment_User_Guide_April_2020.pdf.

- Completing the three phases of an assessment process
 1. Critical service scope
 - Ask: Which service will be the focus of the self-assessment?
 2. Organizational scope
 - Ask: Which parts of the organization deliver the critical service?
 3. Asset scope
 - Ask: Which assets are required for delivery of the service?
- Working with the organization to ensure the assessment produces high-quality results
- Facilitating the completion of the assessment form
- Driving the generation, development, and management of the assessment report
- Distributing the assessment report to the sponsor and designees
- Assisting in the planning of follow-on activities

Subject Matter Experts (SMEs) are members of the agency’s organization who have the most direct understanding of the system or function in question. During the self-assessment, SMEs provide answers that best represent the organization’s true cybersecurity capabilities in relation to the function being evaluated. SMEs should not be chosen by position. Rather, they should have an ability to provide input based on knowledge. The SME should be:

- Closely involved in the planning, implementation, or management of the domain represented
- Able to represent organizational functions being assessed
- Able to represent one or more of the organization’s activities in the assessed domains.²³

A cyber assessment is an effort to identify, estimate, and prioritize information system risks by looking at vulnerabilities and the capability to manage them. The above team leverages the assessment tools and framework to gather and order information. The next phase of the process is to use this information to define a roadmap to remediate vulnerabilities identified and mitigate key risks, relative to their potential impact on the organization.

Assessment Support

One of the first decisions the agency needs to make is to determine the optimal support required to deliver on the outcomes of the assessment. Vendors can be engaged to support the assessment, although the process cannot be fully outsourced. At minimum, the key roles identified above need to be engaged from within the organization.

²³ *ibid.*

Some agencies may choose to conduct an assessment without engaging outside resources. However, at some point, an external perspective may be essential to fully assessing the agency's cyber posture. At the very least, periodic penetration tests should be performed with outside support so that the agency's vulnerabilities can be fully tested by a third party.

Assessment Process

The information systems and operational technologies that support critical functions must be known and documented to adequately secure them. The practice of cataloging and measuring vulnerabilities will also assist in identifying undocumented assets and systems. When these assets are silently working within an enterprise, they pose a liability and cyber risk. Risk managers will not know what the assets are doing, who has access to them, or what impact they may have on the effectiveness of the organization's plans, processes, and procedures.

Any combination of the following techniques can be used in gathering information relevant to the IT system within its operational boundary.

Questionnaire. To collect relevant information, risk assessment personnel can develop a questionnaire concerning the management and operational controls planned or used for the IT system. This questionnaire should be distributed to the applicable technical and nontechnical personnel who are designing or supporting IT systems.

On-site Interviews. Interviews with IT system support and management personnel can enable risk assessment personnel to collect useful information about the IT system (e.g., how the system is operated and managed).

Document Review. System documentation (e.g., system user guide, system administrative manual, system design and requirement document, acquisition document) and security-related documentation (e.g., previous audit report, risk assessment report, system test results, system security plan, security policies) can provide good information about the security controls used by and planned for the IT system.

Use of Automated Scanning Tool. Proactive technical methods can be used to collect system information efficiently. For example, a network mapping tool can identify the services that run on a large group of hosts and provide a quick way of building individual profiles of the target IT system(s).²⁴

²⁴ Stoneburner, Gary, Alice Goguen, and Alexis Feringa. 2002. *Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology*. NIST Special Publication 800-30. National Institute of Standards and Technology, U.S. Department of Commerce. <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf>.

Plans and Procedures

The cybersecurity assessment reviews the plans and procedures that are in place. Ideally, the transit operator will have a security plan or security specific plan (SSP) in place—a document that outlines how an organization implements its security requirements. An SSP defines the roles and responsibilities of security personnel. It details the different security standards and guidelines that the organization follows. An SSP should include high-level diagrams that show how connected systems talk to each other. The organization should outline its design philosophies in its SSP. Design philosophies should include defense-in-depth strategies, which are a series of security mechanisms and controls that are thoughtfully layered throughout a computer network to protect the confidentiality, integrity, and availability of the network and its data.²⁵ All information in the SSP should be high-level but should include enough information to guide the design implementation of the organization’s systems.²⁶

Transit Industry Preparedness?

From *Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness* (MTI Study):

- 42% don’t have an incident response plan; of those that have one, over half have not had a drill in over a year
- 36% do not have a disaster recovery plan
- 53% do not have a continuity in operations plan
- 58% do not have a business continuity plan
- 67% do not have a crisis communications plan²⁷

Assessment Scope

The assessment scope consists of three components:

1. **Vulnerabilities** – the internal characteristics of the systems and organization that increase risk
2. **Threats** – the external variables that affect risk and inform the scale and roadmap for risk mitigation processes
3. **Response and recovery** – the ability of the organization to effectively respond and recover when incidents occur

²⁵ Center for Internet Security. “Election Security Spotlight – Defense in Depth (DiD).” Accessed December 1, 2021. <https://www.cisecurity.org/spotlight/cybersecurity-spotlight-defense-in-depth-did/>.

²⁶ CyberAssist. “Cybersecurity Maturity Model Certification (CMMC) Practice CA.L2-3.12.4 – System Security Plan.” Accessed November 15, 2021. <https://ndisac.org/dibsc/cyberassist/cybersecurity-maturity-model-certification/level-2/ca-2-157/>.

²⁷ Belcher et al., *op cit*.

Managing Vulnerabilities

Vulnerabilities are weaknesses in the system. A performance expectation or service level agreement is essential to unearth vulnerabilities. A weakness in the code that most software and hardware components have, when exploited, results in a negative impact to confidentiality, integrity, or availability. These outcomes or resulting consequences can have cascading effects that render a system inoperable.

Patching vulnerabilities and managing them can reduce the risk. Some systems can be patched through architectural changes, software updates, and hardware exchange. However, vulnerabilities are not always known. A cybersecurity assessment can identify vulnerabilities and provide insights into the risk posed to other systems. The follow-on to the assessment is just as important and provides an opportunity to prioritize the mitigation of the vulnerabilities.

Understanding Threats

Cyber threats are attempts to damage or disrupt a computer network or system. Cyber threats can exploit vulnerabilities present within a network, hardware, or software. CISA advises that most cybersecurity guidance addresses access control, configurations, and accountability,²⁸ but businesses cannot determine risk or know where to invest in security until they know the threat landscape facing their organization.

Cyber threats emanate from many sources. Nation states, independent hackers, experimenters, and hacktivists all pose a risk to information systems. Less recognized are internal threats. Employees and stakeholders with access to systems can do damage based on their knowledge of the enterprise and understanding of vulnerabilities. This is one reason protection tactics such as network segmentation are important. The cybersecurity assessment will identify if these practices are being implemented. If they are not, the identification of the vulnerability will populate the roadmap of items to resolve. This is a critical step toward network resiliency.

Response and Recovery

Given the increasing number of cybersecurity attacks occurring around the globe, organizations should plan for their defenses to be breached. Proper planning can improve resilience by ensuring that an organization's risk management processes include comprehensive recovery strategies. Identifying and prioritizing organization resources helps to guide effective plans and utilizing realistic test scenarios will hone these plans. Adequate preparation

²⁸ Bartock, Michael, Jeffrey Cichonski, Murugiah Souppaya, et al. 2016. *Guide for Cybersecurity Event Recovery*. NIST Special Publication 800-184. National Institute of Standards and Technology, U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf>.

enables rapid recovery from incidents and will help to minimize the impact on the organization and its stakeholders. Organizations should strive to create a culture of ongoing institutional learning so that recovery plans can be improved and updated based on lessons learned directly or via the experiences of other organizations.

Recovery is executing contingency plan activities to restore organizational mission and business functions. Reconstitution takes place following recovery and includes activities for returning systems to fully operational states.²⁹

Assessment Frequency

An assessment is often done in the face of a changing environment. Organizations should codify the risk assessment's scope, methodology, and frequency with an understanding that new devices are potentially being added more frequently than reviews of the network are conducted. It is important that the organization appreciates that an assessment is a reoccurring stage in the process, not just the beginning.

In fact, NIST recommends that organizations engage in a System Development Life Cycle (SDLC) approach (shown in Figure 3-1), whereby assessment is only a gate on a continuous process of maturing and iterating the firm's cybersecurity posture.

²⁹ Computer Security Resource Center. "NIST Risk Management Framework (RMF)." National Institute of Standards and Technology, U.S. Department of Commerce. Accessed November 4, 2021. <https://csrc.nist.gov/projects/risk-management/sp800-53-controls>.

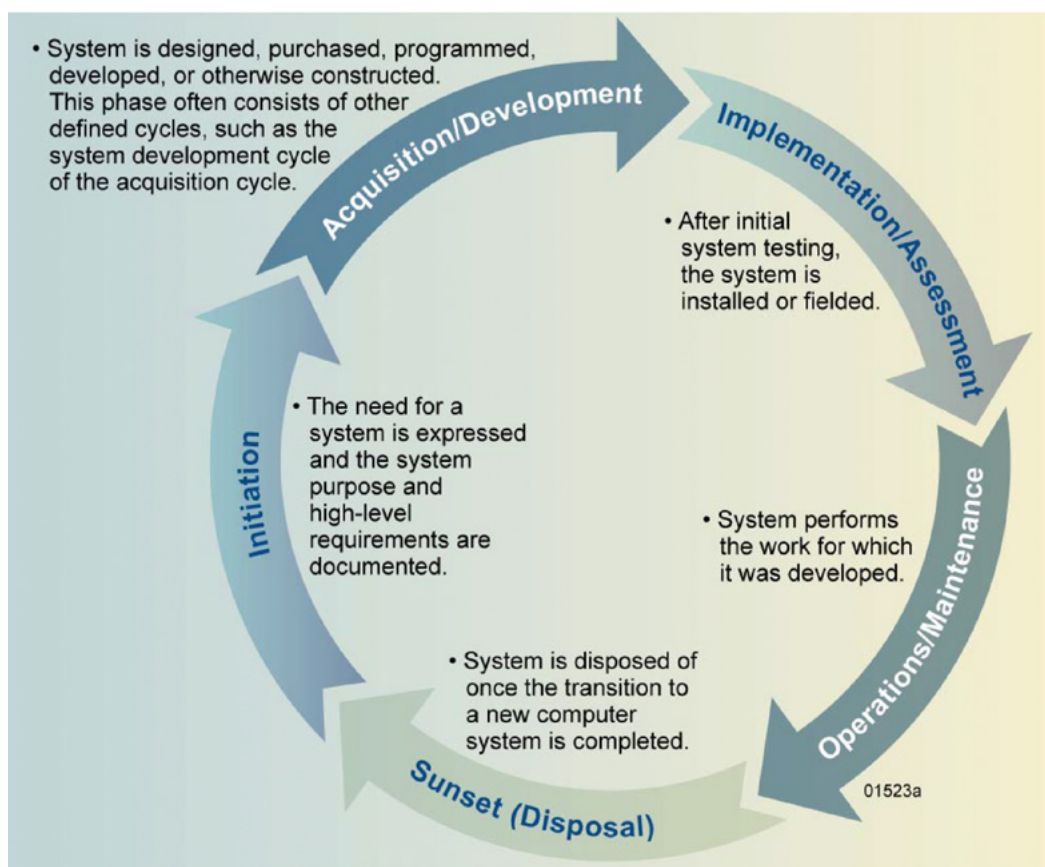


Figure 3-1 NIST System Development Life Cycle³⁰

Assessments are a part of an action plan for resilience. The environment in which a system-of-interest is engineered is rarely static. Keeping abreast of changes, additions, system access, configurations, modernization impacts, and maintenance is a difficult task. However, properly assessing systems and their interconnectivity against reference points, or baselines, makes managing this environment easier and can ultimately save money.

Assessments must produce an outcome that informs potential investment actions. In some cases, the assessment results may support reprioritizing budget expenditures because vulnerabilities to address are found to reside in parts of the system or organization that do not have budget allocation to make the fix.

³⁰ Radack, Shirley (ed.). "The System Development Life Cycle (SDLC)." National Institute of Standards and Technology, p. 3. Accessed October 16, 2021. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=902622.

Improving the Assessment

The following elements will further improve the effectiveness of the assessment process and enable an organization to move faster in maturing its cyber risk program and processes.

System Classification

A key first step to building a resilient transit system is to identify and understand systems across the enterprise. Organizations must identify the critical services that will serve as the focus of the assessment. A critical service is defined as:

A set of activities that the organization carries out in the production of a product while providing services to its customers, that are so important to the success of the organization that disruption to the service would severely impact the organization’s operations or business.³¹

The key to securing digital systems is the handling of data: how it is being handled, where it is maintained, and how it is transferred. Plans should be in place to ensure critical data remains available in the face of disruptions—and only to those individuals or systems authorized to use it. Data streams should be monitored to ensure data is not corrupted. This concept is referred to as the “CIA Triad” and should be at the forefront of consideration when seeking to protect electronic networks, systems, and assets.³²

The CIA Triad

Confidentiality – Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Integrity – Guarding against improper information modification or destruction; includes ensuring information non-repudiation and authenticity.

Availability – Ensuring timely and reliable access to and use of information.³³

Effective management of data per the structure of the CIA Triad is not a new concept; many industries and organizations employ the concept to plan and design a system architecture that minimizes risk to data. The primary difference for public transit is the key role these systems play in ensuring the safety of

³¹ Cybersecurity and Infrastructure Security Agency, 2020, *op cit*.

³² Walkowski, Debbie. “What Is the CIA Triad?” Learning Center, F5 Labs. July 8, 2019. <https://www.f5.com/labs/articles/education/what-is-the-cia-triad>.

³³ *ibid*.

agency customers and employees. Understanding how safety is impacted when defining CIA across data streams is critical. This observation was given particular attention as the project team built out the assessment tool for public transit agencies. Leveraging the CIA Triad, each system should be characterized to define the potential risk it introduces to the mission and operations of the organization.

APTA standards present information management and the delivery ecosystem of a transit agency as having three main parts: operational systems, enterprise information systems, and managed systems. A robust transit agency must combine and integrate dozens of key systems that fall into each of these three areas and safety zones.

A greater discussion about conveyances including trains, buses, and ferries are out of scope for this document. However, if viewed as endpoints of a network, they must be acknowledged and identified. Comprehensive assessments require that an assessor see the entirety of the system. In transit, the network boundaries are extended and potentially moving. Considerations such as bidirectional information flow, the safety impacts an attack may present, and physical connections to conveyances that link to networks are very much in scope.

System Criticality

Transit operators can identify the criticality of systems through several methods. One method is to use existing knowledge about artifacts, processes, and dependencies. The output of previous assessments, system failures, design, safety, and other processes that an organization is already performing are all elements of existing knowledge. A cyber assessment will consider this information when analyzing the transit agency's capabilities to mitigate threats.

The matrix presented in Table 3-1 can assist in classifying the criticality of systems.

Table 3-1 Potential Impact Definitions for Security Objectives³⁴

Security Objective	Low	Moderate	High
Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., Sec. 3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity: Guarding against improper information modification or destruction; includes ensuring information non-repudiation and authenticity. [44 U.S.C., Sec. 3542]	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability: Ensuring timely and reliable access to and use of information. [44 U.S.C., Sec. 3542]	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

After the Assessment

NIST, CISA, FTA, and TSA recognize that the secure growth of networks is not easy. Many of their products and much of their guidance acknowledges the variability in maturity levels across agencies. These guides can help an organization understand where they are among peers and the next steps to take in the maturation process. Cybersecurity standards and best practices that address interoperability, usability, and privacy seek to enable greater development and application of practical, innovative security technologies and methodologies that enhance resiliency.

Capacity

Capacity planning should lead to the specification of resilience requirements. The factors that determine an organization's capacity needs over time are dependent on its business needs and growth. Some factors that should be considered when creating a capacity management plan include:

³⁴ National Institute of Standards and Technology. 2004. *Standards for Security Categorization of Federal Information and Information Systems*. Federal Information Processing Standards (FIPS) Publication 199, p. 10. <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf>.

- Current utilization—the analysis and metrics can be used to help plan any increase
- Anticipated network growth and contraction to plan the IT roadmap
- Current and historical people, information, technology, and facility projections

System Monitoring

Cybersecurity requires that the trained people, processes, and technologies used in a layered defense strategy be effective. The Security Information and Event Management (SIEM) tools are a set of applications that provide the ability to gather security data from information system components and present that data as actionable information via a single interface. SIEM tools provide an important capability as part of a cyber toolset. At its core, a SIEM system offers a central repository for all security events generated in an enterprise. Modern SIEM solutions include some artificial intelligence capabilities to alert automation and automated behavioral analytics. The analytical components review combinations of events to identify suspicious activity. The system should also deliver incident management and case management functionality from a console to allow analysts to gather and share evidence. The SIEM system must also be able to archive events for forensic analysis of historical events.

SIEM capability supports many other cybersecurity functions within an organization. Since SIEM pulls in logs from multiple sources, it can be used to build a picture of an enterprise. One issue with SIEM is that the outputs are only as good as the data ingested. This is a reason assessors must understand the transit agency's information sharing and data collection practices.

In general, all organizations should work toward an ability to perform continuous monitoring. NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, offers guidance on ISCM program development.³⁵ An ISCM program assessment informs organizational leadership on the effectiveness and completeness of the organization's ISCM program, including a review of ISCM strategies, policies, procedures, operations, and an analysis of continuous monitoring data. The ISCM assessment approach can be used as presented or as the starting point for an organization-specific methodology. It includes example evaluation criteria and assessment procedures that can be applied to organizations.

³⁵ Dempsey, Kelley, Nirali Shah Chawla, Arnold Johnson, et al. 2011. *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*. NIST Special Publication 800-137. National Institute of Standards and Technology, U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf>.

Cyber Threat Information Sharing

NIST defines a cyber threat as:

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.³⁶

Through the exchange of cyber threat information with other sharing community participants, organizations can leverage the collective knowledge, experience, and capabilities to gain a more complete understanding of the threats they may face. Cyber threat information sharing is essential to thwarting successful hacks and minimizing consequences should a breach occur.

Cyber threat information is any information that can help an organization identify, assess, monitor, and respond to cyber threats. Examples of cyber threat information include indicators (e.g., system artifacts or observations associated with an attack), tactics, techniques, and procedures (TTPs), security alerts, threat intelligence reports, and recommended security tool configurations. Most organizations already produce multiple types of cyber threat information that are available to share internally as part of their information technology and security operations efforts. An assessor needs to examine the information being produced and the data being captured to inform the continuous improvement of cyber defenses.

External cyber threat information feeds are valuable especially if they are coming from like entities with similar assets, systems, or networks. The FBI, DHS, and regional threat-sharing organizations often share this information for free. There are a host of subscription-based services selling cyber threat information. The exchange of this data can help organizations keep up with attack methods, trends, and program systems to block the attacks.

CISA promotes cyber threat information sharing for all organizations, categorizing organizations by level of maturity.³⁷

³⁶ National Institute of Standards and Technology. 2012. *Guide for Conducting Risk Assessments*. NIST Special Publication 800-30 Revision 1. U.S. Department of Commerce. http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

³⁷ Cybersecurity and Infrastructure Security Agency. "Cyber Information Sharing and Collaboration Program (CISCP)." Information Sharing. Accessed November 4, 2021. <https://www.cisa.gov/ciscp>.

Category 1: “Emergent”

Stakeholders in Category 1 are consumers of general cyber awareness, security, or risk data and may not have a strong awareness of cyber threats. Generally, this category consists of smaller-sized organizations, but it may contain larger organizations that are just becoming aware of cybersecurity concerns and are beginning a broader investment in cybersecurity. These organizations may be devoting attention to cybersecurity for the first time and may lack the resources and/or requisite knowledge to employ basic cybersecurity measures. They may not generate cyber analytic data and they may perceive their cyber risk profile as low, with limited consequences from potential events.

Category 2: “Developing”

Stakeholders in Category 2 are or can become consumers of technical and/or analytical computer network defense threat or vulnerability data. The stakeholders in this category consist of organizations that have invested resources in building a basic cybersecurity architecture that addresses major risks to their networks and assets. They possess basic security policies and employ generic security practices (i.e., vulnerability assessments, inventory of devices/hardware/software, configuration management, and patch management). They may have a dedicated or matrixed information technology (IT) staff with a remedial to mid-level capability of receiving or acting on threat data. Many may also outsource network and security support.

Category 3: “Established”

Stakeholders in Category 3 are or are able to become consumers and periodically reliable generators of technical and/or analytical computer network defense threat or vulnerability data. The stakeholders in this category can capture and produce threat data with enough volume and reliability to be genuine contributors to collaborative information sharing. These organizations possess enough computer network defense capability and analytical skill to capture their own data and act on the basis of indicators of compromise. They have invested significant resources and staff toward the construct of a cybersecurity architecture that addresses the major risks posed to their networks and assets. They possess mature cybersecurity policies, a robust security architecture, well-trained IT staff, and a security operations center (SOC) that monitors network security. They can detect internal/external threats to their network, and their IT analysts will often understand initial appropriate remediation actions. These stakeholders are typically mid-sized or larger organizations, with a dedicated annual cybersecurity budget but they lack the native ability to enhance or further contextualize threat data.

Category 4: “Advanced”

Stakeholders in Category 4 are or are able to become advanced consumers and consistent generators of industry-led, high-quality technical and/or analytical

computer network defense threat or vulnerability data. These stakeholders generally have a high degree of automated threat action integrated enterprise-wide and operate a full-scale, advanced threat monitoring environment. They are advanced cyber threat data contributors and maintain and operate SOCs and threat intelligence centers. They employ analysts highly capable of discovering and acting on threats posed to the network and they generate advanced actionable and reliable cyber analytical data. These organizations represent significant contributors to information sharing and operate as substantial mentors to other participants via tradecraft training and technical/collaborative analyst exchanges.

Category 5: “Commercial”

Stakeholders in Category 5 represent commercial entities whose primary line of business concerns providing network security, network monitoring, or cybersecurity data and threat intelligence as a service or providing security products in the commercial marketplace. These organizations offer information security services to other businesses and government entities including security operations support, 24/7-managed security services, incident response and forensics, and active threat intelligence data feeds. Stakeholders in this category possess the highest industry standards for security monitoring, analytics, and tradecraft, as well as threat intelligence data production.

Category 6: “Information Sharing and Analysis Organizations (ISAOs)”

Stakeholders in Category 6 allow for broader reach to stakeholders with a particular sector, sub-sector, threat, or business interest. Recognized in the Homeland Security Act of 2002, ISAOs are entities that gather, analyze, communicate, and disclose cyber threat information to members to “help prevent, detect mitigate, or recover from the effects of an interference, compromise, or incapacitation” of its members. ISAOs gather data, tailor analytics, and publish data, information, or best practices that enable their members to draw down risks in a manner most effective to their individual business environment.

For many years, large organizations worked with DHS to share indicators of compromise to ensure the protection of critical infrastructure and major business entities. There is an opportunity now for every company to participate and it was institutionalized through Executive Order 13691 in 2015.³⁸ Any business or organization can create an ISAO and access sharing programs established by DHS.

³⁸ Boyens, Jon, Celia Paulsen, Rama Moorthy, and Nadya Bartol. 2015. *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*. NIST Special Publication 800-161. National Institute of Standards and Technology, U.S. Department of Commerce. <https://csrc.nist.gov/publications/detail/sp/800-161/final>.

Supply Chain

Cyber supply chain risks touch sourcing, vendor management, supply chain continuity and quality, transportation security, and many other functions across the enterprise and require a coordinated effort to address. There are several cyber supply chain security principles:

1. Develop your defenses based on the principle that your systems will be breached. When you start from the premise that a breach is inevitable, it changes the decision matrix for next steps. The question becomes not just how to prevent a breach, but also how to mitigate an attacker's ability to exploit the information accessed and how to recover from the breach.
2. Cybersecurity is never just a technology problem; it's a people, processes, and knowledge problem. Breaches tend to be less about a technology failure and more about human error. IT security systems won't secure critical information and intellectual property unless employees throughout the supply chain use secure cybersecurity practices.
3. Security is Security. There should be no gap between physical and cybersecurity. Sometimes the bad guys exploit lapses in physical security to launch a cyberattack. By the same token, an attacker looking for ways into a physical location might exploit cyber vulnerabilities to gain access.

Purchasing

It is vital to begin a collaboration between security and the purchasing department working with risk. All acquisitions should be assessed for cybersecurity importance early in the requirements definition phase of the acquisition.

Agencies should conduct a high-level criticality analysis of all acquisitions in designated risk categories. This agency-level risk analysis should focus on fit-for-use and should occur as early as possible during the requirements definition process, preferably prior to developing a government cost estimate or obtaining funds for the acquisition. Results of this analysis will dictate:

1. Which cybersecurity controls are appropriate for the acquisition and should be included in the requirements package
2. Which risk decisions are critical for the acquisition
3. The risk owner that will make those decisions

IT acquisitions should have cybersecurity concurrence/approval prior to issuing the solicitation and again prior to contract award. These kinds of analyses can get lost in the assessment of controls, but they are essential to keeping a managed system within the frame of risk tolerance.

Having the proper cybersecurity controls in place does not guarantee the vendor will not introduce vulnerabilities or be a threat to the enterprise. The SolarWinds attack of 2020 was ultimately a supply-chain attack. Customers of the company SolarWinds ingested malware when performing their normal updates provided by the company. It showed the importance of the vendor assuring software development security and it also made customers more cognizant of everything put into their networks. This is even from trusted sources. It has become more important than ever for software users to have processes allowing the burn-in, reversing updates, and network configurations. The ability to roll back to an earlier network configuration or to do a comparison of network activity cannot be overlooked by network assessors.

Supply Chain Agreements

External dependency management focuses on external entities that provide, sustain, or operate information and communications technology (ICT) to support an organization.

One caveat to outsourcing is that organizations can outsource business functions, but they cannot outsource the risk and responsibility to a third party. These must be borne by the organization that asks the population to trust they will do the right thing with their data.³⁹

The assessor should work to understand:

- Does your organization document security objectives in agreements with third parties?
- Does your organization monitor compliance to security objectives in agreements?
- Does your organization document specific security objectives in agreements with third parties?
- Does your organization include measures of cybersecurity performance in third party agreements?
- Does your organization monitor compliance with security objectives in agreements with third parties?
- Is cybersecurity performance considered when selecting third parties?

³⁹ Butkovic, Matthew J. "Cybersecurity SLAs: Managing Requirements at Arm's Length." Presentation at Symposium on Cyber Security Incident Management for Health Information Exchange, Carnegie Mellon University, June 26, 2013. https://resources.sei.cmu.edu/asset_files/Presentation/2013_017_101_54269.pdf.

Section 4

Gap Analysis

Major cyberattacks against SolarWinds, Microsoft, the Colonial Pipeline, and Kaseya have caused significant disruption and cost to the global economy. The transit industry has experienced a number of high-profile attacks that disrupted operations across North America, including the Metropolitan Transportation Authority (MTA) in New York City, Martha's Vineyard Ferry in Massachusetts, Southeastern Pennsylvania Transportation Authority (SEPTA) in Pennsylvania, and TransLink in Vancouver, Canada.

The COVID pandemic exacerbated the escalation in cyberattacks by forcing organizations across the nation to meet new, urgent technology requirements to support remote work. Access to e-mail was no longer the basic need; critical systems had to be remotely accessible as well. In many cases, connections among systems had to be quickly stood up and made available. In meeting these requirements, many organizations turned to cloud computing among other technologies to quickly augment existing technology and communications tools to support remote work. The security of these connections took a back seat to ensuring the systems remained accessible in a remote work environment.

Prior to 2020, most transit agencies followed best practices by managing critical systems with strict requirements that constrained and/or forbade outright access via the unsecure Internet. Some systems required users to physically access certain systems where they stood because they purposely were not networked. This segmentation is no longer practical or feasible in the post-pandemic world.

Cybersecurity//

The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.⁴⁰

As with other industries, cybersecurity risks were growing for transit operators prior to the pandemic as they transitioned to more digital, connected operations. The more access points that a transit operator creates to the Internet, the more vulnerabilities it creates, whether for payment systems or vehicle tracking or other new technologies. COVID only made things worse as it required many in the workforce to access some of these critical systems

⁴⁰ National Initiative for Cybersecurity Careers and Studies. "Cybersecurity Glossary." Cybersecurity & Career Resources. Last Updated July 6, 2022. <https://niccs.cisa.gov/about-niccs/cybersecurity-glossary#C>.

remotely. The success of cybercriminals in exploiting network vulnerabilities has increased the urgency to have an effective cybersecurity program in place, especially for those that provide a critical service such as public transit operators. Proper tools and resources are needed to identify and understand a cyberattack when it occurs. Adequate planning must be in place to support resilience after an incident is identified.

To support organizations in the face of growing cyber threats, the U.S. Congress established the Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security (DHS) in 2018. According to DHS, “CISA is the Nation’s risk advisor, working with partners to defend against today’s threats and collaborating to build more secure and resilient infrastructure for the future.”⁴¹ CISA coordinates a collective defense to identify and vet procedures to manage and reduce the impact from disruption to critical infrastructure. In this role, the organization builds and coordinates relationships across industries working with sector specific agencies, such as the U.S. Department of Transportation (DOT), the Federal Transit Administration (FTA), and the Transportation Security Administration (TSA).

CISA’s role is to unite government and private sector partners, with a particular focus on 16 critical infrastructure sectors:

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.⁴²

The public transit industry is part of the Transportation Systems Sector (TSS), one of these 16 sectors. As such, the industry has direct access to CISA’s capabilities and resources, such as intelligence analysis, data assessment, response methods development, and assistance to manage risks to critical infrastructure that often spike from emerging threats. CISA leads a systematic approach to manage and reduce cyber risk that includes providing services, cyber training, support to critical infrastructure operators, and risk analysis. These tools and services are free to all critical infrastructure entities. CISA products assist critical infrastructure owners and operators in honing their approach to cyber defenses and risk management. No organization can eliminate all cyber risk; however, the risk can be managed more effectively with CISA’s support.

⁴¹ Cybersecurity and Infrastructure Security Agency. “About CISA.” Accessed November 16, 2021. <https://www.cisa.gov/about-cisa>.

⁴² Cybersecurity and Infrastructure Security Agency. “Critical Infrastructure Sectors.” Infrastructure Security. Last Updated October 21, 2020. <https://www.cisa.gov/critical-infrastructure-sectors>.

Underlying CISA's mandate is the work of the National Institute of Standards and Technology (NIST), specifically the NIST Cybersecurity Framework (CSF).⁴³ The NIST CSF is the bedrock of U.S. cybersecurity policy and support. Almost all organizations leverage aspects of NIST's work in their cybersecurity programs. In addition to the CSF, NIST has developed several detailed frameworks and tools to standardize and support cybersecurity program development.

Beyond the NIST CSF, the ISO 27000 family of standards is another framework that cybersecurity professionals use to guide development of their programs. The NIST CSF is broadly promoted to critical infrastructure owners and operators in the United States. The ISO 27000 series provides guidance on how to implement a cybersecurity program leading to organizational security standards and is relied upon mostly outside the United States. Developed as instructed from a 2013 Presidential Executive Order, the NIST CSF is free.⁴⁴ ISO standards are not. As cost is a factor to implementing cybersecurity best practices, the CATT project team is focusing on opportunities to leverage the NIST suite of frameworks and guidance.

CISA has developed cybersecurity assessment tools in partnership with other government agencies such as NIST, industry experts, and other private sector partners. The overall objective of a cybersecurity assessment is to determine the effectiveness of an organization's defenses and assess its resilience capabilities—an important launch pad for building resilience in any organization.

Review of Cyber Assessment Tools

To effectively understand cyber risk, public transit agencies must first assess their risk against a baseline. Many tools exist that allow agencies to assess their existing infrastructure relative to best practices as defined outside the public transit industry. When it comes to cybersecurity, much is the same across industries. The cybersecurity assessment process analyzes cybersecurity controls and capabilities to identify, detect, protect, respond, and recover from disruption.⁴⁵

Best practices have been developed in recent years by experts and practitioners from around the world to ensure the security teams have visibility into both the current state of the threat and the current state of an organization's vulnerabilities. Traditional cyber threat intelligence serves as a key input.

⁴³ National Institute of Standards and Technology. "Cybersecurity Framework." Accessed November 27, 2021. <https://www.nist.gov/cyberframework>.

⁴⁴ National Institute of Standards and Technology. "History and Creation of the Framework." Cybersecurity Framework. Last Updated November 21, 2019. <https://www.nist.gov/cyberframework/online-learning/history-and-creation-framework>.

⁴⁵ National Institute of Standards and Technology. 2018. *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.1*. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

Standards organizations such as NIST, CISA, and ISO have laid out frameworks, tools, and other resources to equip organizations to effectively mature their cybersecurity posture. The consensus is that implementation of these best practices lowers cyber risks.⁴⁶

Though most of the systems in a transit agency environment resemble those in other industries, the network architecture and protection of critical functions serve a particularly prominent role in defining their cyber posture when compared to other industries. Vulnerabilities must be identified; existing tools, resources, and technologies in use must be understood; and risks must be assessed relative to the unique network architecture and safety requirements of the public transit industry. It is essential that cyber assessments are conducted in the context of each agency's current unique operating environment.

When it comes to managing cyber risk, every industry has its unique characteristics, and the transit industry is no different. Transit is a people-centric environment and is historically heavily OT dependent. Like most industries over the past decade, the transit environment has become more Internet-technology reliant.

When compared to other industries, the transit industry differs in some key priorities. The physical safety of transit passengers and operators, as well as the heavy reliance on OT systems to deliver a dependable, secure, and critical service for the community, is paramount.

IT teams have inherited equipment and systems that existed prior to modern networking and system management technology. The challenge is to effectively and efficiently integrate IT and OT systems while maintaining a secure environment. The newly interconnected systems make attacks possible that have the potential to undermine safety mechanisms. The cyber-physical environment poses unique challenges. When assessing an agency's cyber posture, attention must be paid to characteristics of known attack vectors and the system's ability to withstand a debilitating event. In addition, the cyber-physical environment continues to evolve with the growing breadth of communication technologies employed and the emergence of connected and autonomous vehicles.

Cybersecurity is at its foundation a form of risk management. To effectively manage risk, the organization must have a clear understanding of its risk tolerance and an acute visibility into how its resource investments and other decisions are moving the needle closer to or farther away from this threshold. Critical to this risk analysis is a proper understanding of the impact of an organization's security practices, attained and achieved through ongoing and regular assessment.

⁴⁶ Belcher et al., *op cit.*

The prevailing rationale and impact for utilizing assessment tools will vary across organizations based on various factors. Some operators employ an assessment to lay a foundation for a more formal cyber risk management program. Other operators use an assessment to enhance and mature an existing program. All assessment use cases, however, employ an enumerated set of defined tactics and processes, rooted in a well-defined framework connected directly to the organization's mission. While there are many assessment tools that can support different cyber resilience frameworks, none are honed to provide the small to mid-sized transit agency the most accurate view of its cyber posture.

Maturity Models

Cybersecurity is not a project; it requires a System Development Life Cycle approach (SDLC), whereby incremental improvements are made over time. To facilitate this approach, many assessment tools leverage maturity models to describe the incremental progress from a weaker posture to a more mature, stronger program to ensure effective cyber resilience. A maturity model is a framework used to establish targets for comparison to others inside and outside the industry through the lens of the assessed organization's processes and capabilities. Maturity models evaluate a given risk assessment and provide paths to optimize the current posture through such comparisons to others. The strategies are rooted in maturity by which an organization can measure and adjust its cyber posture. An assessment of an organization's maturity level helps determine its security posture relative to its risk tolerance and in comparison to peers, and it establishes a snapshot of current cybersecurity practices—essential for constructing a baseline and a roadmap to strengthen the security posture.

Because public transit agencies are part of the TSS and of critical concern to the federal government, there are considerable resources available to them. One of the most valuable is the TSS Cybersecurity Framework Implementation Guidance and its companion workbook, which provides an approach for TSS members to apply the tenets of the NIST Cybersecurity Framework to their organizations. CISA provides that:

A maturity model is a framework used to establish targets for comparison when looking at an organization's processes. It evaluates capability and implements strategies based on level of acceptable risk. An assessment of an organization's maturity level helps determine its security posture and establish an accurate snapshot of its current cybersecurity practices, which is essential for constructing a baseline for framework implementation. Maturity models provide an internal benchmark that an organization can utilize to measure capabilities of structural practices, assess processes and methods currently implemented, establish allocation of resources,

and establish goals and priorities for enhancements. When used correctly, maturity models create a snapshot of an organization's present cybersecurity posture and identify areas of opportunity for enhancement.⁴⁷

The purpose of the TSS Cybersecurity Framework is to assist organizations within the sector to characterize their current cybersecurity posture, identify opportunities to improve their program, identify existing tools, standards, and guidelines that can support implementation, and assess and communicate their approach to internal and external stakeholders. Though helpful, the framework is not prescriptive.

Another prevailing maturity framework that is driving activity among other industries is the Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC). This program requires all defense contractors and service providers to assess their cybersecurity maturity against a common framework and certify that assessment as part of any procurement or related contract.⁴⁸

More specific to public transit, APTA's Control and Communications Security Working Group (CCSWG) is developing the Operational Technology Cybersecurity Maturity Framework (OT-CMF) for Surface Transportation Industry. When completed and approved, the goal is that this framework will ensure agencies develop and demonstrate compliance with cybersecurity requirements by using a standardized program tailored to surface transportation needs across OT environments.

⁴⁷ U.S. Department of Homeland Security. 2015. *Transportation Systems Sector Cybersecurity Framework Implementation Guidance*. https://www.cisa.gov/sites/default/files/publications/tss-cybersecurity-framework-implementation-guide-2016-508v2_0.pdf.

⁴⁸ U.S. Department of Defense. "Securing the Defense Industrial Base: CMMC 2.0." Acquisition and Sustainment. Accessed October 22, 2021. <https://www.acq.osd.mil/cmmc/>.

Section 5

Cybersecurity Resilience Review

The project team evaluated numerous cybersecurity assessment tools (noted in Appendix C). The intent of this review was to assess the tools available to provide a basis for the Cybersecurity Assessment Tool for Transit (CATT, or Assessment Tool), as well as to guide the team in adjusting the base assessment tool to address the key risk priorities of public transit agencies. Tools that focused on measuring an organization's maturity were considered, but the project team determined that for small and mid-sized transit agencies, the primary objective is to help them understand the outcomes of improper cyber practices, known vulnerabilities, and unclear responsibilities.

Given the above, the project team identified a base assessment tool produced by CISA called the Cybersecurity Resilience Review (CRR) and chose it as the foundation for CATT. The CRR is a no-cost, voluntary, non-technical assessment of an organization's cybersecurity practices and posture. It goes beyond assessing an organization's cybersecurity practices by also evaluating an organization's operational resilience.

Considering the critical nature of public transit agency services and the growing threat of disruptive incidents, all transit agencies, no matter the size, have the responsibility to provide effective transit services and assure the safety of stakeholders. Agencies must understand their cyber posture and the threat vectors that can undermine service, safety, and security.

The original CRR was created based on the Community Emergency Response Team (CERT) Resilience Management Model (CERT-RMM) by the CERT Division at Carnegie Mellon University's Software Engineering Institute (SEI). The tool was designed as a capability-focused maturity model for process improvement. Its goal is to assist government and private sector entities in managing operational resilience across the disciplines of security management, business continuity management, and information technology operations management.⁴⁹

The Cybersecurity Resilience Review may be conducted as a self-assessment. Though technical in some areas, most small and mid-sized public transit agencies have the staff to at least oversee its use. In addition, because of the public transit industry's status as part of the TSS, CISA makes resources and analysis available to directly support assessments using the CRR tool.⁵⁰

⁴⁹ Caralli, Richard A., Julia H. Allen, David W. White, et al. 2016. *CERT Resilience Management Model, Version 1.2*. Software Engineering Institute, Carnegie Mellon University. <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084>.

⁵⁰ Cybersecurity and Infrastructure Security Agency. "Transportation Systems Sector." Critical Infrastructure Sectors. Accessed November 2, 2021. <https://www.cisa.gov/transportation-systems-sector>.

The CRR assesses programs and practices across a range of 10 domains. The assessment is designed to measure existing organizational resilience as well as provide a gap analysis for improvement based on recognized best practices. The CRR captures an understanding and qualitative measurement of an organization's ability to adapt to risk that affects the organization's core operational capacities. It also highlights the organization's ability to manage operational risks to critical services and associated assets during normal operations and during times of operational stress and crisis.

The results of the CRR can be used to evaluate the agency's environment independent of other assessments being used by the entity such as penetration tests or other more technical assessments. Many of the risk management programs employ multiple tools such as CISA's Tabletop Exercise Package (CTEP)⁵¹ to build a common, thorough perspective on resiliency and overall risk. The key goal of the CRR is to ensure that core process-based capabilities exist, are measurable, and are meaningful as predictors to understand an organization's cyber posture.

Use of the CRR as a Foundation

The project team used the CRR as the baseline tool for CATT for several reasons. One objective was utilizing an assessment method to infuse with current knowledge about threats and operational transportation standards. Of the many assessment tools available (noted in Appendix C), some charge fees but CRR does not. In addition, others are more technology-focused and lack the resilience focus found among CRR's question set. The fact that the CRR is a no-cost, voluntary assessment to evaluate an organization's operational resilience and cybersecurity practices together also made it an ideal choice to serve as the basis for CATT. Given that it was developed by DHS, the CRR is not only available for enhancement, but such improvements are also welcomed and supported by its creators.

The CRR is widely accepted as a tool to assess vulnerabilities leading to an understanding of resilience. Much of the mapping between NIST standards and controls has been done by DHS and NIST. Organizations such as MITRE have also played a role in identifying the usability of CRR. The CRR has the backing of government, the private sector, and academic institutions, all advocating its use at critical infrastructure entities. This foundational support will be leveraged to promote CATT's utility to the public transit industry.

Figure 5-1 shows the CRR domains for cyber assessment. For CATT, the domains remain the same, but two topic areas were reinforced given the nature of public transit: Operational Technology and Safety Management Systems.

⁵¹ Cybersecurity and Infrastructure Security Agency. "CISA Tabletop Exercises Packages." Critical Infrastructure Exercises. Accessed October 17, 2021. <https://www.cisa.gov/publication/cisa-tabletop-exercise-package>.

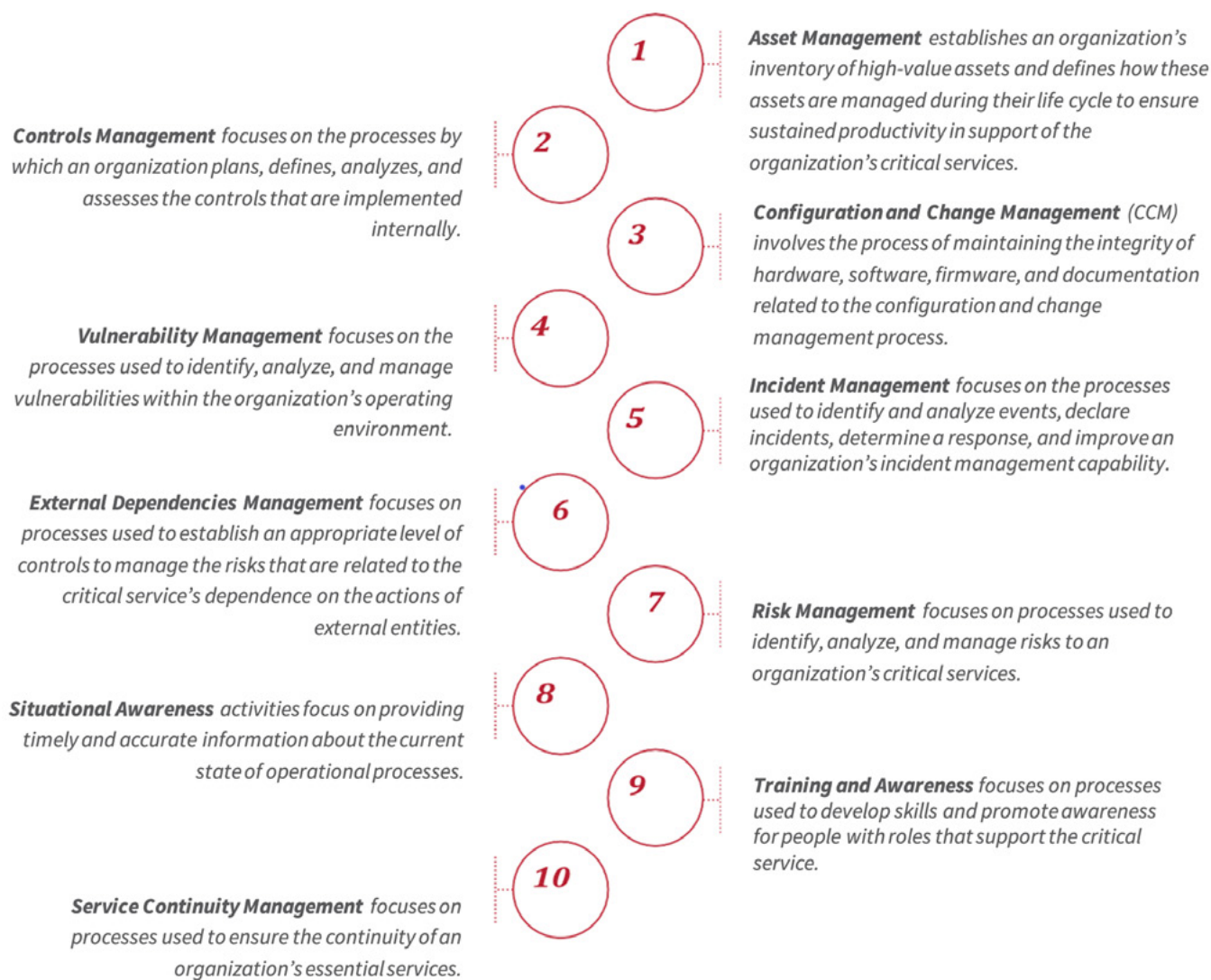


Figure 5-1 Cyber assessment: Cyber Resilience Review (CRR) domains

Section 6

Enhancing the CRR

The project team chose to build upon the CRR to deliver an Assessment Tool customized for the public transit industry. The 299 questions of the CRR create an opportunity to leverage work by cybersecurity experts across government, industry, and academia, led by DHS and CISA. Cybersecurity Resilience Review provides an ideal foundation given its coverage of both cybersecurity practices and attention to resilience.

Using the CRR as a baseline, the project team developed CATT to address the needs of the public transit industry. CATT addresses opportunities to focus the CRR given the state of cybersecurity in public transit and provides more fidelity and alignment to the specific needs of the industry. The output of this methodology will be an effective, refined assessment tool specifically calibrated for the unique needs and context of the public transit industry.

Primary Resources

To inform the methodology for enhancing the CRR, the project team identified a robust set of inputs to guide customization for the public transit industry.

NIST

NIST has developed a number of detailed cybersecurity standards, guidelines, best practices, and resources to meet the needs of U.S. industry, federal agencies, and the broader public. The work of NIST is defined and assigned by federal statutes, executive orders, and policies—including developing cybersecurity standards and guidelines for federal agencies. NIST's cybersecurity program supports its overall mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and related technology through research and development.

NIST creates the baseline for cybersecurity standards and works closely with organizations in the public and private sectors to ensure that information can be readily leveraged to address specific cybersecurity issues faced today. Cybersecurity standards and best practices established under the NIST umbrella that address interoperability, usability, and privacy continue to be critical for the nation. Across their many programs and working groups, NIST enables greater development and practical application of innovative security technologies and methodologies to better address current and future computer and information security challenges.

The project team reviewed the NIST portfolio of standards and guidance for assessments, risk management, resilience, and information security. In addition to the NIST Cybersecurity Framework, the team employed:

- Risk Management Framework for Information Systems and Organizations (SP 800-37 Rev. 2)⁵²
- Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans (SP 800-53A Rev. 4)⁵³
- Developing Cyber Resilient Systems: A Systems Security Engineering Approach (SP 800-160 Vol. 2)⁵⁴
- Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems⁵⁵

MITRE ATT&CK

MITRE ATT&CK (MITRE) is a globally accessible knowledge base of cybersecurity adversary tactics and techniques based on real-world observations: “The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, government, and the cybersecurity product and service community.”⁵⁶

Researchers and cyber professionals around the world contribute to the database. Information and details related to method and mitigation are openly shared. As attackers make specific moves, the actions and documented practices can be better counteracted based on past observed behavior.

The MITRE ATT&CK framework details numerous techniques that an attacker can use to achieve several different goals. MITRE suggests asking the following questions:

- What behaviors are most common?
- What behaviors have the most adverse impact?
- For what behaviors is data readily available?
- Which behaviors are most likely to indicate malicious behavior?⁵⁷

⁵² National Institute of Standards and Technology. 2018. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. NIST Special Publication 800-37 Revision 2. U.S. Department of Commerce. <https://doi.org/10.6028/NIST.SP.800-37r2>.

⁵³ National Institute of Standards and Technology. 2014. *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*. NIST Special Publication 800-53A Revision 4. U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>.

⁵⁴ Ross, Ron, Victoria Pillitteri, Richard Graubart, et al. 2019. *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*. NIST Special Publication 800-160 Volume 2. National Institute of Standards and Technology, U.S. Department of Commerce. <https://doi.org/10.6028/NIST.SP.800-160v2>.

⁵⁵ FIPS Publication 199, *op cit*.

⁵⁶ MITRE ATT&CK. Accessed November 11, 2021. <https://attack.mitre.org/>.

⁵⁷ Strom, Blake E., Joseph A. Battaglia, Michael S. Kemmerer, et al. 2017. *Finding Cyber Threats with ATT&CK™-Based Analytics*. Technical Report MTR170202, MITRE Corporation. <https://www.mitre.org/sites/default/files/2021-11/16-3713-finding-cyber-threats-with-attack-based-analytics.pdf>.

The project team used real-world attack methods as categorized and defined by MITRE to inform the assessment for managing risk. This additional level of detail enables public transit agencies to build a program informed by strategies and tactics given specific attack methods.

APTA

Standards are an important program activity of APTA and in the public transportation industry. Through its Standards Policy and Planning Committees, APTA plays a major role in creating active working structures among public transit agencies focused on the development of standards. Several hundred industry volunteers serving on numerous working groups have developed standards for bus transit, rail transit, commuter rail operations, maintenance, design, procurement, security, safety, technology, and sustainability.

APTA has more than 26 active working groups developing standards and best practice documents. Two working groups focus on cybersecurity specifically, the Control and Communications Security Working Group (CCSWG) and the Enterprise Cybersecurity Working Group (ECSWG).

The CCSWG focuses on OT and draws upon existing standards from the North American Electric Reliability Corporation Critical Infrastructure Protection program (NERC CIP), NIST, Internet Security Alliance, the Institute of Electrical and Electronics Engineers (IEEE), physical security knowledge, and logical/administrative security.

The ECSWG develops APTA standards pertaining to mass transit cybersecurity. Specifically, it provides strategic recommendations for chief information officers and decision-makers regarding business cybersecurity, information systems, fare collection, and general cybersecurity technologies.

Key Opportunities for Enhancement

Leveraging CISA guidance, NIST resources, MITRE, and APTA research, the project team enhanced the CRR with a focus on the needs of small and mid-sized public transit agencies. To address CRR weaknesses given its broad focus, the following key dimensions were identified from a thorough survey and review of available materials. These dimensions served as a guide for the project team to identify opportunities for improvement among the existing CRR questions.

- **Frequency** is defined as “the rate of a repetitive event.”⁵⁸ Organizations are not static. The CRR was originally designed to assess a cybersecurity

⁵⁸ Computer Security Resource Center. “Glossary.” National Institute of Standards and Technology, U. S. Department of Commerce. Accessed October 27, 2021. <https://csrc.nist.gov/glossary/term/frequency>.

program at a point in time. True assessment requires a stable cadence of understanding over time. The Assessment Tool was designed to assess events that take place on a reoccurring basis such as bus communications with the operations center and electronic payment systems.

- **Quality property** of a cybersecurity program is defined as an “emergent property of a system that includes, for example: safety, security, maintainability, resilience, reliability, availability, agility, and survivability. This property is also referred to as a *systemic property* across many engineering domains.”⁵⁹ Given the project team’s understanding of the specific risk priorities for public transit, many opportunities exist to enhance the CRR questions in the Assessment Tool to drive maturation of a higher quality cyber risk program.
- **Depth** of an attribute associated with an assessment method addresses the rigor and level of detail associated with the application of the method.⁶⁰ Given the broad focus of the CRR, many opportunities exist to enhance the Assessment Tool by guiding assessors to go deeper in certain areas that are specific to public transit than the CRR is designed to take them.
- **Control parameter** is the means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of an administrative, technical, management, or legal nature—an attribute assigned to an asset that reflects its relative importance or necessity in achieving or contributing to the achievement of stated goals.⁶¹ Given the project team’s understanding of the fundamental goals and priorities of the industry, an understanding of control priority for the public transit industry was leveraged to enhance CRR questions in the Assessment Tool.
- **Classification security categorization** provides a structured way to determine the criticality and sensitivity of the information being processed, stored, and transmitted by an information system based on the potential impact.⁶² Given the unique safety requirements, among other factors, the project team injected its understanding of criticality and sensitivity to key systems as part of its question enhancement process.

Vetting the questions of the CRR improves cyber assessments for small and mid-sized public transit agencies. Equally important is reviewing the underlying output from assessment questions to identify opportunities for equipping transit leaders with the best information available to inform maturation of their cybersecurity program. This assures a stronger assessment foundation.

⁵⁹ Ross et al., *op cit.*

⁶⁰ NIST Special Publication 800-53A Revision 4, *op cit.*

⁶¹ NIST Special Publication 800-37 Revision 2, *op cit.*

⁶² FIPS Publication 199, *op cit.*

Understanding “Criticality”

Understanding the criticality of systems and data is tremendously important. If a system is depended on by or parallel to a safety system, it has high criticality. In effect, the parts inherit the criticality of the most critical, connected component—the adage “the chain is as strong as its weakest link.” Therefore, the overall security impact level of the information system must be determined by examining the full architecture and review of system management.

Simply asking similar questions of each system (critical high and critical low) as if they are equal and independent may impact the initial set of security controls chosen by the transit agency. Notably, while benefitting all stakeholders, these characterizations will be particularly important to the small and mid-sized organizations, as they enable a more effective deployment of limited resources. Such activities can have an outsized input to prioritizing and optimizing otherwise limited resources.

Emphasis on Two Transit-Specific Topic Areas

Cyber Resilience Review is made up of 10 domains that cover the broad areas an organization must assess to ensure the security of its assets, systems, and networks, with a particular focus on IT systems. The project team incorporated question sets for two additional topic areas into the existing 10-domain CRR framework for CATT. These points of emphasis enable the assessor to be more exact in understanding risks and address a key priority for all public transit agencies—ensuring the safety and security of its passengers, employees, and stakeholders.

Operational Technology

Operational Technology (OT) is “the hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes, and events.”⁶³

A transit agency is a complex organization that has assets and equipment controlled by supervisory systems with communications mechanisms throughout its network, in stations, and along railroad tracks. The vulnerabilities and best practices for securing OT systems or hybrid OT/IT systems are different than pure IT systems. New threat vectors include exploits that are now embedded with the components of devices not designed to be secured in hybrid OT/IT environments. This has opened a new set of concerns related to OT security. By including OT functions, the Assessment Tool ensures that assessors fully understand the underlying vulnerabilities given this nuance. In the transit agency, OT considerations are paramount.

⁶³ Gartner, *op cit.*

Industrial control system (ICS) is an information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.⁶⁴

Today, widely available software applications and Internet-enabled devices have been integrated into most industrial control systems (ICS), delivering many benefits but also increasing system vulnerability. Sophisticated malware that targets weaknesses in ICS is on the rise, posing a significant threat to U.S. national security and public transit agencies specifically.

Safety Management Systems

A Safety Management System is a formal top-down, organization-wide approach to managing safety risk and assuring the effectiveness of a transit agency's safety risk mitigation.⁶⁵

Public transit agencies have long relied on Safety Management Systems to ensure the physical safety of their riders, employees, vehicles, and systems. Such critical systems cannot afford failure, so “fail safe” technologies, processes, and procedures have been implemented. In transit, safety is a critical function.

In some cases, safety systems utilize common communication paths and technologies with a transit agency's IT and OT functions. Much of this infrastructure predates the rise of IT; however, due to the cost savings of architecture opportunities, many of these systems take advantage of the broader capabilities IT technologies provide. Mitigating these vulnerabilities will require organizations to understand the mapping of safety functions and commit to limiting their dependency on easily disrupted systems. When vulnerabilities are identified, they must become high-priority items. An awareness of the safety dependencies and potential impacts from cyber disruption will support resilience.

The mechanisms underpinning safety systems must be identified and protected. IT capabilities aligned with them are susceptible to hacking. Even system misconfigurations can create vulnerability for these connected systems. And, while many cyberattacks may emanate from external sources, transit agencies, just like any other organization, are susceptible to attacks

⁶⁴ Computer Security Resource Center. “Glossary.” National Institute of Standards and Technology, U.S. Department of Commerce. Accessed October 29, 2021. <https://csrc.nist.gov/glossary/term/ICS>.

⁶⁵ Part 673 – Public Transportation Agency Safety Plans. C.F.R. Title 49, Subtitle B, Chapter VI (2022). <https://www.ecfr.gov/cgi-bin/text-idx?SID=20f3bb5f4394f0bfe0b35d9afe62de88&mc=true&node=pt49.7.673&rgn=div5>.

from internal sources. Attacks from an internal source, such as a disgruntled employee, have higher probabilities of success. A greater level of access and system familiarity gives an employee knowledge about system weakness. Therefore, physical access to safety systems is not necessary to disrupt them.

The increase in interconnected systems and software-based communications that link safety systems can undermine a transit agency's stability and pose a risk. One goal should be to minimize a successful cyberattack on the agency as a strategy to protect safety systems because such attacks can cascade to impact critical safety systems.

Agencies with Rail Networks

Part 270 of C.F.R. Title 49 requires that the railroad's system safety program be a structured risk reduction program with proactive management processes and procedures to identify and mitigate or eliminate hazards and the resulting risks on the railroad's system including a holistic view of organizational structure and positive safety culture.⁶⁶

U.S. transit agencies have done a great job of developing a culture of physical safety. This culture includes specifications for training, measuring, reporting, analyzing, assessing, and technique awareness. Cyber exploits can undermine these safety gains by both disrupting service and causing injury when functions do not operate as planned.

Effective cyber assessments are a first step to understanding the implication of cyberattacks on safety systems. The increased liability and safety risks from disabled safety mechanisms can be mitigated. It is important, however, that the interdependency of safety systems on IT and OT systems are clearly understood.

CATT Structure

In addition to improving the content of the questions, the project team identified opportunities to iterate on the structure of the CRR to make it more effective and consumable for small and mid-sized public transit agencies. The primary goal of the edits was to reduce the assessment complexity to enable even the smallest, most resource-constrained organizations to learn more about their cybersecurity environment and the steps needed to build resilience into their organizational practices. CATT improves on the CRR in three key areas.

⁶⁶ Part 270 – System Safety Program. C.F.R. Title 49, Subtitle B, Chapter II (2022). <https://ecfr.federalregister.gov/current/title-49/subtitle-B/chapter-II/part-270>.

First, as currently written, the CRR questions offer only three response options—“yes,” “no,” and “incomplete.” The challenge, especially in the realm of cyber risk and security, is that there will always be gradations to each of these answers, especially the “incomplete” option. Instituting cyber risk management and resilience practices would never reach a point of completion for any organization—the risk evolves on a daily basis. Therefore, the project team devised a question set for CATT—using the existing CRR domains—that asks assessors to select the answer that most closely aligns with the type of action or policy (if any) that the transit agency currently has in place. For example, instead of answering “incomplete” to the question “do you have a policy governing asset management,” CATT offers a “no” option and four different maturity levels of “yes.” In this case, the answer may be “yes, my organization has a policy governing asset management,” but it may not be a policy that is documented, reviewed, and distributed. An organization that has the policy *and* takes the additional steps to put it into use and communicate the policy would select one of the “yes” options that corresponds to a higher level of maturity.

The more precise responses are intended to assess and identify what organizations are doing, even if it is not enough. Especially for organizations early in the process of instituting cybersecurity best practices, the existing CRR assessment can result in a final report that is a sea of red—indicating that everything in every domain needs immediate attention. This is not helpful because it does not offer any form of prioritization. The tiered, maturity-based responses used in CATT will help transit agencies provide more precise answers, get assessment “credit” for the responsible practices they already have in place, and generate a report that demonstrates the “green,” “yellow,” and “red” status of operations within the context of the organization’s size and beginner-level cyber posture.

Second, completing the CRR requires a separate document providing guidance for each question; CATT embeds the definitions of key terms throughout the assessment to help respondents better understand the intent of the question set and to allow for quick, efficient term clarification. The CRR is described as “non-technical,” but much of the language associated with any cybersecurity and resilience review has a technical bend to it that a cyber or assessment novice may find challenging. Learning the language of a cyber assessment is part of the cyber education process for individuals and organizations alike; the inclusion of a glossary built into the text is meant to make the learning process less cumbersome.

Third, as a tool tailored to the needs of transit agencies, the project team incorporated language and examples in the assessment text that are familiar to public transit professionals. The critical nature of the services delivered, for example, are taken into account, as is the industry’s increasing reliance on third-party vendors for certain technical capabilities, including fare payment

and video surveillance systems. An additional component of making the tool more transit-specific is the inclusion of question sets focused on operational technology within public transit environments and the central importance of safety to the critical service delivery.

Summary and Findings

Cybersecurity should be considered a fundamental element of any public transit operation. The process of getting there, however, requires a level of investment, expertise, and commitment that can feel beyond the reach of any organization, but especially a smaller transit agency. Whether a transit agency wants to mature an existing program or build one where nothing currently exists, the assessment process is the place to begin.

The process of completing a cybersecurity assessment and its outcome will generate actionable information from which transit executives, IT teams, and cybersecurity professionals can both learn and develop a prioritized list of next steps. Existing assessment tools, including the CRR and the NIST CSF, are intended to help organizations, regardless of industry, accelerate their adoption of best cyber practices and identify gaps that must be addressed to improve the organization's resilience. What the project team found, however, is that these tools do not effectively prioritize next steps for organizations that are new to cybersecurity. The overwhelmingly "red" results confirm what the organization generally already knows—they have work to do.

CATT was specifically designed to fill this gap for resource-constrained transit agencies. There will be areas on the final report that show up "red," but based on the reimagined question format and transit-focused additions to this CRR-based tool, any transit agency that uses the tool as a starting point for its cybersecurity program will come away with the insights needed to take an informed next step. CATT will help transit leaders align their resources with their risk tolerance and inform the important cybersecurity work needed to better secure critical transportation infrastructure.

Understanding the NIST System

The National Institute of Standards and Technology (NIST) is an arm of the U.S. government charged with developing standards and measurements across many areas of U.S. society and responding to the need for research of emerging topics affecting critical infrastructure. The NIST role is non-regulatory, and this allows them to partner with the private sector and academia to produce technology, standards, and metrics that drive innovation.

For cybersecurity subjects, NIST publishes the Special Publication 800-series, which provides guidance documents and recommendations. NIST standards and guidance documents align the best practices with security and privacy controls.

Using NIST products will help a transit agency understand cybersecurity best practices, manage cyber risks, and approach network assessments and monitoring in a systematic way.

Security Controls

To implement a desired state or capability, an organization will put in place a set of security controls. A great example of one might be if an organization wants to secure endpoints. Several controls can contribute to build this capability. Assessments using security controls can allow for a more consistent, comparable, and repeatable approach to understand risks. Controls contribute to the breadth of an organization's understanding of its capabilities to manage cyber risks. Some controls have a higher level of criticality such as those that look at safety systems. Others are important but may relate to the operations of a non-critical system like public Wi-Fi access. An assessor needs to understand the totality of the network architecture because, in some cases, an organization may be using the Wi-Fi for connection to a critical system.

The sequencing of control in an assessment may also assist an assessor to better understand the systems being reviewed. The construct of controls to create a capability helps to assess the severity of vulnerabilities discovered in a system. Ultimately, if there is a failure associated with a vulnerability or the decision not to deploy a certain control affects the overall capability needed for mission/business protection. Assessors should be aware that control interaction may impact the and contribute to the complexity of understanding the outcome of an assessment.

Cybersecurity Framework (CSF)

The NIST Cybersecurity Framework (CSF) is a risk-based approach to managing cybersecurity risk, allowing framework elements to reinforce the connection between business drivers and cybersecurity activities. The Framework was developed to complement, not replace, an organization's established risk

management process and cybersecurity program. An organization can use its current processes and leverage the Framework to identify opportunities to strengthen and communicate its management of cybersecurity risk while aligning with industry practices. For organizations with no formal cybersecurity program in place, the Framework can provide a foundation upon which to implement a robust cybersecurity program. The outputs from the cybersecurity assessment are input into the NIST CSF.

The Framework is composed of three parts:⁶⁷

Framework Core: The cybersecurity activities describe desired outcomes and references critical infrastructure sectors. The Core, broken into five functions, presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The functions are described as follows:

- Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Framework Tiers: These tiers provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. The tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe increasing levels of effort and detail to integrate cyber risk management practices into an organization's overall risk management approach based on business need.

Framework Profile: The profile represents the outcomes based on business needs, risk tolerance, and resource requirements that an organization has selected from Framework categories and subcategories. To ensure adaptability and enable technical innovation, the Framework is technology neutral. The Framework relies on a variety of existing standards, guidelines, and practices to advance critical infrastructure providers to achieve resilience.

⁶⁷ NIST "Cybersecurity Framework," *op cit.*

Cyber Resources for Transit

Cyber Hygiene: Vulnerability Scanning: Vulnerability Scanning helps secure Internet-facing systems from weak configuration and known vulnerabilities, and encourages the adoption of modern security best practices. CISA performs regular network and vulnerability scans and delivers a weekly report for your action. Once initiated, this service is mostly automated and requires little direct interaction. After CISA receives the required paperwork for Cyber Hygiene, their scans will start within 72 hours and you'll begin receiving reports within two weeks.

Phishing Campaign Assessment (PCA): measures your team's propensity to click on e-mail phishing lures. Phishing is commonly used to breach an organization's network. The assessment occurs over a six-week period, and the results can provide guidance for anti-phishing training and awareness.

Risk and Vulnerability Assessment (RVA): allows you to select from a menu of several network security services, including:

- network mapping and vulnerability scanning
- phishing engagements
- web application or database evaluations
- a full penetration test

The assessment period differs by the number and type of services requested, but a typical RVA occurs over a two-week period. There is one week of testing from the Internet and one week of evaluation, at your location, internal to your network.

(NOTE: After CISA receives the required paperwork for an RVA, you will be prioritized based on national mission needs, number of prior stakeholders in your sector, etc. CISA is taking proactive steps and creating new services, such as remote penetration testing, to assist stakeholders with security relevant issues.)

Validated Architecture Design Review (VADR): evaluates your systems, networks, and security services to determine if they are designed, built, and operated in a reliable and resilient manner. VADRs are based on standards, guidelines, and best practices and are designed for Operational Technology (OT) and Information Technology (IT) environments.

A VADR includes:

- Architecture Design Review
- System Configuration and Log Review
- Network Traffic Analysis

Other Resources

- American Public Transportation Association (APTA)
 - <https://www.apta.com/research-technical-resources/safety-security/cybersecurity-resources/>
- Cybersecurity and Infrastructure Security Agency (CISA)
 - <https://www.cisa.gov>
 - <https://us-cert.cisa.gov/ncas/current-activity/2021/06/30/cisas-cset-tool-sets-sights-ransomware-threat>
 - <https://www.cisa.gov/ict-supply-chain-toolkit>
- Federal Bureau of Investigation
 - <https://www.dsac.gov/topics/cyber-resources>
- SAE
 - <https://www.sae.org/cybersecurity>
- Transportation Security Administration (TSA)
 - <https://www.tsa.gov/for-industry/surface-transportation-cybersecurity-toolkit>

Set of Cyber Assessment Tools Reviewed

- [Axio Cybersecurity Program Assessment Tool](#)
A free assessment tool that assists in identifying an organization's cyber posture.
- [Baldrige Cybersecurity Excellence Builder](#)
A self-assessment tool to help organizations better understand the effectiveness of their cybersecurity risk management efforts and identify improvement opportunities in the context of their overall organizational performance.
- Cohesive Networks' [Putting the NIST Cybersecurity Framework to Work](#)
A guide for using the NIST Framework to direct best practices for security audits, compliance, and communication.
- [Facility Cybersecurity Framework \(FCF\)](#)
An assessment tool that follows the NIST CSF and helps a facility manage cyber security risks in core OT and IT controls.
- FINSECTECH's [Cybersecurity Framework as a Service](#)
A user-friendly Framework management tool.
- Information Systems Audit and Control Association's [NIST Cybersecurity Audit Program](#)
An audit program based on the NIST Cybersecurity Framework. It covers sub-processes such as asset management, awareness training, data security, resource planning, recovery planning, and communications.
- Rival Security's [Vendor Cybersecurity Tool](#)
A guide to using the Framework to assess vendor security.
- The DHS Cyber Resilience Review (CRR)
The CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices.
- The Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team's (ICS-CERT) Cyber Security Evaluation Tool (CSET) [download](#), [fact sheet](#), [introductory CSET videos](#)
- The Cyber Security Evaluation Tool (CSET) is a software tool for performing cybersecurity assessments of an organization's enterprise and industrial control cyber systems. It was designed to help asset owners identify vulnerabilities and improve the organization's overall cybersecurity posture by guiding them through a series of questions that represent network security requirements and best practices.
- Robert H. Smith School of CyberChain Portal-Based Assessment Tool
Provided guidelines to measure and assess cyber supply chain risk; no longer available.



Appendix D

Cybersecurity Assessment Tool for Transit (CATT) Independent Review



MetroLINK
Cybersecurity Assessment
Tool for Transit (CATT)
Security Assessment Report

December 19, 2022

Draft version 0.1

Executive Summary

The Rock Island County Metropolitan Mass Transit District (**MetroLINK**) has engaged SYSUSA, Inc. (**SYSUSA**) as an independent, third-party company to assess their U.S. Federal Transit Administration (FTA) grant funder Cybersecurity Assessment Tool for Transit (CATT).

The COVID-19 pandemic forced agencies to expand their demarcation points, increased the need for remote work, and quickly pushed critical operations to new technologies that exponentially increased threat vectors. At the same time, cyber-attacks and network intrusions continue to increase.

MetroLINK obtained a grant from **FTA** to develop a cybersecurity assessment tool and supporting documentation to assess its cybersecurity posture and those of other small and mid-sized transit agencies. The tool was developed in response to the recent MTI study and other recently developed publications and research highlighting the lack of cybersecurity preparedness within the transit industry.

SYSUSA is a niche IT and security services company with the depth and breadth of knowledge and experience in security and privacy laws, regulations, and industry best practices. SYSUSA's highly qualified and skilled cybersecurity experts are certified in domestic and international security and privacy disciplines. We are also an accredited audit company through our partnership with the Professional Evaluation and Certification Board (PECB).

The project objective was to develop a tool built on industry best practices and proven methodologies. Additionally, MetroLINK required the tool to be user-friendly in identifying vulnerabilities and threats and determining the consequences, including potential impact, across a transit agency. The tool will also establish a baseline that can be enhanced further to improve the agency's overall cyber posture.


The project has two primary objectives:

1. Develop a prototype cybersecurity risk assessment tool for MetroLINK; and
2. Revise and refine the assessment tool for replication within the transit industry to reduce overall cyber security risk.

FTA projects supported with grant funds have certain requirements that grant recipients must meet. FTA requires MetroLINK to evaluate the CATT tool by contracting an independent, third-party evaluator to assist in developing an evaluation plan and collecting, storing, and managing the data to fulfill the evaluation requirement. FTA also requires MetroLINK to share the performance metrics established by the independent, third-party evaluator with FTA.

High-Level Findings and Recommendations

SYSUSA assessed the CATT and found it to be a useful and comprehensive tool that can deliver value to transit agencies in evaluating their security posture, and position them on a path toward achieving higher maturity levels over time. However, as with every tool or technology, there are areas of improvement that can further enhance the ability to deliver better results and enable the target audience to improve their state. The areas of improvement for CATT are as follows:

1. The tool guides security professionals at every step to complete the questionnaire with hyperlinks and popup callouts. Additional guidance can be incorporated in the hyperlinks and popups to enable ordinary users with limited security knowledge to take advantage of the tool. Furthermore, some terms are not defined and are therefore open to the end user's interpretation. For example, the term Service Continuity Plans has no hyperlink or popup to explain what is required.
2. The questions are very simple. In each section, at least one option will apply to the organization, regardless of the organization's size or the maturity of its practices. Therefore, there should be no reason for any organization to skip a section, which is currently possible. MetroLINK should modify the CATT to prevent users from skipping any sections. It should be mandatory to select at least one option in every section.
3. The report generated from the tool is comprehensive and provides an accurate state of security based on the selected inputs during the assessment. However, when the report is retrieved, the *Revise Report* tab cannot be used to correct the inputs.
4. The blue question mark  provides some valuable information on the control. However, it can be further enhanced by providing additional reference information or links to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) to help clarify and interpret the question as intended. In some cases, the information provided is mapped directly to the function itself; in others, it is mapped to the sub-categories with their IDs.
5. In the overview section of the CATT, a brief explanation of each of the five NIST CSF functions can be added to help clarify the questionnaire and to provide additional guidance for the agencies in leveraging the external NIST CSF guidance to complete the questionnaire.
6. The NIST CSF summary dashboard results in the report show the number of practices performed and the number of practices *not* performed for every category within a function, based on the user input. Upon comparing the dashboard results with the input values provided by the user, we discovered that some of the dashboard results do not match the input.

Approach

To analyze the security and comprehensiveness of the CATT, SYSUSA took a very simple yet holistic approach that enabled it to evaluate the tool's user interface, maturity, and completeness of the report. We evaluated it for ease of use and the end user's ability to navigate and understand the questions and set expectations.

We started with the role of an end user (security assessor or technical lead) who will be using the tool to assess the security posture across the agency's operations technology environment(s). In this role, we filled out the questionnaire. We selected various options to understand how the tool would react and if the reports generated would display the variances in our answers appropriately to reflect the correct state of the environment. We repeated the exercise over 20 times to ensure the tool functions as intended and provides the desired results represented graphically with correct maturity levels.

Second, we adopted the role of an auditor/evaluator. In this role, the goal was to ensure that the tool is consistent and that the inputs are correctly and consistently represented in the outputs. We checked each report against the inputs to ensure that the inputs provided in the questionnaire were reflected in the report as answered/selected. It was a very tedious exercise. Evaluating the reports against inputs helped us determine the accuracy of the reports and understand the approach to developing this questionnaire.

Evaluation & Analysis

The CATT was analyzed in multiple phases. Each phase comprised several steps and had multiple underlying tasks to help understand the tool and establish the foundation for the next step or phase.

The Overview section of the CATT denotes, "*The components of this report package include:*

- *CATT Final Report*
- *CATT-Self Assessment Package*
- *CATT Final Report Presentation*
- *MetroLINK Cybersecurity Assessment (not to be distributed)*
- *CATT Project Evaluation"*

In evaluating the CATT, we only found the following:

- CATT-Self Assessment PDF
- CATT Final Report (generated after completing the assessment)

Additionally, documents referenced in the overview section were not evaluated or submitted for evaluation.

Phase I – User Experience and Data Input

The overall assessment of the CATT interface is good, with the questionnaire layout appearing to be readable and coherent. Consideration is given to several sub-areas, including navigation structure, screen components, the hierarchy of questions, and ease of use. A slight delay was observed while opening the CATT form. Access to every component of the CATT was simple and intuitive, with most options apparent and accessible. The arrangement of the questions with all the options was proper. Additionally, the supportability of each screen element was evaluated.

1: Asset Management

1: Asset Management

1.1 Select one from 5 options.

- 1. Agency's [critical services](#) are **not** identified.
- 2. Agency's [critical services](#) are identified. ?
- 3. [Critical services](#) are identified and prioritized based on analysis of the potential impact if the services are disrupted. ?
- 4. [Critical services](#) are prioritized, documented, and potential impact, if the services are disrupted, is communicated to appropriate [stakeholders](#). ?
- 5. [Critical services](#) are prioritized, documented, and analysis of potential impact, is reviewed bi-annually with [stakeholders](#). ?

1.2 Select one from 5 options.

- 1. Organization's [mission, vision, values and purpose](#), including the organization's place in critical infrastructure is **not** identified. This includes the relationship with municipal and federal government.
- 2. Organization's [mission, vision, values and purpose](#), including the organization's place in critical infrastructure is identified. This includes the relationship with the municipal and federal government. ?
- 3. Organization's [mission, vision, values and purpose](#), including the organization's place in critical infrastructure is evangelized to the agency staff. ?

Figure 1: User Interface

Small typographical errors on the user interface have no impact on the tool's usage. Certain questions were assessed to have complex terms which require explanation. There is a need for judicious use of exact keywords and terms. The

use of certain terms requires explanation, such as *Service Continuity Plan*, which the user must first understand to select the option corresponding to it correctly. Also, the mapping between options and sub-categories does not always indicate that they are in sync. The first option selection is smooth, while a lag is observed upon changing the option.

This process was repeated with different options for 20+ reports. In different scenarios, inputs were provided randomly for every section in all the domains in each case. In each scenario, we chose different answers to each section. In some scenarios, we chose the same answer for each section, and the output was generated successfully. In one scenario, we selected only Option 2 in each section for all the domains to generate the report and validate that the output was reflected correctly. Reports were generated for a different combination of selected options, such as selecting only those options that refer to fundamental details or limiting the number of questions attempted. The selections were reflected in the CATT Summary portion of the report.

5: Incident Management

5: Incident Management

5.1 Select one from 5 options.

- 1. The agency does **not** have a plan for managing [cyber incidents](#).
- 2. The agency has a plan for managing [cyber incidents](#). ?
- 3. The [cyber incident](#) management plan is reviewed and updated. ?
- 4. The roles and responsibilities in the [cyber incident](#) plan are included in job descriptions. ?
- 5. Staff have been assigned to the roles and responsibilities detailed in the incident management plan. ?

5.2 Select one from 5 options.

- 1. Known [cybersecurity threats](#) to [operational technology](#) are **not** shared with [stakeholders](#).
- 2. Known [cybersecurity threats](#) to [operational technology](#) are shared with [stakeholders](#).
- 3. [Stakeholders](#) are trained on new [cybersecurity threats](#) to [operational technology](#).
- 4. There are a set of procedures for [operational technology vulnerability](#) and [threat](#) management. ?
- 5. Changes to policies and procedures related to [operational technology](#) are shared with appropriate [stakeholders](#). ?

Figure 2: User Interface Hyperlinks

In subsequent tests, random possibilities were chosen for several sections across the 20+ scenarios in 10 domains. We observed that the modifications were reflected in the report, and the maturity shifted from one report to the other reports.

The CATT was also determined to be user-friendly across all platforms, including Chrome, Internet Explorer, and Adobe Acrobat. Following the selection of the appropriate options, submitting the form is simple.

Phase II – Output Generation

SYSUSA evaluated the CATT using a combination of inputs. In each scenario, as mentioned above, we used a different input to generate an output to analyze the tool.



Figure 3: *Report Banner Page*

The reports generated in each scenario provided important information to help the agency leadership understand the current security state across the assessed operational technology (OT) domains and opportunities for improvement.

Although the report provided an option to revise the assessment, the link sometimes did not work as intended, and the report could not be revised. The report provided a high-level overview of scoring criteria.

STAAT Review Scoring

The STAAT is an interview-based assessment. It is understood that participants often do not have complete knowledge of an organization's operations. Actual performance may vary from what is indicated in this report. Organizational performance is presented across several dimensions within the report. Scores are provided for individual Practices, Goals, and Domains.

Basic Rules

For each Goal, participants are asked to select the description that most aptly applies to their organization. There is no "right" or "wrong" answer. The intent is to document the current state of your cybersecurity program so that the STAAT can assist in identifying gaps and help the organization in remediating areas where limited or no aspects of the program have yet been created. The discussion that this decision prompts is often as valuable as the selection itself.

Scoring Rubric

For each Goal, five descriptions of a practice are provided that accomplish the Goal, starting with "the practice is not performed".

Figure 4: CATT Review Scoring

The report provided insight into 10 assessed security domains derived from a larger security and business continuity framework CERT® Resilience Management Model (CERT-RMM), deployed by the CERT Program at Carnegie Mellon University's Software Engineering Institute. These domains are as follows:

1. Asset Management
2. Controls Management
3. Configuration and Change Management
4. Vulnerability Management
5. Incident Management
6. Service Continuity Management
7. Risk Management
8. External Dependencies Management
9. Training and Awareness
10. Situational Awareness

The report also provided the performance status of the above-stated domains with a view using two dashboards. These dashboards are:

- CATT Performance Summary
- NIST Cybersecurity Framework Summary

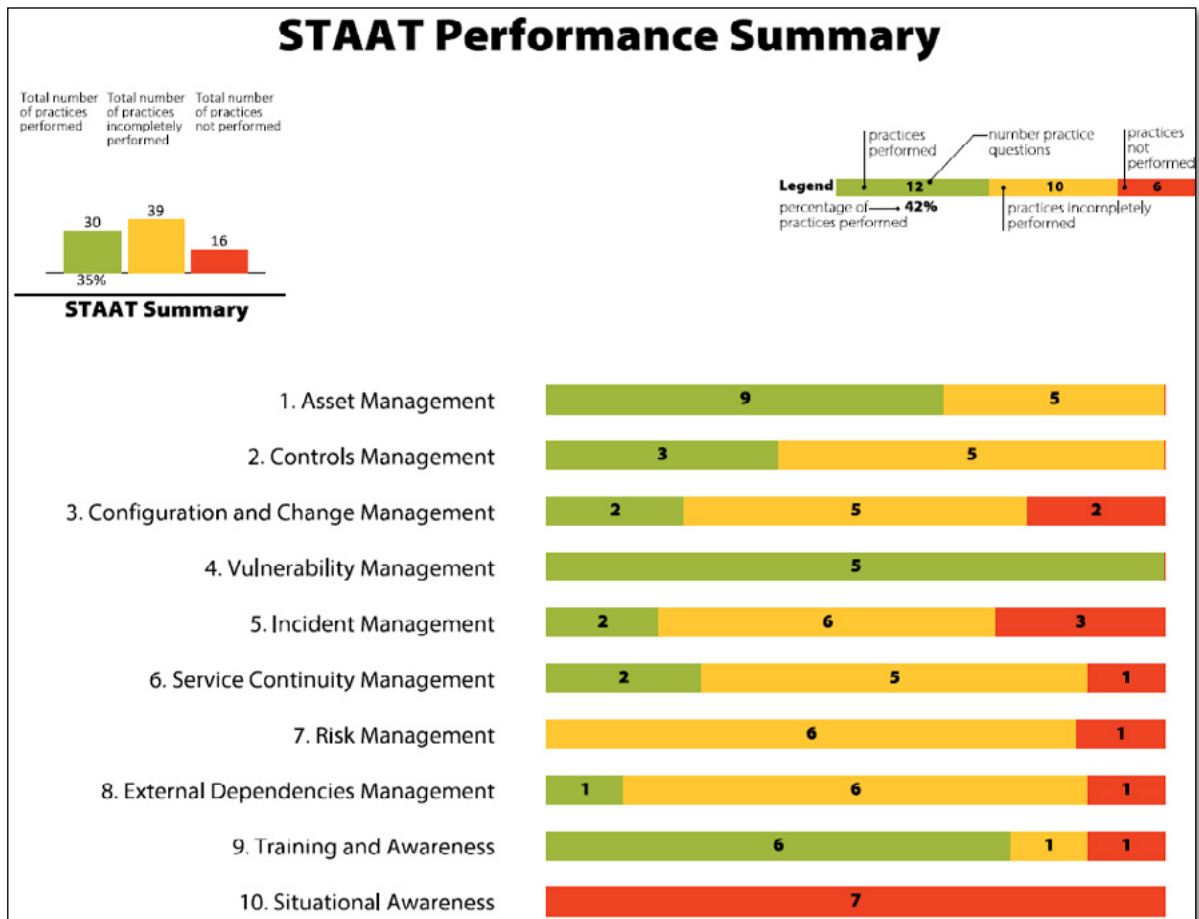


Figure 5: CATT Performance Summary

The CATT Performance Summary provides the overall score of adopted/performed practices following the 10 security domains, as shown in *Figure 5: CATT Performance Summary*. It gives the management a high-level view of control performance and maturity in a particular OT domain, enabling them to make risk-based informed decisions for future security investments with the highest return on investment. The security teams can use this dashboard to understand their level of maturity and conformance in each of the 10 domains and develop a roadmap prioritizing the areas in critical need of higher maturity levels and increased resilience.



Figure 6: NIST CSF Summary

In contrast, the NIST Cybersecurity Framework Summary provides the overall score of adopted/performed practices broken down by NIST CSF functions, as illustrated in Figure 6.

It groups the controls following the NIST CSF function areas (Identity, Protect, Detect, Respond and Recover) and provides the control performance for the agency in each of the categories under each function. It provides the organization with additional information to build upon the CATT performance summary and the state of security across the agency.

Phase III – Input/Output Validation

The output from CATT is critical for agencies. Management teams will rely on CATT reports representing their environment's state of security with scoring to support their use cases and potential requests for resources to achieve higher maturity levels.

Keeping this in mind, we explored the CATT deeply by validating the outputs against selected inputs. This phase was the most critical in determining if the CATT can deliver what it promises: a report on all findings aligned with the input from the end user.

To ensure that the inputs and outputs were aligned, we took the following steps to analyze the output and validate the results to determine the CATT's comprehensiveness and consistency in delivering results:

1. We started our analysis by selecting a particular option in each section of every domain in the CATT for our use case to verify and validate the inputs and outputs.
2. Next, we generated a report for that assessment by clicking the *Generate Report* button at the top.
3. Next, we opted to print the report by clicking the *Print Report* button at the top.
4. Next, we analyzed the CATT and NIST CSF Summary by examining and validating the outcomes/scores by choosing a course of action. The results were examined using the methodology outlined in the section below:
 - a. A goal/practice is considered **RED** if it is not consistently performed.
 - b. A goal/practice is considered **YELLOW** if it is consistently performed but not yet consistently measured or managed.
 - c. A goal/practice is considered **GREEN** if it is consistently performed, managed, and measured.
5. The colors red, yellow, and green are also aligned with the options selected in the reports, and the summary dashboards in the report must match these colors.
 - a. **RED** depicts Option 1.
 1. Practice is not performed (**RED**)
 - b. **YELLOW** depicts Options 2 and 3.

2. Practice is starting to be performed, but it is not yet consistently performed (YELLOW)
3. Practice is consistently performed but not measured and managed (YELLOW)
- c. GREEN depicts Options 4 and 5.
 4. Practice is performed and is starting to be measured and managed (GREEN)
 5. Practice is performed, and both measured and managed (GREEN)

We performed these steps in each use case below to achieve the results.

Use Case 1 - TR Option 2 (selecting option 2 for all questions)

In **Use Case 1 - TR Option 2**, we selected **Option 2** for each section in all 10 domains. According to the scoring rubric, Options 2 and 3 represent the **YELLOW** goal. For example, Option 2 was provided for all 14 sections in the **Asset Management** domain. The CATT Performance Summary dashboard, shown in Figure 7, represented the Asset Management domain with a **YELLOW** label for all 14 sections.

Upon verifying the inputs with the report generated for all the other domains for Option 2, we were able to validate that the CATT Performance Summary dashboard correctly represents the input data provided.

The dashboard displays the 10 domains and a number corresponding to them, displaying how many questions were attempted in each. The numbers matched with the input and were validated.

The **YELLOW** color in Figure 7 depicts that either Option 2 or 3 was selected for all the questions in all the domains. The results in Figure 7 verify the scoring rubric was being followed correctly, i.e.:

- **RED** depicts Option 1.
- **YELLOW** depicts Options 2 and 3.
- **GREEN** depicts Options 4 and 5.

Please note that in this use case, only Option/Practice 2 was selected for all the domains during the assessment. The score generated in the report was expected to reflect the **YELLOW** color, which is validated in Figure 7.

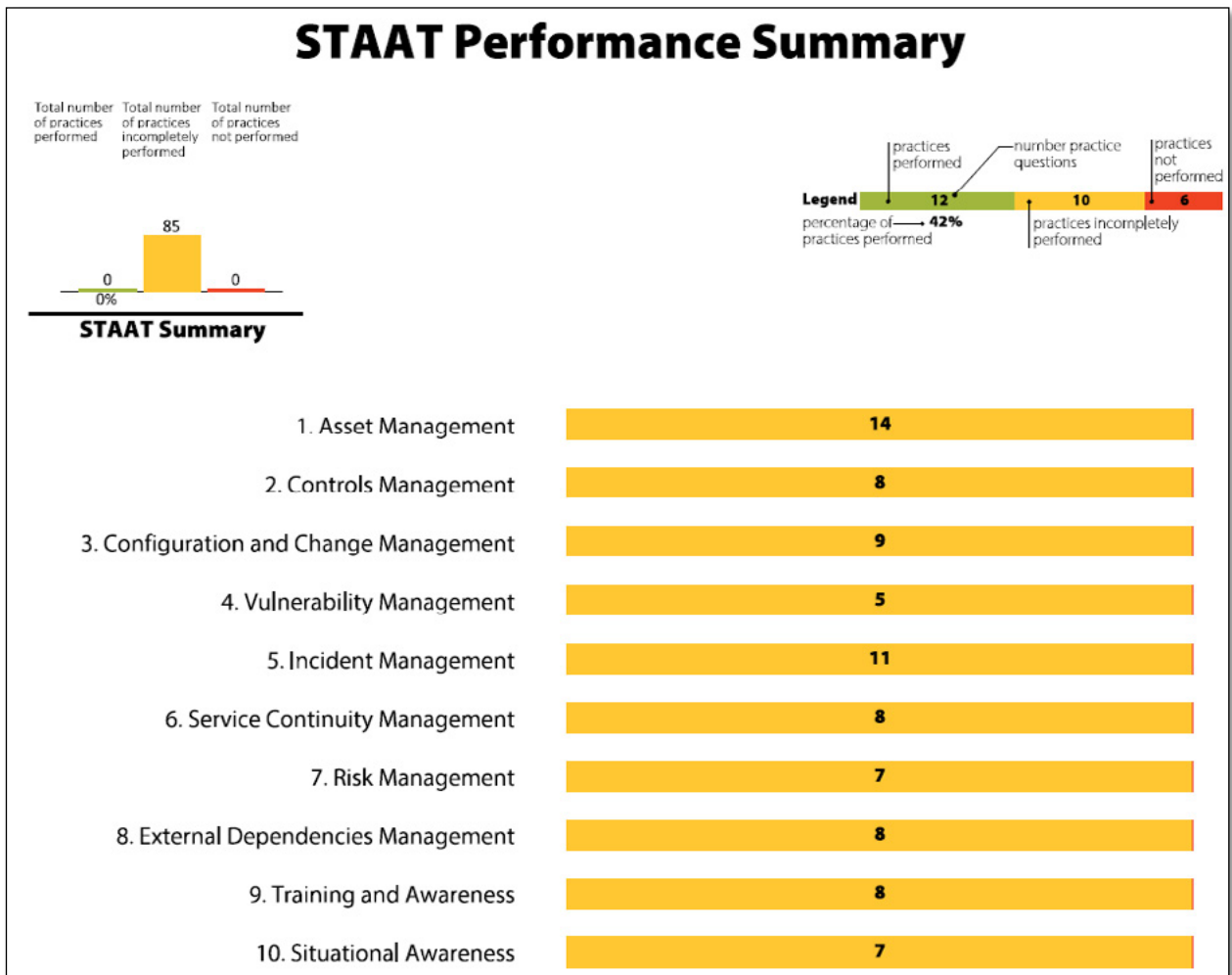


Figure 7: Use Case 1 - TR Option 2 CATT Performance Summary

Use Case 2 - TR Option 3 (selecting option 3 for all questions)

In **Use Case 2 – TR Option 3**, we selected **Option 3** for each section in all 10 domains. According to the scoring rubric, Options 2 and 3 represent the **YELLOW** goal. For example, when we selected Option 3 for all 14 sections in the **Asset Management** domain, the CATT Performance Summary dashboard for the Asset Management domain was expected to be YELLOW. The screenshot of the dashboard, shown in Figure 8, validates that output. Once we verified the inputs with the corresponding outputs in the generated report for the respective domains for Option 3, the CATT Performance Summary dashboard correctly represents the inputs.

The dashboard displays the 10 domains and a number corresponding to them, displaying how many questions were attempted in each. The numbers matched with the input and were validated.

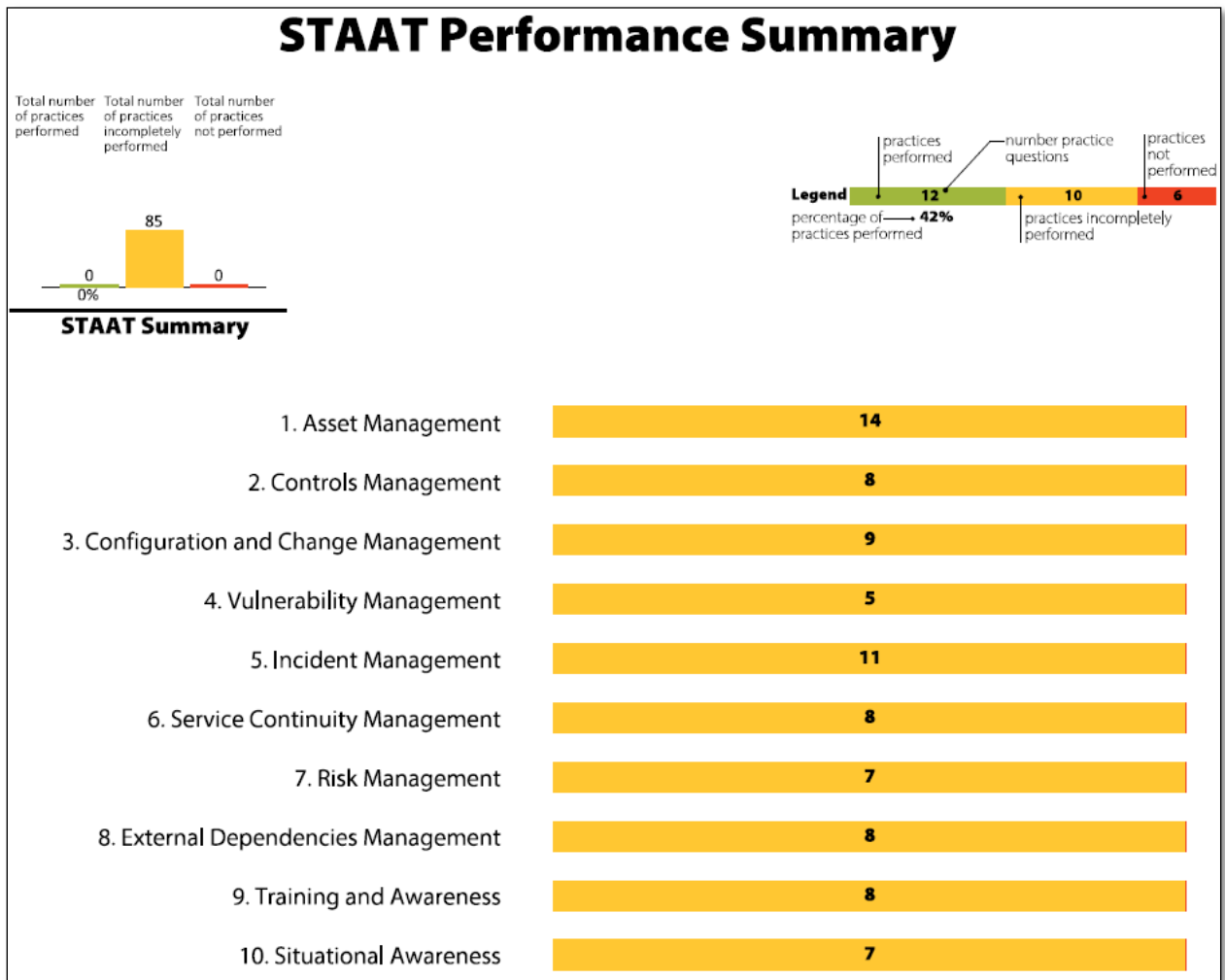


Figure 8: Use Case 2 - TR Option 3 CATT Performance Summary

The YELLOW color in Figure 8 depicts that either Option 2 or 3 was selected for all questions in all domains. The results in Figure 8 verify the scoring rubric was being followed correctly, i.e.:

- RED depicts Option 1.
- YELLOW depicts Options 2 and 3.
- GREEN depicts Options 4 and 5.

Additionally, the output was validated with the data input for a specific domain, **Configuration & Change Management**, and the percentage of practices performed was 0 percent. The rank among domains from least to most practiced was 3/10, validating the output in terms of "percentage of practices performed" and "rank among domains" to be correct based on input provided. We also validated the same for the **Vulnerability Management** domain, where

the percentage of practices performed was 0 percent, and the rank among domains from least to most practiced was 4/10.

Please note that in this use case, only Option/Practice 3 was selected for all the domains during the assessment. The score generated in the report was expected to reflect the YELLOW color, which is validated in Figure 8.

Use Case 3 - TR Random Selection 1

In **Use Case 3 – TR Random Selection 1**, we randomly selected answers for each section in every domain. For example, in the **Asset Management** domain, random options were provided for all 14 sections.

The CATT Performance Summary dashboard represented the Asset Management domain with a GREEN label for all 14 sections. Following the scoring rubric, Options 2 and 3 represent the YELLOW goal, while Options 4 and 5 represent the GREEN goal.

Upon verifying the inputs with the generated report for all the domains for randomly selected options, we verified and validated that the CATT Summary dashboard correctly represents the input data.

The dashboard screenshot in Figure 9 displays the 10 domains. It depicts the number of randomly selected inputs for every section in all the domains. All the inputs selected during the assessment represented the YELLOW and GREEN goals, which is correctly represented in the CATT summary report.

- RED depicts Option 1.
- YELLOW depicts Options 2 and 3.
- GREEN depicts Options 4 and 5.

Additionally, the output was validated with the data input for a specific domain, **Incident Management**, and the percentage of practices performed was 100 percent. The rank among domains from least to most practiced was 3/10, validating the output in terms of "percentage of practices performed" and "rank among domains" to be correct based on input provided. We also validated the same for the **Service Continuity Management** domain, where the percentage of practices performed was 0 percent, and the rank among domains from least to most practiced was 7/10.

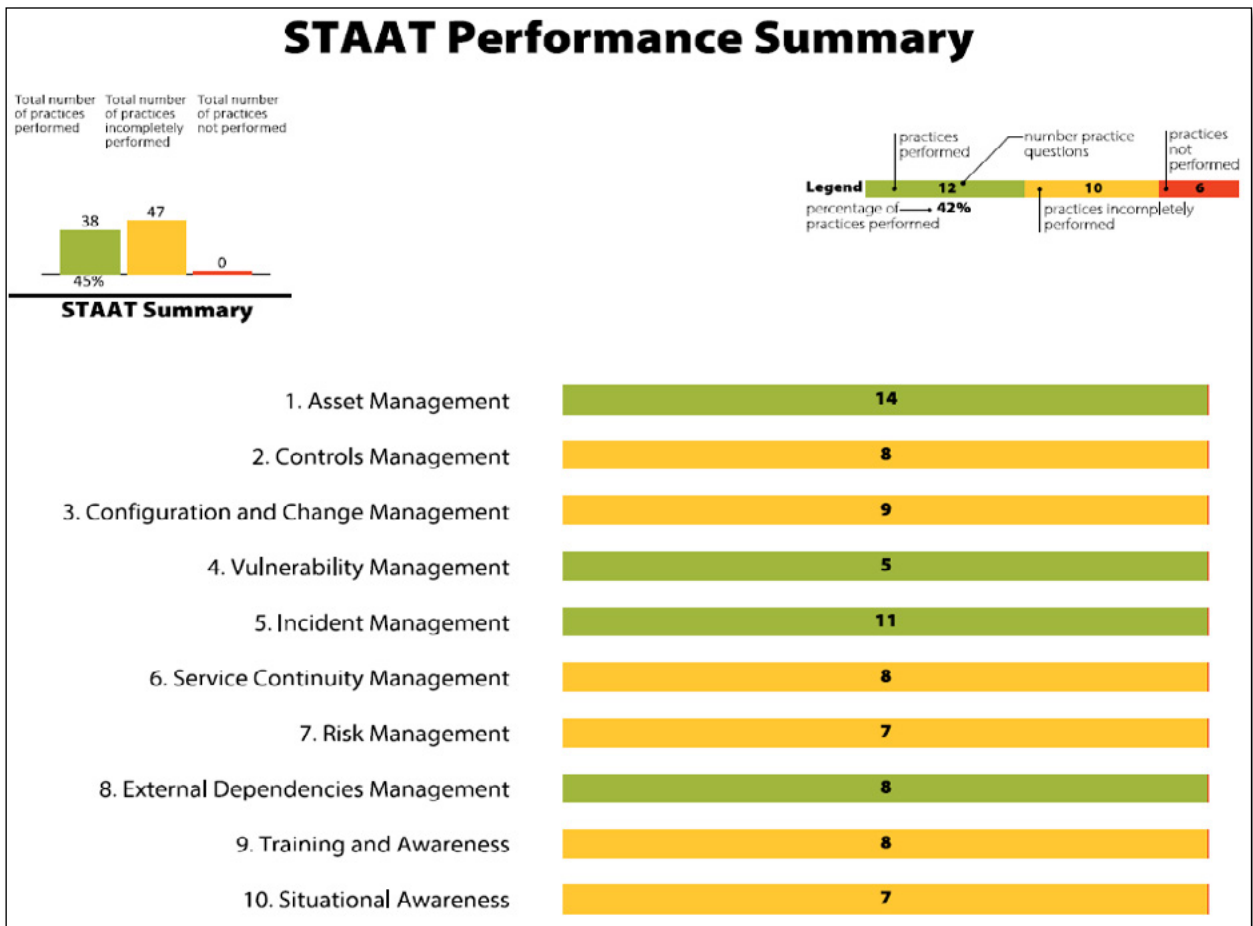


Figure 9: Use Case 3 - TR Random Selection 1 CATT Performance Summary

Use Case 4 - TR Random Selection 2

In **Use Case 4 – TR Random Selection 2**, we randomly selected options for each section in every domain. According to the scoring rubric, **Options 2 and 3** represent the **YELLOW** goal, and **Options 4 and 5** represent **GREEN** goals. For example, in the **Asset Management** domain, random options were provided for all 14 sections. The CATT Performance Summary dashboard represented the Asset Management domain with half as GREEN and half as YELLOW for all 14 sections.

Upon verifying the inputs with the report generated for all the other domains for randomly selected options, we were able to validate that the CATT Performance Summary dashboard correctly represents the data input.

The dashboard screenshot in Figure 10 displays the 10 domains. It depicts the number of randomly selected inputs for every section, based on the selected domain. All these input options represent the YELLOW, GREEN, and RED goals, which is represented correctly in the CATT summary report.

- **RED** depicts Option 1.
- **YELLOW** depicts Options 2 and 3.
- **GREEN** depicts Options 4 and 5.

Additionally, the output was validated with the data input for a specific domain, **Risk Management**. The output was evaluated against the "percentage of practices performed" and "rank among domains" and determined to be correct based on the input. The percentage of practices performed was 43 percent, and the rank among domains from least to most practiced was 8/10. The percentage of practices performed was 50 percent, and the rank among domains from least to most practiced is 7/10. Likewise, we validated the **Training Awareness Management** domain.

The overall results observed were in line with the inputs shown in Figure 10. All the domains' total scores match the CATT Performance Summary Graphic score.

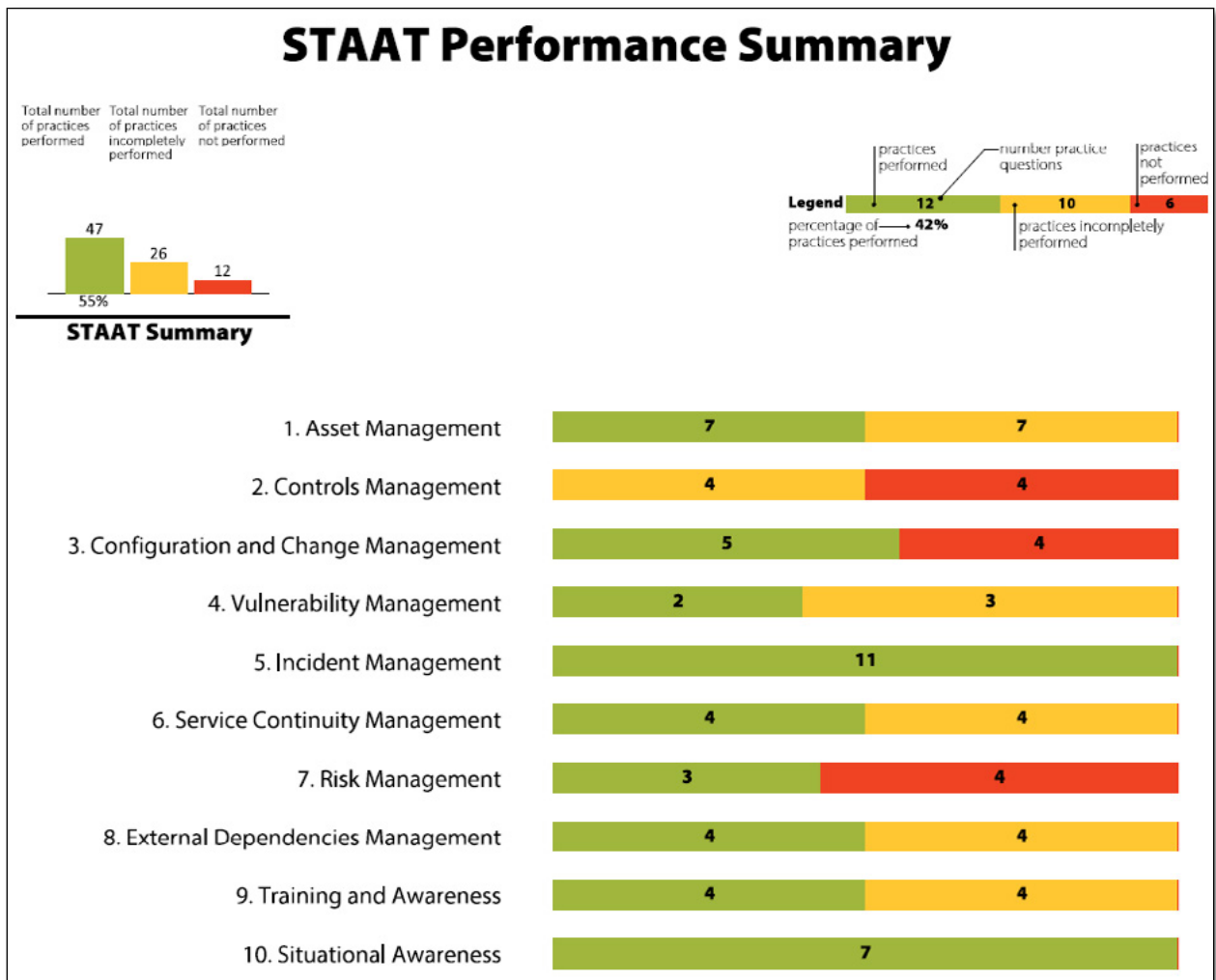


Figure 10: Use Case 4 - TR Random Selection 2 CATT Performance Summary

NIST CSF SUMMARY ANALYSIS

Assessment of the NIST CSF dashboard was initiated by analyzing the bar charts for each function and the bar charts generated for each category associated with the functions, as shown below in the NIST dashboard screenshot. The functions are briefly defined below:

- **Identify (ID)** – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. The activities in the *Identify* function are foundational for the effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome categories within this function include:
 - Asset Management;
 - Business Environment;
 - Governance;
 - Risk Assessment; and
 - Risk Management Strategy.
- **Protect (PR)** – Develop and implement appropriate safeguards to ensure the delivery of critical services. The *Protect* function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome categories within this function include:
 - Identity Management and Access Control;
 - Awareness and Training;
 - Data Security;
 - Information Protection Processes and Procedures;
 - Maintenance; and
 - Protective Technology.
- **Detect (DE)** – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The *Detect* function enables the timely discovery of cybersecurity events. Examples of outcome categories within this function include:
 - Anomalies and Events;
 - Security Continuous Monitoring; and
 - Detection Processes.
- **Respond (RS)** – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The *Respond* function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome categories within this function include:

- Response Planning;
 - Communications;
 - Analysis;
 - Mitigation; and
 - Improvements.
- **Recover (RC)** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The *Recover* function supports timely recovery to normal operations to reduce the impact of a cybersecurity incident. Examples of outcome categories within this function include:
 - Recovery Planning;
 - Improvements; and
 - Communications.

Each bar chart associated with a category contains **RED** and **GREEN** sections. The GREEN section within the bar chart represents the number of practices performed, and the RED section represents the number of practices *not* performed. The numbers in the GREEN section and the RED section within the bar chart represent the number of practice questions that correspond to the practices performed (GREEN) and the practices *not* performed (RED), respectively, based on the inputs provided in the questionnaire by the user.

Several actions were performed against the NIST CSF Summary to determine whether the results were verifiable. Table 1 explains the analysis in Excel for TR Option 2. Figures 14 and 15 are visualizations of the analysis and provide a better understanding of the approach to analyzing the outputs.

Table 1: NIST CSF Verification

The following criteria determine whether the results can be verified or not.	
<p>If there is a mismatch between the score in green and red (i.e., if Green has more value than predicted or even less), the comparison is deemed incorrect. Similarly, if more or fewer values/scores in red are received than what the report anticipates, there is also a mismatch. Therefore, in the CATT EVALUATION METRIX excel sheet, the status will be listed as Not verified.</p>	Not verified
<p>According to the report generated for NIST CSF Summary, if the comparison of the red and green score values is accurate, it is put under Verified status, and the observation is marked as a Match in the excel sheet.</p>	Verified

Take the example of a report that generated the dashboard shown in Figure 11 for the *Identify* function (ID) based on user inputs.

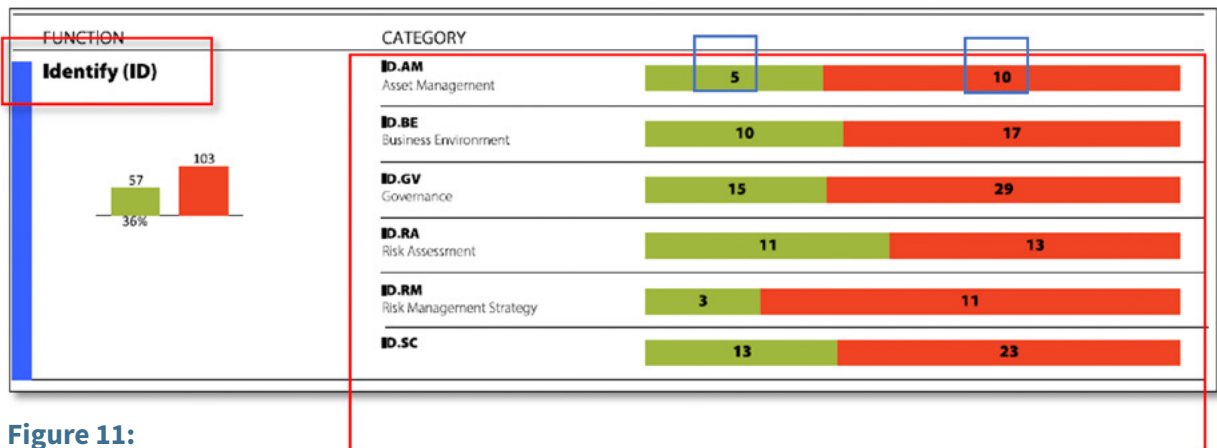


Figure 11:
NIST CSF Summary Identity

The ID.AM category (Asset Management) in Figure 11 is represented by a bar chart. It contains five questions corresponding to practices that have been performed (GREEN) and 10 questions corresponding to practices that have *not* been performed (RED). It also means that the category Asset Management is mapped 15 times through 15 practice questions in the questionnaire related to Asset Management (ID.AM).

We took a deeper dive to analyze and understand how the numbers in the GREEN and RED Sections (5 and 10) shown in Figure 11 were attributed to ID.AM (Asset Management).

We looked at the questions in the CATT for every domain. Each question has five options, with Option 1 corresponding to practice not followed at all and Option 5 corresponding to practice completely followed for the referenced domain. For Options 2, 3, 4, and 5 for all the questions throughout the questionnaire, there is a clickable *Info* icon option with a popup dialog box, as shown in Figure 12.

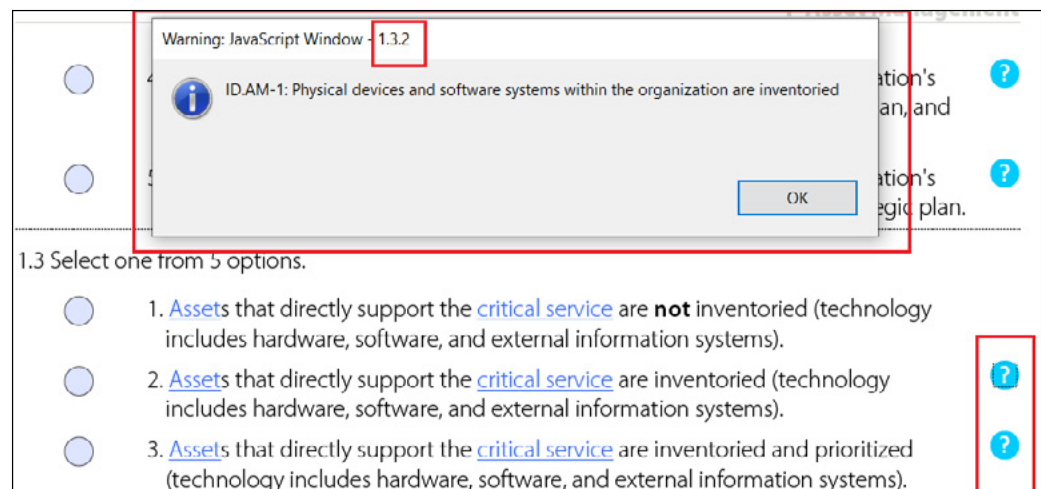




Figure 12: Popup Window Numbering ID.AM-1

Each *Info* icon  represents a category or a set of categories.

For example, in Figure 12, upon clicking Option 2 of Question 1.3, the dialog box displays *ID.AM-1 (Physical devices and software systems within the organizations are inventoried)*. The number 1.3.2 displayed on top of the dialog box can be broken down to help us understand the numbering nomenclature as follows:

- **One** refers to the security **domain** 1 (Asset Management),
- **Three** refers to the **section** within that security domain.
- **Two** refers to a specific **question** number in a specific section of a specific security domain ID.AM – 1

Similarly, when we click on the *Info* icon  against the third option (Option 3) of Question 1.3, the dialog box in Figure 13 displays *ID.AM-5 (Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value)* in the number 1.3.3 displayed on top of the dialog box.

- **One** refers to the security **domain** 1 (Asset Management),
- **Three** refers to the **section** within that security domain.
- **Three** refers to a specific **question** number in a specific section of a specific security domain ID.AM – 5

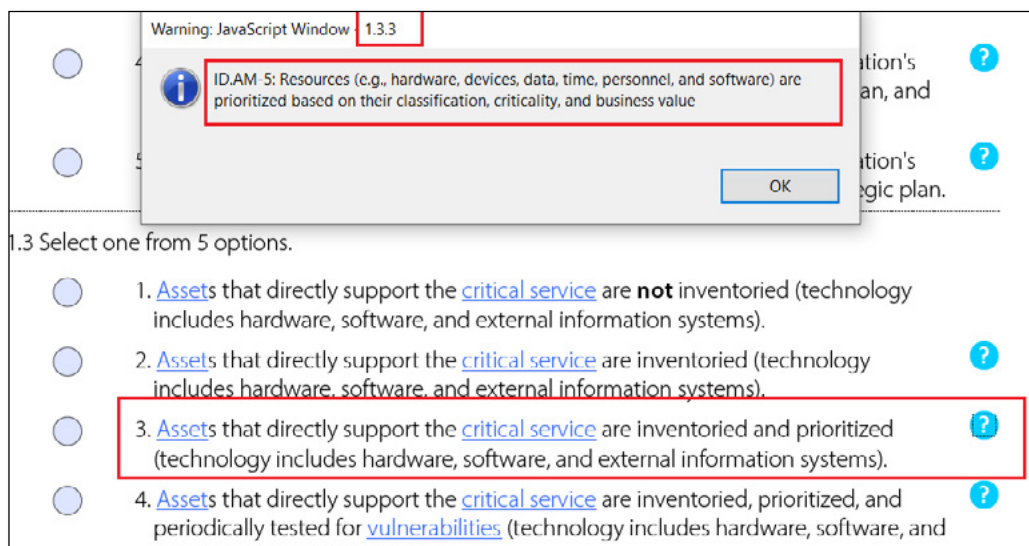


Figure 13: *Popup Window Numbering ID.AM-5*

Based on our understanding, we discovered that the practice would be considered performed for ID.AM-5 if Option 3 is selected by the user while providing the data input. Further, even if Options 4 and 5 are selected by the user while providing the data input, the practice for ID.AM-5 (at Option 3) will be

considered performed (coded as GREEN) because of the minimum threshold for ID.AM-5 in Question 1.3 has been set as corresponding to Option 3.

In contrast, when we navigate from Options 1 to 2 and 5, the trend of practices being performed increases with every option. If a user enters any value greater than Option 3, the practice for ID.AM-5 will be considered performed. It includes Options 4 and 5. However, if the user selects Option 2 (an option less than 3), then the practice will be considered as *not* performed (coded as RED).

We traversed the questions in the CATT and maintained a repository of practice mappings to a particular category in an Excel sheet. We then checked, for each category, whether the practice was being performed or not based on the user input in different scenarios. In doing so, we discovered some irregularities.

Following the logic explained above, three use cases are displayed below. In the following use case, TR Option 2, we have taken Option 2 as the selected option by the user throughout the questionnaire for every question in all the domains.

TR Option 2 (only option 2 is selected throughout the form)

As shown in Figure 14, in the Asset Management category (ID.AM), there are a total of 16 questions being referenced in the questionnaire. Out of these 16 questions, there are five questions that correspond to practices being performed (in GREEN) and 11 questions that correspond to practices *not* being performed, based on our findings about how the results are generated.

Category	Subcategory	Reference Question
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	ID.AM 1.10.4, 1.3.2, 1.10.2, 3 questions mapping with ID-AM 1
	ID.AM-2: Software platforms and applications within the organization are inventoried	
	ID.AM-3: Organizational communication and data flows are mapped	1.10.5, 1 question mapping with ID-AM 3
	ID.AM-4: External information systems are catalogued	
	ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	1.3.3, 1.7.2, 1.7.3, 1.10.3, 5.1.5, 5 questions mapping with ID-AM 5
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	2.7.4, 3.7.5, 10.3.2, 8.6.3, 4.4.2, 5.6.4, 5.8.3, 7 questions mapping with ID-AM 6

Figure 14: NIST CSF Report Discrepancies 1

When the results of the report shown in Figure 11 were compared with the analysis shown in Figure 14, it was discovered that in Figure 11, five questions correspond to practices being performed (GREEN), and 10 questions correspond

to practices *not* being performed (RED). As shown in Figure 11, 10 questions correspond to practices *not* being performed, while in Figure 14, there are 11 questions corresponding to practices *not* being performed. There is a difference of 1, as depicted in Figure 15.

Subcategory	Refer	STATUS for TR option 2 is selected	Nist summary Value (No. of Values in Green / No. of Values in Red)	Observations for TR option 2 is selected	Delta Criteria		
<div style="border: 1px solid red; padding: 2px;">ID.AM-1: Physical devices and systems within the organization are inventoried</div>	3	Not-Verifiable	results as per NIST Dashboard 5/10 Nist summary = 15	results as per our analysis Mismatch 5/11 Observation = 16	<div style="border: 1px solid green; padding: 2px;">DeltaDelta - 1 in green = one extra value in green as compared to NIST summary</div> <div style="border: 1px solid red; padding: 2px;">Delta +1 in red = one extra value in red as compared to the NIST summary report</div> <div style="border: 1px solid green; padding: 2px;">DeltaDelta - 1 in green = one value less in green as compared to NIST summary</div> <div style="border: 1px solid red; padding: 2px;">Delta - 1 in red = one value less in red as compared to the NIST summary report</div> <div style="border: 1px solid red; padding: 2px; margin-top: 10px;">Delta + 1 in red</div>		
<div style="border: 1px solid red; padding: 2px;">ID.AM-2: Software platforms and applications within the organization are inventoried</div>	5						
<div style="border: 1px solid red; padding: 2px;">ID.AM-3: Organizational communication and data flows are mapped</div>	5						
<div style="border: 1px solid red; padding: 2px;">ID.AM-4: External information systems are catalogued</div>	5						
<div style="border: 1px solid red; padding: 2px;">ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value</div>	2						
<div style="border: 1px solid red; padding: 2px;">ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established</div>	3						

Figure 15: NIST CSF Report Discrepancies 2

Next, the results were validated against the dashboard, shown in Figure 11. The findings did not match the dashboard results for ID.AM. **The methodology used in Figures 14 and 15 to attain the result of “Not-Verifiable” is as follows:**

According to the reasoning explained above, it was found that Option 1.10.4 in Figure 14 will be considered *not* performed (RED) for ID.AM-1 because the user has selected Option 2 while providing the data input.

Further, even if Option 5 is selected by the user while providing the data input, the practice for ID.AM-1 (Option 2) will be considered to be *not* performed (RED) because of the minimum threshold for ID.AM-1 in Question 1.3 has been set as corresponding to Option 2. Therefore, in this case, when the user inputs any value that is greater than Option 2, the practice for ID.AM-1 will be considered to be *not* performed. It includes Options 3, 4, and 5. However, if the user selects Options 1 or 2 (an option less than Options 2 and 3 is where ID-AM 1 is mapping), then the practice will be considered performed (GREEN).

Similarly, the other options seen in Figure 14 are mapped to ID-AM 3, ID-AM 5, and ID-AM 6 sub-categories Options 3, 4, or 5 (e.g., 1.10.5 at ID-AM 3) and are considered not performed (RED). On the other hand, the options mapped as Option 2 against the same sub-categories (e.g., 1.7.2 at ID-AM 5) are considered performed (GREEN). No mappings were found across the questionnaire for the sub-categories like ID-AM 2 and ID-AM 4. Therefore, they are blank in Figure 15.

There is a difference of 1, as depicted in Figure 15, in the total number of practices performed, as seen in Figure 11. Only 10 questions correspond to practices not being performed. At the same time, in Figures 14 and 15, we have 11 questions corresponding to practices not being performed, so the delta in Figure 15 is "1 in RED."

NIST Performance Summary Dashboard:

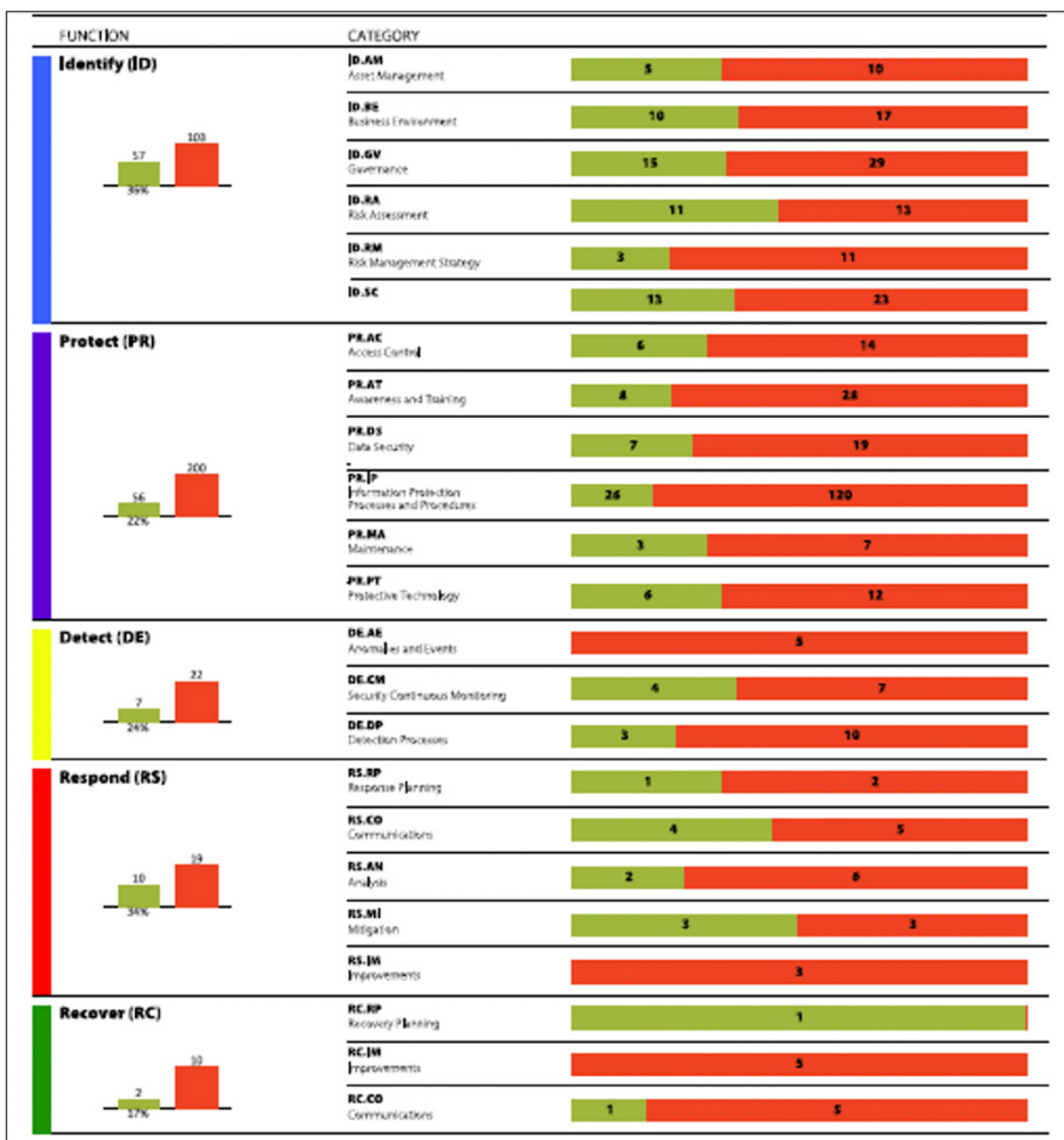


Figure 16: NIST Performance Summary Dashboard

The NIST CSF Summary Graphic was checked to determine if the outcome score against each function/category is valid. For the function Identify (ID), the following values were obtained for GREEN/RED:

Total Score green/red TR Option 2	132	354
-----------------------------------	-----	-----

TR Option 3 (only option 3 is selected throughout the form)

ID.RA-1: Asset vulnerabilities are identified and documented	<p>4+2+1+3+2+12= 24 Total of 24 questions mapping to various sub-categories in ID-RA</p> <p>4 options mapped with ID-RA 1</p> <p>D.RA 10.3.4, 10.4.2 4.2.5, 4.3.2,</p>
ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	<p>2 Options mapped with ID-RA2</p> <p>10.2.2, 10.2.3,</p>
ID.RA-3: Threats, both internal and external, are identified and documented	<p>1 Option mapped with ID-RA 3</p> <p>10.2.3</p>
ID.RA-4: Potential business impacts and likelihoods are identified	<p>3 Options mapped with ID-RA 4</p> <p>7.2.2, 7.2.3, 7.3.3,</p>
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	<p>2 Options mapped with ID-RA 5</p> <p>8.1.5, 7.3.2,</p>
ID.RA-6: Risk responses are identified and prioritized	<p>12 Options mapped with ID-RA 6</p> <p>3.4.5, 10.5.2, 9.8.5, 8.7.2, 7.3.4, 7.3.5, 7.4.2, 7.4.3, 6.3.5, 4.5.2, 5.9.2, 6.7.2,</p>

Figure 17: NIST CSF Report Discrepancies 3

As shown in Figure 17, the Risk Management category (ID.RA), has 24 questions referenced in the questionnaire. Of these 24 questions, 16 correspond to practices performed (GREEN), and 8 correspond to practices not performed (RED).

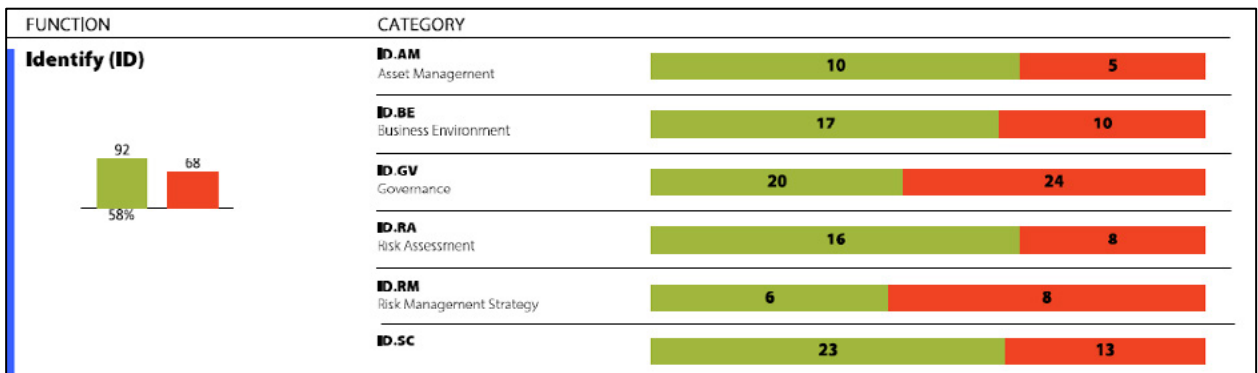


Figure 18: NIST CSF RA Category Validation

When the results in Figure 18 are compared with the analysis in Figure 17, it can be observed that in Figure 18, there are 16 questions corresponding to practices performed (in GREEN) and 8 questions corresponding to practices not performed (RED). As depicted in Figure 19, there is no difference in the total number of practices performed. Questions that correspond to practices not performed in Figure 18 are in agreement with the results of our analysis in Figure 19.

Category	Verification Status	Results as per NIST Dashboard	Results as per our analysis	Discrepancy
ID.RA-1: Asset vulnerabilities are identified and documented	Verified	16/8 Nist summary = 24	Match 16/8 Observation = 24	Nil
ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources				
ID.RA-3: Threats, both internal and external, are identified and documented				
ID.RA-4: Potential business impacts and likelihoods are identified				
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk				
ID.RA-6: Risk responses are identified and prioritized				

Figure 19: NIST CSF Report Discrepancies 4

The results were then validated using the report's dashboard, shown in Figure 18. Upon validating, we found that our findings match the dashboard results for ID.RA.

The methodology outlined in Figures 17 and 19 was used to attain the following result:

As explained above, it was found that Option 10.3.4 in Figure 17 will be considered *not* performed (RED) for ID.RA-1 because the user has selected Option 3 while providing the data input. Further, if Option 5 is selected by the user during the assessment, the practice for ID-RA 1 (Option 4) will be considered not performed (RED), as the minimum threshold for ID.RA-1 in Question 10.3 has been set as corresponding to Option 3.

Therefore, in this case, when the user enters any value greater than Option 4, the practice for ID.RA-1 will not be performed. It includes Option 5. However, if the user selects Options 1, 2, or 3 (option less than Option 4 where ID-RA 1 is mapping), then the practice will be considered performed (GREEN).

Similarly, for all the options seen in Figure 17 mapped to the rest of the sub-categories (ID-RA 2, ID-RA 3, ID-RA 4, ID-RA 5, ID-RA 6), the ones with Option 5 (e.g., 6.1.5 at ID-RA 5) will be considered *not* performed (RED). At the same time, the options mapped as Options 2, 3, and 4 against the sub-categories (e.g., 10.2.2, 10.2.3 at ID-RA 2) will be considered performed (GREEN).

There is no difference, as depicted in Figure 19. The total number of practices performed, compared to Figure 18 and Figure 19, shows 8 questions that correspond to practices *not* performed and 16 questions that correspond to practices performed.

TR Random Selection 1

<p>RS.IM-1: Response plans incorporate lessons learned</p>	<p>3 + 1 = 4 Total of 4 Options mapping with sub-categories in RS-IM</p>
<p>RS.IM-2: Response strategies are updated</p>	<p>3 options mapped with RS-IM 1</p>
	<p>RS IM 4.3.4, 6.2.5 5.10.3</p>
	<p>1 Option Mapped with RS-IM 2</p>
	<p>5.10.3</p>

Figure 20: Random Control Selection

In figure 20, for the Respond category (RS.IM), 4 questions are referenced in the questionnaire. Out of these 4 questions, there are 3 questions corresponding to

practices performed (GREEN) and 1 corresponding to practices *not* performed (RED). When the results from the report in Figure 22 are compared with the analysis in Figure 20, it can be observed that in Figure 21, there are 3 questions corresponding to practices performed (GREEN) and 0 questions corresponding to practices *not* performed (RED).



Figure 21: Respond Random Control

There is a difference of 1, as depicted in Figure 22, in the total number of practices performed. As seen in Figure 21, no questions correspond to practices *not* performed, while in Figures 20 and 22, there is 1 question that corresponds to practices *not* performed (RED).

Next, the dashboard results generated in the report, shown in Figure 21, were used to validate the results. Upon validating, it was found that our results do not match with the dashboard results for RS.IM.

The methodology adopted in Figures 20 and 22 were used to attain the following result:

According to the reasoning explained above, it was found that Option 6.2.5 in Figure 20 will be considered *not* performed (RED) for RS.IM-1 because the user has selected Option 3 while providing the data input for Question 6.2. Further, even if Option 4 is selected by the user while providing the data input, the practice for RS.IM-1 (at Option 5) will be considered not performed (RED) because the minimum threshold for R.IM-1 in Question 6.2 has been set as corresponding to Option 3. Therefore, in this case, when the user enters any value that is greater than Option 3, the practice for RS.IM-1 will be considered *not* performed. For the next option mapped for RS.IM-1, i.e., 4.3.4, as user data input is at Option 4, this practice is considered performed (GREEN).

Similarly, for Option 5.10.3 mapped to RS.IM-1, user data input is at Option 4. Hence, this practice is also considered to be performed (GREEN).

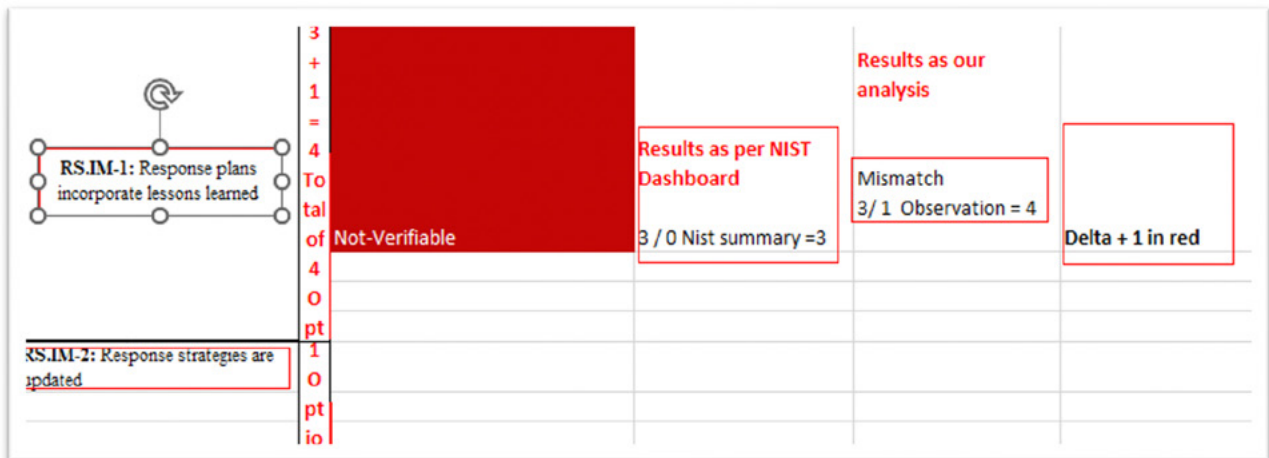


Figure 22: TR Random Selection 1 -Validate

For Option 5.10.3 mapped against sub-category RS.IM-2, the user input is at 5.10.4, i.e., Option 4 is selected, implying that this practice is considered performed (GREEN).

There is a difference of 1 depicted in Figure 22. The total number of practices performed, as seen in Figure 21, is 3. No questions correspond to practices not being performed. On the other hand, in Figures 20 and 22, 3 questions correspond to practices performed, and 1 question corresponds to practices not performed, so delta in Figure 22 is 1 in RED.

Conclusion

In conclusion, the tool overall is a good starting point for a small to mid-size transit agencies to embark on a security maturity journey and secure its operation technology. However, it will need to mature over time to ensure it stays current and relevant to the changing needs of cybersecurity.

MetroLINK can start by adopting the recommendations in the report to enhance the tool and add more questions to ensure that it is comprehensive.

Cybersecurity Assessment Tool for Transit (CATT) Project Team Response to the Independent Evaluation

The following is the CATT project team's response to the independent evaluation performed by SYSUSA v0.1, dated December 19, 2022.

1. The tool guides security professionals at every step to complete the questionnaire with hyperlinks and popup callouts. Additional guidance can be incorporated in the hyperlinks and popups to enable ordinary users with limited security knowledge to take advantage of the tool. Furthermore, some terms are not defined and are therefore open to the end user's interpretation. For example, the term *Service Continuity Plans* has no hyperlink or popup to explain what is required.

Project team response: There is no doubt that more information can be incorporated into the tool. Adding additional information to the tool is considered an enhancement that has not been budgeted. Given the diversity of reviews that have been performed on the tool, we believe the definitions included to date are sufficient to publish at this time.

2. The questions are very simple. In each section, at least one option will apply to the organization, regardless of the organization's size or the maturity of its practices. Therefore there should be no reason for any organization to skip a section, which is currently possible. MetroLINK should modify the CATT to prevent users from skipping any sections. It should be mandatory to select at least one option in every section.

Project team response: Such restrictions could inhibit how the agency chooses to leverage the tool. If the tool was designed to provide evidence of a cybersecurity program for regulatory or other means, such restrictions may be warranted. However, the tool was designed to assist agencies in beginning their journey to develop a cybersecurity program.

3. The report generated from the tool is comprehensive and provides an accurate state of security based on the selected inputs during the assessment. However, when the report is retrieved, the *Revise Report* tab cannot be used to correct the inputs.

Project team response: When the user clicks the *Generate Report* button, the report is generated. The button changes to *Revise Assessment* once the report is generated. The user is then able to click the *Revise Assessment* button to correct inputs. The project team was unable to recreate the issue noted by the independent evaluator.

4. The blue question mark provides some valuable information on the control. However, it can be further enhanced by providing additional reference information or links to NIST CSF to help clarify and interpret the question as intended. In some cases, the information provided is mapped directly to the function itself; in others, it is mapped to the sub-categories with their IDs.

Project team response: There is no doubt that more information can be incorporated into the tool. Adding additional information to the tool is considered an enhancement that has not been budgeted. Given the diversity of reviews that have been performed on the tool, we believe the NIST CSF information included to date is sufficient to publish at this time.

5. In the overview section of the CATT, a brief explanation of each of the five NIST CSF functions can be added to help clarify the questionnaire and to provide additional guidance for the agencies in leveraging the external NIST CSF guidance to complete the questionnaire.

Project team response: There is no doubt that more information can be incorporated into the tool. Adding additional information to the tool is considered an enhancement that has not been budgeted. Given the diversity of reviews that have been performed on the tool, we believe the NIST CSF information included to date is sufficient to publish at this time.

6. The NIST CSF summary dashboard results in the report show the number of practices performed and the number of practices *not* performed for every category within a function based on the user input. Upon comparing the dashboard results with the input values provided by the user, we discovered that some of the dashboard results do not match the input.

Project team response: This tool was designed as an on-ramp for organizations to begin using NIST processes. Many organizations find NIST confusing and do not use NIST based assessments. The goal was to simplify the NIST family of controls and begin a process for organizations looking at the most relevant assessment indicators (selected by the project team). The Cybersecurity and Infrastructure Security Administration's (CISA's) existing Cyber Resilience Review (CRR) was used as a basis for the tool; the team added references to the NIST CSF to align with the broader intent of using it as the foundation for U.S. cybersecurity practices. We leveraged the existing CRR to NIST CSF crosswalk to append NIST CSF information to the tool. However, this crosswalk is not exact and all-encompassing, given the adaptations made to the CRR. Additional work could be done to better fit the tool to the NIST CSF. However, this additional work is considered an enhancement that has not been budgeted. Given the diversity of reviews that have been performed on the tool, we believe the NIST CSF information included to date is sufficient to publish at this time.



U.S. Department of Transportation
Federal Transit Administration

U.S. Department of Transportation
Federal Transit Administration
East Building
1200 New Jersey Avenue, SE
Washington, DC 20590
<https://www.transit.dot.gov/about/research-innovation>