A Conceptual Foundation For Critical Infrastructure Information Security Awareness

Marufu Lamidi & Israel Emmanuel | Cybersecurity, Forensics, & Information Assurance | Century College

Summer 2023

Introduction

In March 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). CIRCIA is aimed at improving America's cybersecurity by requiring the Cybersecurity and Infrastructure Security Agency (CISA) to develop and implement regulations that will allow CISA to rapidly analyze security reports across critical infrastructure sectors, deploy resources to victims of cyber attacks, and share security information with network defenders to warn other potential victims. Regardless of the maturity and sophistication of an organization's cybersecurity infrastructure, the information security posture depends on the employees' threat awareness level and cultivated habits that provide a critical element of deterrence. While security awareness programs can be focused on one specific group (e.g., leadership), to be effective and holistic, the program should address all stakeholders, including leadership, employees, third-party vendors, and external service providers.

Problem

The increase in connected physical operating technology devices has increased the attack surface, leading to the rise of cyberattacks against these technologies. Operational technology is poorly protected and vulnerable to cyberattacks due to the shortage of enough operational technology security professionals compared to IT security counterparts. The cost of launching successful cyberattacks by criminals is consistently decreasing. Unfortunately, this decrease in cost has also led to a rise in the number of attacks.

Facts

- Cybersecurity threats exploit critical infrastructure systems' increased complexity and connectivity, putting the nation's security, economy, public safety, and health at risk.
- According to the FBI Internet Crime Complaint Center's annual report, more than one-third of ransomware attacks reported to the FBI in 2022 impacted organizations in a critical infrastructure sector,
- The largest sector hit by ransomware in 2022 was the healthcare and public health sector, with a share of 210 attacks. Of the 2,385 ransomware attacks reported to the FBI in 2022, 870 hit critical infrastructure organizations.
- Stuxnet computer virus Cyber targeted attack that disrupted the Iranian nuclear program, which damaged centrifuges used to separate nuclear material, is an example of a high-profile cyber-attack against critical infrastructure.
- Cybersecurity risk does not only affect organizational business transactions and reputation, it also affects the company's bottom line. It harms an organization's ability to innovate, drives up costs, affects revenue, negatively impacts customer loyalty, and increases its overall risk management.
- Most critical infrastructure and manufacturing cyber-attacks are aimed at industrial control systems rather than stealing data.
- The American States and Trend Micro research organization surveyed 500 US critical infrastructure suppliers, 54% reported attempts to control systems, and 40% reported systems shutdown attempts.

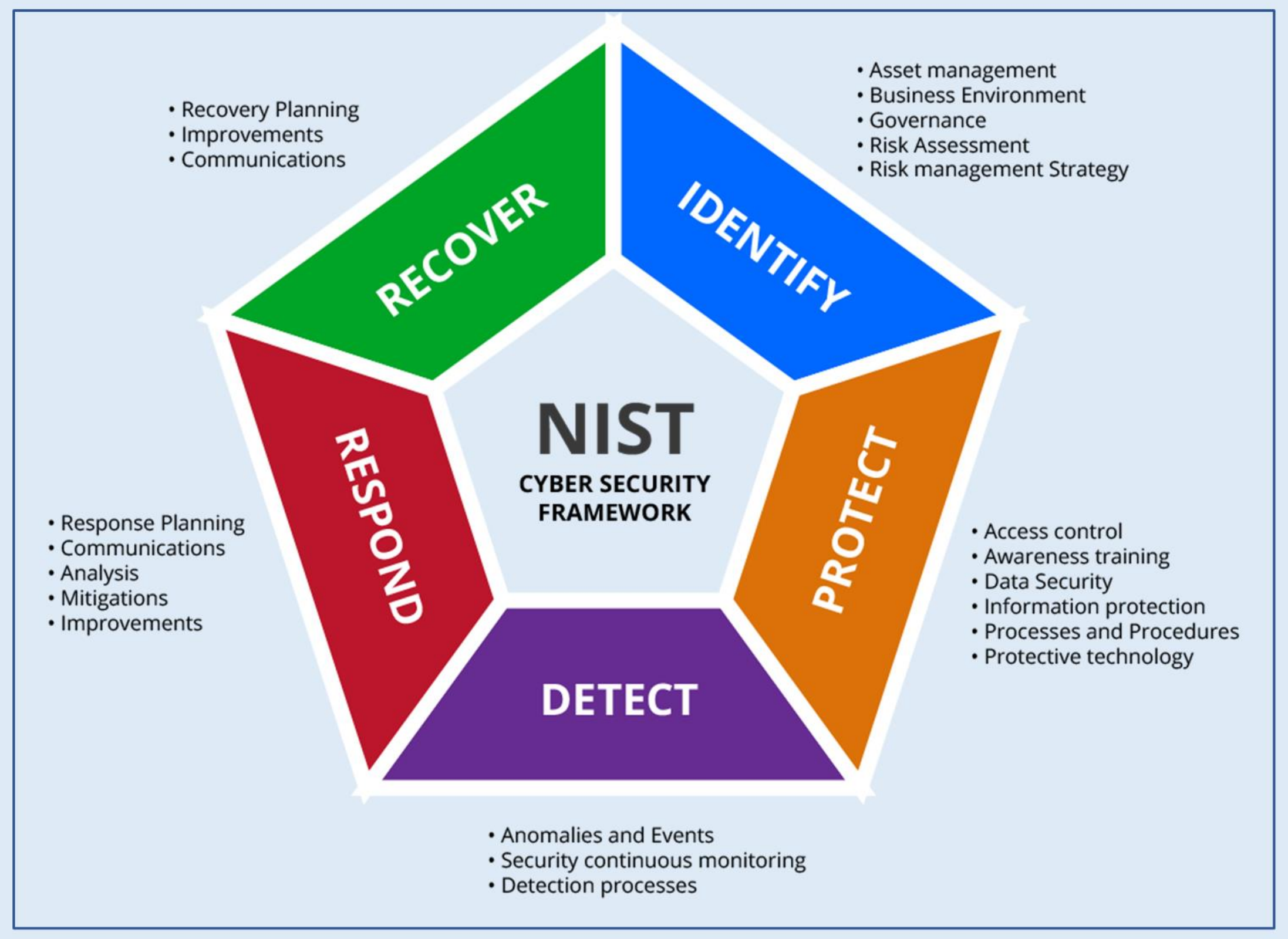
Project Scope, Goals & Objectives

The project aims to provide a roadmap for reducing cybersecurity risk that aligns with the organization`s critical infrastructure. It starts by creating a current profile and desired cybersecurity target outcome profile. The Current Profile indicates current cybersecurity outcomes. The Target Profile is the desired cybersecurity risk management goal. It compares Current Profile and Target Profile, revealing gaps needed to meet cybersecurity risk management objectives.

Recommended Solutions

Understanding specific cybersecurity activities that are common across all critical infrastructure sectors is essential. In the figure below, the National Institute of Standards and Technology (NIST) provides a framework listing Functions, Categories, Subcategories, and Informative references for managing cybersecurity risk.

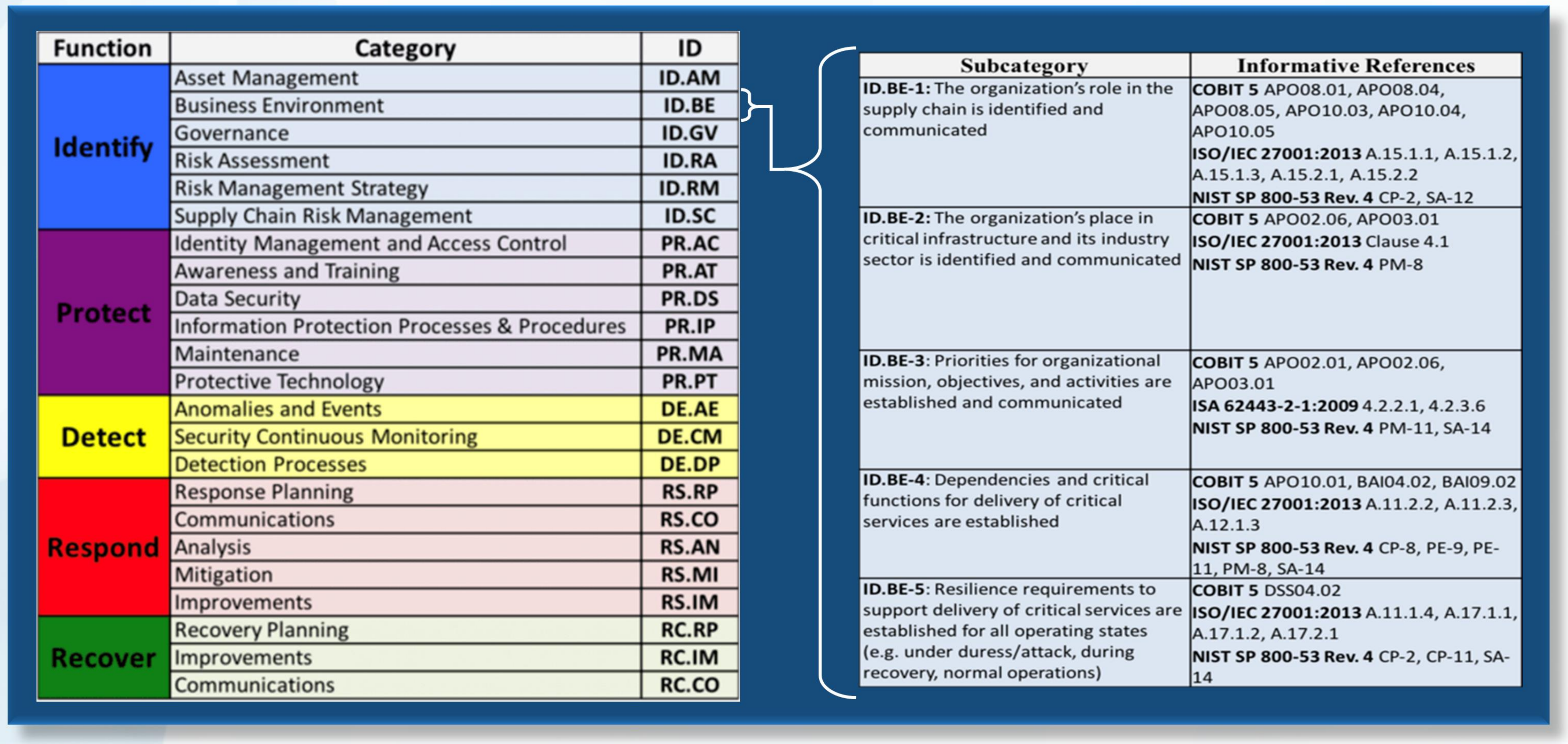
An Information Security Awareness Campaign is an organized effort to make an organization aware of risks to personal and organizational and to provide personnel with the knowledge and skills necessary to avoid those risks. Following the best practices for implementing a security awareness program will help to develop organizational cyberthreat intelligence and good habits.



The National Institute of Standards and Technology (NIST) recommends the following steps to establish a cybersecurity program or review previously existing cybersecurity programs to determine their effectiveness.

- **Step 1:** Prioritize and Scope. Organizations should identify their business/mission objectives and high-level organizational priorities.
- **Step 2**: Orient - Identify threats and vulnerabilities of those systems and assets by looking at the source.
- **Step 3:** Create a Current Profile: Use the framework to develop category and subcategory outcomes to provide baseline information.
- **Step 4:** Conduct a Risk Assessment: Analyze your operational environment to discern the cybersecurity event likelihood and organization impact of such an event.
- **Step 5:** Create a Target Profile: This should be focused on the framework assessment of the Categories and Subcategories that describe the organization's desired cybersecurity outcomes.
- **Step 6:** Determine, Analyze, and Prioritize Gaps: The organization should compare the Current. Profile and the Target Profile to determine and address gaps. Determines resources necessary to address the gaps.
- **Step 7**: Implement Action Plan. Address any identified gaps by adjusting current cybersecurity practices to the target profile.

Industrial control systems and connected devices security must catch up to information systems (IT) security. For society to benefit from Operational technology, cybersecurity must protect data and systems that connect critical infrastructure to networks and the internet. The same level of public confidence in cybersecurity that keeps aircraft in the air is necessary for critical national infrastructure. Organizations can use the NIST framework to create or improve existing cybersecurity programs. In addition, critical infrastructure cybersecurity professionals could use these steps repeatedly as necessary to improve critical infrastructure cybersecurity continuously. Organizations may also use this process to align their cybersecurity program with their desired Framework Implementation Tier.



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Anticipated Results

The current security profile will reveal how critical infrastructure organizations align or deviate from NIST's five high-level core categories and subcategories standards.

Organizations should conduct cyber and physical security exercises with government and industry partners (CISA) to enhance security and resilience of critical infrastructure. These exercises will provide all stakeholders with effective and practical mechanisms to identify best practices, lessons learned, and areas for improvement in plans and procedures.

The project should help critical infrastructure organizations develop action plans that strengthens existing cybersecurity practices and reduces cybersecurity risk.

Organization should conduct standard cybersecurity training curriculum that incorporate cybersecurity training into the physical security and safety educational programs.

Project Cost

Action Item	Services	Unit Cost ($ Per Hour)	Quantity / Hour	Unit Total Cost ($)
Current security profile assessment	Consultant	200.00	28	5600.00
Develop a target security profile	Consultant	200.00	16	3200.00
Gap Analysis	Consultant	160.00	8	1280.00
Training Organizational Personnel	Consultant	90.00	12	1081.00
Develop or update security policies	Consultant	125.00	8	1000.00
				12160.00

Conclusion

The cybersecurity risk for critical infrastructure framework is not a one-size-fits-all approach. Organizational threats, vulnerabilities, and risk tolerance could be unique from one organization to the other. Therefore, organizations should determine critical activities that are important to their service delivery to maximize and prioritize their organizational investment in the better management of their cybersecurity risk.

Given that humans are often the weakest link in the chain when it comes to information security. Many modern cyber incidents are caused by a lack of knowledge, skills, and personnel preparedness to detect and prevent cyber-attacks. Information security awareness campaigns that make organization's employees aware of risks to personal and organizational information should be holistic in nature provide adequate training and skills necessary to avoid cyber risks.

References

1. Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 National Institute of Standards and Technology April 16, 2018 Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (nist.gov)
2. Cybersecurity Drive. Ransomware hit critical infrastructure hard in 2022, FBI says. https://www.cybersecuritydive.com/news/ransomware-critical-infrastructure-2022/645068/#:~:text=Of%20the%202%2C385%20ransomware%20attacks,in%202022%2C%20the%20FBI%20said.
3. Allianz Global Corporate & Specialty Expert risk article | June 2016 https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html#:~:text=The%20most%20high%20profile%20example,used%20to%20separate%20nuclear%20material.
4. http://www.nist.gov/cyberframework/

Cybersecurity, Forensics, and Information Assurance
Cybersecurity and Information Assurance Track (AAS)

3300 Century Avenue North
White Bear Lake, Minnesota 55110
www.century.edu | 651.779.3300