Commercial Facilities Sector Cybersecurity Framework Implementation Guidance

2015

Homeland Security

Foreword

The National Institute of Standards and Technology (NIST) released the 2014 *Framework for Improving Critical Infrastructure Cybersecurity* (Framework) as a voluntary, risk-based set of standards and best practices to help organizations of all sizes manage cybersecurity risks in any sector. The Department of Homeland Security (DHS) recognizes that many sectors have a distinct set of existing tools and standards that can help implement the Framework's risk-based approach. With that in mind, we worked with our private sector partners and the Office of Cybersecurity and Communications to develop this sector-specific Cybersecurity Framework Implementation Guidance (hereafter Implementation Guidance) to provide organization and structure to today's multiple approaches to cybersecurity.

This Implementation Guidance aims to simplify the process for all organizations in the Commercial Facilities Sector—regardless of their size, cybersecurity risk, or current level of cybersecurity sophistication—to apply the principles and best practices of risk management. Ultimately, the Framework and this Implementation Guidance are focused on helping individual organizations reduce and better manage their cybersecurity risks, contributing to a more secure and resilient sector overall.

The Department of Homeland Security appreciates the dedication and technical expertise of all members of the Commercial Facilities Sector Coordinating Council (SCC) who participated in the development of this Implementation Guidance, as well as all the inputs provided by public and private stakeholders.

Commercial Facilities Sector organizations can use the Implementation Guidance to determine how best to implement the Framework, which provides a repeatable process to identify and prioritize cybersecurity improvements and choose investments that maximize the impact of each dollar spent. As you use the Implementation Guidance, I ask for your continued feedback to update and improve the document and make it a robust and valuable guide for your organization as well as your sector partners and peers.

I encourage your use of and reference to the NIST Framework and this Implementation Guidance as we work together to improve the security and resilience of our Nation's critical infrastructure from cyber and other attacks.

Caitlin Durkovich
Assistant Secretary
Office of Infrastructure Protection
National Protection and Programs Directorate
Department of Homeland Security

Table of Contents

Introduction

The National Institute of Standards and Technology (NIST) released the voluntary *Framework for Improving Critical Infrastructure Cybersecurity* (Framework) in February 2014 to provide a common language that critical infrastructure organizations[1] can use to assess and manage their cybersecurity risk. The Framework enables an organization—regardless of its sector, size, degree of risk, or cybersecurity sophistication—to apply the principles and effective practices of cyber risk management to improve the security and resilience of its critical infrastructure. It recommends an approach that enables organizations to prioritize their cybersecurity decisions based on individual business needs without additional regulatory requirements.

Given the broad nature of the Framework, organizations cannot simply be "compliant" with the Framework or "adopt" it. Organizations have unique cybersecurity risks, including different threats, vulnerabilities, and tolerances, all of which affect benefits from investing in cybersecurity risk management. Rather, organizations must apply the principles, best practices, standards, and guidelines to their specific context and implement practices based on their own needs.

The Commercial Facilities Sector embraces the flexibility the Framework offers. The U.S. Department of Homeland Security (DHS), as the Sector-Specific Agency (SSA), worked with the Commercial Facilities Sector Coordinating Council (SCC) and Government Coordinating Council (GCC) to develop this Implementation Guidance specifically for Commercial Facilities Sector owners and operators. This Implementation Guidance provides Commercial Facilities Sector organizations with:

- Background on the Framework terminology, concepts, and benefits of its use;
- A mapping of existing cybersecurity tools and resources used in the Commercial Facilities Sector that can support Framework implementation; and
- Detailed Framework implementation steps tailored for Commercial Facilities Sector owners and operators.

The Framework applies to organizations of any size and level of cybersecurity sophistication. For organizations with no formal risk management practices, the Framework provides the foundational principles and elements for building a cybersecurity program. For organizations with a robust cybersecurity program in place, implementing the Framework provides a means to identify areas for improvement and demonstrate that the organization's program aligns with a nationally recognized approach for cyber risk management.

[1] This document uses the term "organization" to describe an operational entity of any size that uses the same cybersecurity risk management program within its different components, and that may individually use the Framework. This Implementation Guidance is designed for any organization—whether the organization is the entire enterprise or a process within that enterprise.

Framework Overview and Benefits

To establish critical infrastructure cybersecurity as a national priority, President Obama signed Executive Order 13636: Improving Cybersecurity Critical Infrastructure in February 2013. The Executive Order charged NIST to develop the *Framework for Improving Critical Infrastructure Cybersecurity* and led DHS to develop the Critical Infrastructure Cyber Community (C³) Voluntary Program—which now serves as a central repository for government and private sector tools and resources. The C³ Voluntary Program provides critical infrastructure sectors; academia; and State, local, tribal, and territorial (SLTT) governments with businesses tools and resources to use the Framework and enhance their cyber risk management practices. DHS, as the Commercial Facilities Sector-Specific Agency, is also a key source of cybersecurity information and tools for sector organizations.

The Framework, released in February 2014, is based on a collection of cybersecurity standards and industry best practices. The Framework:

- Provides guidance on risk management principles and best practices;
- Provides common language to address and manage cybersecurity risk;
- Outlines a structure for organizations to understand and apply cybersecurity risk management; and
- Identifies effective standards, guidelines, and practices to manage cybersecurity risk in a cost-effective manner based on business needs.

The Framework broadly applies across all organizations, regardless of size, industry, or cybersecurity sophistication. Whether an organization has a mature risk management program and processes, is developing a program or processes, or has no program or processes, the Framework can help guide an organization in improving cybersecurity and thereby improve the security and resilience of critical infrastructure as a whole.

Potential Benefits of Implementing the Framework

Each organization will choose if, how, and where it will use the Framework based on its own operating environment. Choosing to implement the Framework does not imply that an existing cybersecurity and risk management approach is ineffective or needs to be replaced. Rather, it means that the organization wishes to take advantage of the benefits that the Framework offers. Specifically, implementing the Framework provides a mechanism for organizations to:

- Assess and specifically **describe its current and targeted cybersecurity posture**.
- **Identify gaps** in its current programs and processes.
- Identify and **prioritize opportunities for improvement** using a continuous and repeatable process.
- **Assess progress** toward reaching its target cybersecurity posture.
- **Demonstrate the organization's alignment** with the Framework's nationally recognized best practices.
- Highlight any current practices that might **surpass the Framework's recommended practices**.
- **Communicate its cybersecurity posture in a common, recognized language** to internal and external stakeholders—including customers, regulators, investors, and policymakers.

NIST designed the Framework to provide a nationally recognized approach to cyber risk management using best practices and proven processes. As more sectors and organizations implement the Framework, its approach will serve as an accepted baseline for cybersecurity practices in critical infrastructure organizations. Early adoption of the Framework's principles may better position Commercial Facilities Sector organizations to receive additional potential benefits in the future:

- **More attractive cybersecurity insurance coverage** — As cyber risks grow, insurance agencies are developing new and refined approaches to evaluate clients' premiums based on their use of sound cybersecurity practices. Insurance coverage may increasingly encourage or require the use of nationally recognized cyber risk management processes. Framework implementation provides an additional, widely accepted means for an organization to measure its cybersecurity posture and demonstrate continuous improvement.
- **Prioritized funding or technical assistance** — The Federal Government provides several hands-on tools that will help an organization assess their current-state of cybersecurity practices and identify areas to grow their cybersecurity resilience. Commercial Facilities Sector organizations are encouraged to visit the US-CERT Critical Infrastructure Community (C^3) Voluntary Program Webpage for additional information related to both facilitated and self-service risk assessment resources. The Federal government uses this assessment to help organizations prioritize next steps, depending on their level of cybersecurity maturity. For example, the government offers preparedness support, assessments, training of employees, and advice on best practices. Under this incentive, the primary criteria for assistance would be criticality, security, and resilience gaps. Owners and operators in need of incident response support will never be denied assistance based on cybersecurity maturity and/or level of prior engagement with the use of the Framework.
- **Demonstration of commitment to cybersecurity —** The Framework does *not* protect any organization from liability in the event of a cyber incident. However, implementation of the Framework provides an organization with a mechanism to demonstrate its proven track record of implementing and continuously evaluating cyber risk management practices appropriate for its individual risks.
- **Government recognition** — For interested organizations, DHS seeks to recognize those organizations and sectors that use the Framework and participate in the C^3 Voluntary Program, regardless of size and maturity level.
- **Workforce development —** Organizations that use the Framework will have a better understanding of the technical capabilities their organization requires and, therefore, the skills required of their cyber workforce. A more accurate understanding of these needs can guide activities such as recruiting, workforce design, and training of existing personnel.

Framework Structure

The Framework uses three main components—the Framework Core Elements, the Framework Implementation Tiers, and the Framework Profiles—that enable an organization to identify its cybersecurity practices, define the maturity of its cybersecurity approach, and profile its current and target (or goal) cybersecurity posture. These three components help an organization examine its cybersecurity activities in terms of individual organizational priorities.

TABLE 1.—Framework Structure.

The Framework Structure		
Core	**Implementation Tiers**	**Profile**
Five functions provide a high-level, strategic overview of the lifecycle of an organization's cybersecurity risk, and are further divided into Categories and Subcategories.	Tiers provide context for how an organization views cybersecurity risk and their in-place processes.	The profile represents the outcomes based on business needs that an organization has selected from the Framework Categories.
Functions 1. Identify 2. Protect 3. Detect 4. Respond 5. Recover	**Tiers** 1. Partial 2. Risk Informed 3. Repeatable 4. Adaptive	**Profiles** 1. Current Profile 2. Target (Goal) Profile

Framework Core

The Framework Core uses four elements that enable stakeholder identification of cybersecurity focus areas:

1. **Functions:** The Core Functions are five areas on which organizations can focus their attention to develop a strategic view of their cybersecurity postures. Although the Functions do not replace a risk management process, they provide a concise way for senior executives and others to distill the fundamental concepts of cybersecurity risk so they can assess how identified risks are managed, and see how their organizations align with existing cybersecurity standards, guidelines, and practices. The five Functions are:
    a. Identify—Lay the foundation for effective Framework use. The activities in the Identify Function include systems, assets, data, capabilities, and other foundational elements that are critical to the organization.
    b. Protect—Develop and identify appropriate safeguards to ensure delivery of critical infrastructure services.
    c. Detect—Identify and implement the tools to identify the occurrence of cybersecurity incidents.
    d. Respond—Use the tools and activities to support the containment of a cybersecurity event.
    e. Recover—Bolster resilience and restore any capabilities or services impaired by the cybersecurity event.
2. **Categories:** The Framework subdivides Functions into Categories, which are activities or processes that support identification, protection, detection, response, or recovery. In the Identify Function, for example, Categories include Governance, Business Environment, and Asset Management.
3. **Subcategories:** Subcategories are the subcomponents of Categories and detail the specific outcomes of the activity, tool, or approach used in the Category.
4. **Informative References:** References are specific sections of standards, guidelines, and practices. References provide a method to achieve the outcomes associated with each Subcategory. The Framework identified several national and international standards that organizations can use to achieve the outcomes in each Subcategory. This Implementation Guidance identifies additional standards, tools, and resources that Commercial Facilities Sector organizations may use to achieve the outcomes of each Category and Subcategory.

Table 2 provides an overview and examples of the four Framework Core elements.

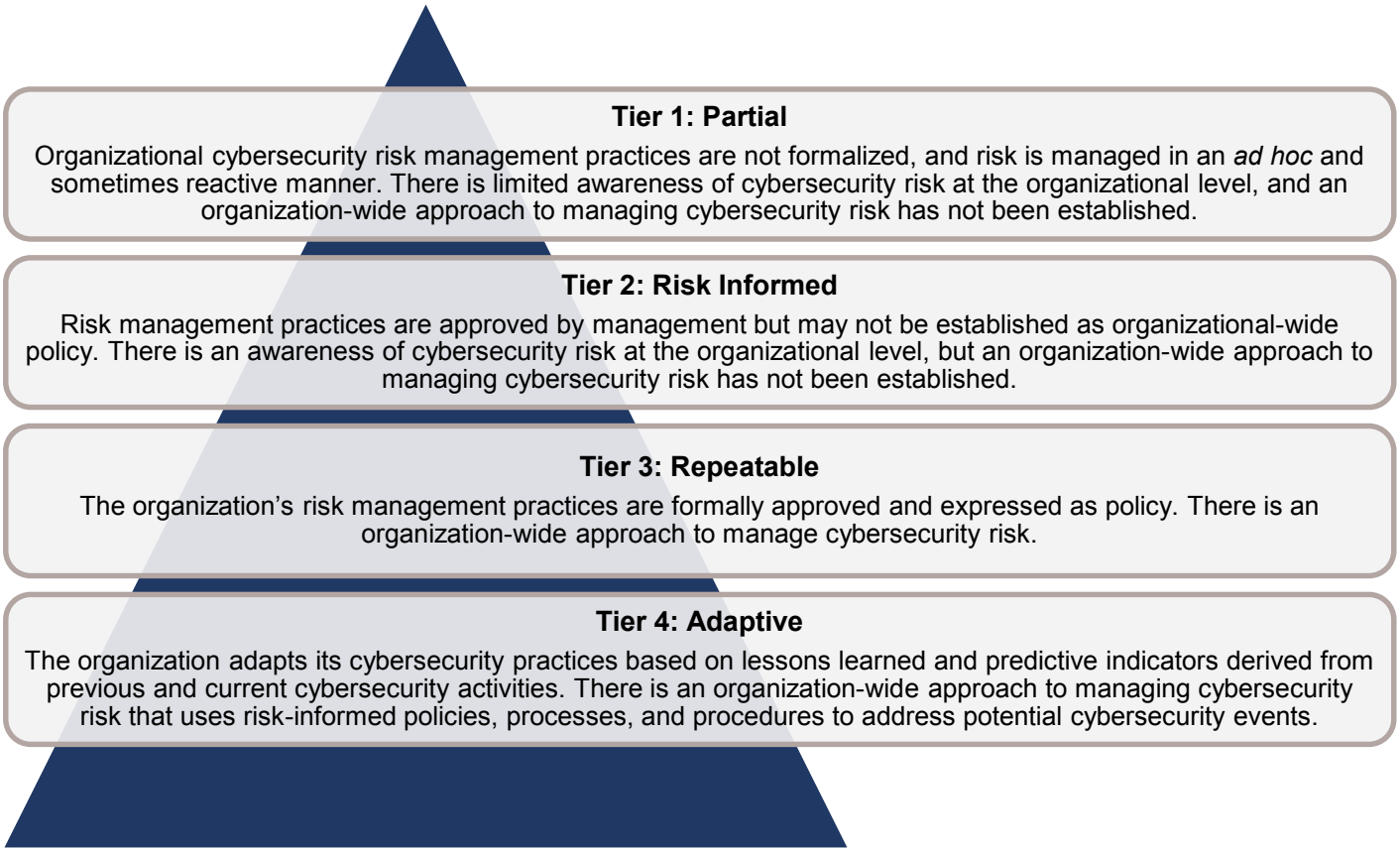
TABLE 2.—Framework Core Structure.

Functions	Categories	Subcategories	Informative References
Organize **basic cybersecurity activities** at their highest level and align with existing methodologies for incident management.	Subdivide Functions into groups of particular **cybersecurity activities** or programmatic **needs**.	Divide further into **specific outcomes** of technical and management activities. **Expressed as *results*.**	Reference specific sections of standards, guidelines, and practices that **illustrate a method to achieve the outcomes** of each Subcategory.
IDENTIFY	**Asset Management**	Ex: Organizational communication and data flows are mapped	Ex: NIST SP 800-53: AC-4, CA-3, CA-9, PL-8, etc.
		Ex: Resources are prioritized based on their classification, criticality, and business value	Ex: NIST SP 800-53: CP-2, RA-2, SA-14, etc.
	Business Environment		
	Governance		
	Risk Assessment		
	Risk Management Strategy		
PROTECT	**Access Control**		
	Awareness and Training		
	Data Security		
	Information Protection Processes and Procedures		
	Maintenance		
	Protective Technology		
DETECT	**Anomalies and Events**		
	Security Continuous Monitoring		
	Detection Processes		
RESPOND	**Response Planning**		
	Communications		
	Analysis		
	Mitigation		
	Improvements		
RECOVER	**Recovery Planning**		
	Improvements		
	Communications		

Implementation Tiers

The Framework Implementation Tiers outline how an organization views and handles cybersecurity risk and the processes in place to handle that risk. There are four Implementation Tiers, shown in Figure 1.

FIGURE 1.—Framework Tiers.



Note that the Framework encourages progression toward a higher Tier, so long as that change would cost-effectively reduce cybersecurity risk for the individual organization. Although the Framework Core elements do not directly correspond to specific Implementation Tiers, the Core can inform an organization's Tier determination.

Framework Profile

The Framework Profile aligns to the Framework core elements and establishes an organization's cybersecurity state. The Profile can represent an organization's current cybersecurity posture or its target cybersecurity state. Organizations can compare their present and goal stance, and identify the best course of action to reach that end state. Ultimately, Profiles provide a mechanism to reduce cybersecurity risk with outcomes based on an organization's business needs. This Implementation Guidance will provide further instructions on how an organization can develop its Current and Target Profile using the Framework's seven-step implementation approach.

Cybersecurity Tools and Resources to Support Framework Implementation

The Framework's Informative References mapped a set of broad national and international cybersecurity standards to the Framework Core, providing owners and operators with sample methods to achieve the cybersecurity outcomes described by each Function, Category, and Subcategory. This section outlines additional existing cybersecurity tools, standards, and approaches used within the Commercial Facilities Sector and provides an initial mapping of those methods to the Functions, Categories, and Subcategories. This mapping may help Commercial Facilities Sector owners and operators identify additional tools and resources—many of which they may already be using or considering—that can help them implement the Framework or demonstrate how they are already applying Framework concepts.

TABLE 3.—Existing Commercial Facilities Sector Cybersecurity Risk Management Approaches.

Name	Summary	Additional Information
Cyber Resilience Review (CRR)	This resource evaluates an organization's operational resilience and cybersecurity practices across 10 domains.	CRR Information CRR NIST Framework Crosswalk
Cyber Security Evaluation Tool (CSET)	This tool guides users through a step-by-step process to assess their control system and information technology network security practices against recognized industry standards.	Assessment Program Overview CSET Fact Sheet

TABLE 4.—Existing Subsector Cybersecurity Risk Management Approaches.

Lodging Subsector

Name	Summary	Additional Information
Payment Card Industry Data Security Standards (PCI-DSS)	PCI-DSS establishes worldwide information security standards to help organizations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to not only retail operations, but also all organizations that hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.	Payment Card Industry Data Security Standards
Protective Measures Guide for the U.S. Lodging Industry	This DHS Guide provides options for hotels to consider when implementing protective measures. To enhance a hotel's cybersecurity program, the guide recommends basic security precautions to prevent sensitive information falling into the wrong hands.	Commercial Facilities Publications
Hotel Security and Safety Assessment Form	This form is designed to help hotel customers assess health, safety, and security attributes of a given hotel property.	Hotel Security and Safety Assessment Form

Outdoor Events Subsector

Name	Summary	Additional Information
Protective Measures Guide for the U.S. Outdoor Venues Industry	This DHS protective measures guide provides an overview of best practices and protective measures designed to assist owners and operators in planning and managing security at their facilities or events. It includes measures to assist in protecting information and vital computer systems.	Protective Measures Guide for the U.S. Outdoor Venues Industry (For Official Use Only; available on Homeland Security Information Network – Critical Infrastructure)
Risk Assessment Guide for Rides and Attractions	A risk assessment overview presented at a 2014 conference hosted by the International Association of Amusement Parks and Attractions (IAAPA).	Risk Assessment Guide for Rides and Attractions

Public Assembly Subsector

Name	Summary	Additional Information
Intercollegiate Athletics Safety and Security Best Practices Guide	Published by the University of Southern Mississippi's National Center for Spectator Sports Safety and Security, this guide presents a list of vetted best practices to assist colligate sports venue operators. It includes sections on cybersecurity and response planning for cyber intrusions.	Intercollegiate Athletics Safety and Security Best Practices Guide

Retail Subsector

Name	Summary	Additional Information
Payment Card Industry Data Security Standards (PCI-DSS)	PCI-DSS establishes worldwide information security standards to help organizations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to not only retail operations, but also all organizations that hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.	Payment Card Industry Data Security Standards
ISO/IEC 27001:2013	The International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) 27002:2013 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size, or nature.	ISO/IEC 27001:2013
Critical Security Controls (CSC) for Effective Cyber Defense	The Council on CyberSecurity's Critical Security Controls is a recommended set of actions for cyber defense that provide specific and actionable ways to thwart the most pervasive attacks. The Controls have been developed and maintained by an international, grassroots consortium which includes a broad range of companies, government agencies, institutions, and individuals from every part of the ecosystem who have banded together to create, adopt, and support the Controls.	Critical Security Controls for Effective Cyber Defense

Name	Summary	Additional Information
Control Objectives for Information and Related Technology (COBIT 5)	COBIT 5 is the latest edition of ISACA's globally accepted framework, providing an end-to-end business view of the governance of enterprise IT that reflects the central role of information and technology in creating value for enterprises. The principles, practices, analytical tools, and models found in COBIT 5 embody thought leadership and guidance from business, IT, and governance experts around the world.	Control Objectives for Information and Related Technology

Sports Leagues Subsector

Name	Summary	Additional Information
Protective Measures Guide for U.S. Sports Leagues	This DHS guide provides an overview of protective measures designed to assist sports teams and owners/operators of sporting event facilities in planning and managing security at their facilities. The guide includes a section on cybersecurity, including a list of protective measures recommended for use to address information and computer systems security.	Protective Measures Guide for U.S. Sports Leagues (For Official Use Only; available on Homeland Security Information Network – Critical Infrastructure)
IAVM 2015 Venue Safety and Security Survey	The International Association of Venue Managers' (IAVM) 2015 Venue Safety and Security Survey reports on a comprehensive list of safety and security practices and procedures in use at venues today. Learn what venues like yours are doing to secure their premises and ensure the safety of their patrons.	IAVM 2015 Venue Safety and Security Survey

Framework Mapping

Subject matter experts identified existing cybersecurity tools and approaches in the Commercial Facilities Sector and evaluated them against the Functions, Categories, and Subcategories of the Framework. When all or a portion of an existing tool or approach was determined to align to a particular Subcategory, it was marked as such in Table 5. To determine whether a tool or approach mapped to a particular Subcategory, the sector considered this key question: can the tool or approach help an organization further understand or address the particular Subcategory and achieve the associated outcome? Based on this question, many sector-level documents and approaches do help organizations address the Framework.

This initial mapping is a first attempt at aligning existing tools and approaches to the Framework using open-source research. These six tools listed in Table 5 can be used across the Commercial Facilities Sector unlike some of the approaches listed above, which only apply to certain subsectors of the sector. In some cases, access to the tools and approaches was not available via open-source research, so fact sheets and program descriptions were used to hypothesize where tools and approaches aligned. This mapping is designed to be altered in future versions by sector stakeholders with a solid understanding of the tools and approaches.

TABLE 5.—Commercial Facilities Sector Framework Mapping Matrix.

Function	Category	Subcategory	CRR	CSET	PCI	ISO 27001/2	CSC	COBIT
IDENTIFY (ID)	**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 business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	X	X		X	X	X
		ID.AM-2: Software platforms and applications within the organization are inventoried	X	X	X	X	X	X
		ID.AM-3: Organizational communication and data flows are mapped	X	X	X	X	X	X
		ID.AM-4: External information systems are catalogued	X	X	X	X		X
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	X	X		X		X
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	X	X	X	X		X

Function	Category	Subcategory	CRR	CSET	PCI	ISO 27001/2	CSC	COBIT
IDENTIFY (ID)	**Business Environment (ID.BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	X	X		X		X
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	X	X		X		X
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	X	X				X
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	X	X		X		
		ID.BE-5: Resilience requirements to support delivery of critical services are established	X	X	X	X		X
IDENTIFY (ID)	**Governance (ID.GV):** The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established	X	X		X		X
		ID.GV-2: Information security roles and responsibilities are coordinated and aligned with internal roles and external partners	X	X		X		X
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	X	X		X		X
		ID.GV-4: Governance and risk management processes address cybersecurity risks	X	X	X			X

Function	Category	Subcategory	CRR	CSET	PCI	ISO 27001/2	CSC	COBIT
IDENTIFY (ID)	**Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	X	X	X	X	X	X
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	X	X		X		
		ID.RA-3: Threats, both internal and external, are identified and documented	X	X				X
		ID.RA-4: Potential business impacts and likelihoods are identified	X	X				X
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	X	X	X	X		X
		ID.RA-6: Risk responses are identified and prioritized	X	X				X
IDENTIFY (ID)	**Risk Management Strategy (ID.RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	X	X				X
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	X	X				X
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	X	X				
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	X	X	X	X	X	X
		PR.AC-2: Physical access to assets is managed and protected	X	X	X	X		X
		PR.AC-3: Remote access is managed	X	X	X	X		X
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	X	X	X	X	X	
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	X	X	X	X		

Function	Category	Subcategory	CRR	CSET	PCI	ISO 27001/2	CSC	COBIT
PROTECT (PR)	**Awareness and Training (PR.AT):** The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	X	X		X	X	X
		PR.AT-2: Privileged users understand roles and responsibilities	X	X		X	X	X
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities	X	X		X	X	X
		PR.AT-4: Senior executives understand roles and responsibilities	X	X		X	X	X
		PR.AT-5: Physical and information security personnel understand roles and responsibilities	X	X		X	X	X
PROTECT (PR)	**Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	X	X	X	X	X	X
		PR.DS-2: Data-in-transit is protected	X	X	X	X	X	X
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	X	X	X	X		X
		PR.DS-4: Adequate capacity to ensure availability is maintained	X	X	X	X		X
		PR.DS-5: Protections against data leaks are implemented	X	X	X	X	X	X
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	X	X	X	X		
		PR.DS-7: The development and testing environment(s) are separate from the production environment	X	X	X	X		X

Function	Category	Subcategory	CRR	CSET	PCI	ISO 27001/2	CSC	COBIT
PROTECT (PR)	**Information Protection Processes and Procedures (PR.IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	X	X		X	X	X
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	X	X		X		X
		PR.IP-3: Configuration change control processes are in place	X	X	X	X		X
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	X	X	X	X		X
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	X	X		X		X
		PR.IP-6: Data is destroyed according to policy	X	X	X	X		X
		PR.IP-7: Protection processes are continuously improved	X	X	X			X
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	X	X		X		
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	X	X	X	X		X
		PR.IP-10: Response and recovery plans are tested	X	X	X	X		X
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	X	X	X	X		X
		PR.IP-12: A vulnerability management plan is developed and implemented	X	X	X	X		

Function	Category	Subcategory	CRR	CSET	PCI	ISO 27001/2	CSC	COBIT
PROTECT (PR)	**Maintenance (PR.MA):** Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	X	X		X		X
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	X	X	X	X		X
PROTECT (PR)	**Protective Technology (PR.PT):** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	X	X	X	X	X	X
		PR.PT-2: Removable media is protected, and its use restricted according to policy	X	X	X	X		X
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	X	X	X	X		X
		PR.PT-4: Commercial Facilities and control networks are protected	X	X	X	X	X	X
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner, and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	X	X	X			X
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	X	X	X	X		
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	X	X	X			
		DE.AE-4: Impact of events is determined		X	X			X
		DE.AE-5: Incident alert thresholds are established	X	X	X			X

Function	Category	Subcategory	CRR	CSET	PCI	ISO 27001/2	CSC	COBIT
DETECT (DE)	**Security Continuous Monitoring (DE.CM):** The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	X	X	X		X	X
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	X	X	X			
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	X	X	X	X		
		DE.CM-4: Malicious code is detected	X	X	X	X	X	X
		DE.CM-5: Unauthorized mobile code is detected	X	X		X		
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	X	X		X		X
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	X	X	X			
		DE.CM-8: Vulnerability scans are performed	X	X	X	X		X
DETECT (DE)	**Detection Processes (DE.DP):** Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	X	X	X	X	X	X
		DE.DP-2: Detection activities comply with all applicable requirements	X	X	X	X		
		DE.DP-3: Detection processes are tested	X	X	X	X		X
		DE.DP-4: Event detection information is communicated to appropriate parties	X	X	X	X		X
		DE.DP-5: Detection processes are continuously improved	X	X	X	X		X
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event	X	X	X	X	X	X

Function	Category	Subcategory	CRR	CSET	PCI	ISO 27001/2	CSC	COBIT
RESPOND (RS)	**Commercial Facilities (RS.CO):** Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	X	X	X	X		
		RS.CO-2: Events are reported consistent with established criteria	X	X	X	X		
		RS.CO-3: Information is shared consistent with response plans	X	X		X		
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	X	X				
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	X	X				
RESPOND (RS)	**Analysis (RS.AN):** Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	X	X	X	X		X
		RS.AN-2: The impact of the incident is understood	X	X		X		
		RS.AN-3: Forensics are performed	X	X	X	X		
		RS.AN-4: Incidents are categorized consistent with response plans	X	X		X		
RESPOND (RS)	**Mitigation (RS.MI):** Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained	X	X	X	X		
		RS.MI-2: Incidents are mitigated	X	X	X	X		
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	X	X		X		

Function	Category	Subcategory	CRR	CSET	PCI	ISO 27001/2	CSC	COBIT
RESPOND (RS)	**Improvements (RS.IM):** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	X	X	X	X		X
		RS.IM-2: Response strategies are updated	X	X	X			
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after an event	X	X	X	X	X	X
RECOVER (RC)	**Improvements (RC.IM):** Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	X	X	X			X
		RC.IM-2: Recovery strategies are updated	X	X				X
RECOVER (RC)	**Commercial Facilities (RC.CO):** Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other Computer Security Incident Response Teams (CSIRTs), and vendors.	**RC.CO-1:** Public relations are managed	X	X				X
		RC.CO-2: Reputation after an event is repaired	X	X				X
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	X	X				

Framework Implementation

Implementing the Framework is largely a matter of translating elements of current risk management activities and programs to the Framework Core and Implementation Tiers. For those organizations seeking to actively use the Framework to build a cybersecurity risk management program, the Framework presents a seven-step process for implementation (see Section 3.2 of the Framework document). An organization can use this approach with any cybersecurity standard or tool for managing cybersecurity risk. The seven-step process is shown in Figure 2. The approach can be an iterative process repeated to address the evolving risk environment.

FIGURE 2.—Implementation Steps and Key Activities.

An organization may repeat the steps as needed to continuously assess and improve its cybersecurity. For instance, organizations may find that more frequent repetition of Step 2: Orient improves the quality of risk assessments. Furthermore, organizations may monitor progress through iterative updates to the Current Profile, subsequently comparing the Current Profile to the Target Profile. Organizations may also use this process to align their cybersecurity program with their desired Framework Implementation Tier.

Implementation should include a plan to communicate progress to appropriate stakeholders, such as senior management. This process should integrate into an organization's risk management program and provide feedback and validation to previous steps. Validation and feedback provide a mechanism for process improvement and can increase the overall effectiveness and efficiency of the process.

Step 1: Prioritize and Scope

When implementing the Framework, an organization first identifies its business or mission objectives and its strategic priorities as they relate to cybersecurity. With this information, an organization can make decisions regarding cybersecurity implementation and determine the breadth and scope of systems and assets that support its objectives. An organization can adapt the Framework to support different business lines or processes, which may have different business needs and associated risk tolerance.

Typical risk management processes includes a strategy that frames, assesses, responds to, and monitors risk. Larger enterprises may already use a strategic-level approach to which the enterprise's organizations subscribe. Whether an organization uses a unique approach or that of a larger enterprise, the applicable strategy should describe the identified cybersecurity risks that the organization considers when making investment and operational decisions.

Current threat and vulnerability information (e.g., information from important vendors, communication of Commercial Facilities threats from an information sharing and analysis center, or other threat advisories) may also help inform scoping decisions.

In order to gain familiarity and experience, an organization using the Framework for the first time may apply it to a small subset of operations. For example, an organization may choose to begin with particular business functions because they are already undergoing similar or related risk management efforts. Then, with a greater understanding, the organization can apply the Framework to a broader subset of operations or to additional divisions of the organization.

Step 2: Orient

At this stage, an organization identifies the systems, assets, requirements, and risk management approaches that fall within the scope of the effort. This includes current organization standards and best practices, as well as any additional items that can enable the organization to achieve its critical infrastructure and business objectives for cybersecurity risk management. The organization's risk management program may have already identified and documented much of this information. In general, organizations should focus initially on critical systems and assets and then expand into systems and assets that are less critical or central to their mission.

Additionally, an organization should identify the approach to determine its current risk management and cybersecurity posture. Organizations can use a variety of methods to identify their current cybersecurity posture and create a Current Profile, including self-evaluations or facilitated approaches. In a self-evaluation, an organization may leverage its own resources and expertise, whereas a facilitated approach relies on the expertise of a third party. The value in a self-evaluation is the additional internal cybersecurity awareness and discovery that the activity can generate.

Step 3: Create a Current Profile

The organization develops a Current Profile and determines its current Implementation Tier by mapping current cybersecurity and risk management practices to specific descriptions in the Framework. The purpose of identifying a Current Profile is not only to develop a map between organizational practices and Category and Subcategory outcomes, but also to help understand the extent to which such practices achieve the outcomes outlined by the Framework. To identify the Current Profile, organizations use the evaluation approach (e.g., self-evaluation or facilitated approach) identified in Step 2 to map current cybersecurity approach and outcomes to the corresponding Category and Subcategory outcomes. In many cases, organizations may be able to leverage existing efforts to facilitate this activity. For example, as a part of their risk assessment programs, organizations may have addressed their current state through regular evaluations or internal audits.

The current Implementation Tier describes the degree of rigor and sophistication of the in-scope cybersecurity risk management program (i.e., the Framework usage scope defined in Step 1). To identify the Implementation Tier, the organization maps its current approach to the Implementation Tier descriptions in the Framework document. Implementation Tiers do not apply to the individual Category and Subcategory outcomes in the Framework Core; the organization identifies an Implementation Tier for the in-scope cybersecurity and risk management program as a whole.

Organizations may already be using tools, standards, and processes or complying with industry standards that closely align with the Framework. Some industry and standards organizations have started to publish their own guidance to map existing standards and tools to the Framework elements to facilitate implementation.

Table 6 provides an example of how a mapping can be used to create a Current Profile for a specific Subcategory outcome (see Section PR.AC-3 of the Framework document) for three organizations using three different approaches. A similar table could be built for Implementation Tiers, keeping in mind that Tiers are focused at broader program level risk management. Note that the examples in these tables are intended to be illustrative of the mapping concept and are unlikely to address any specific organization's particular approach. The level of specificity and granularity required for a Profile to be useful will be unique to each organization.

TABLE 6.—Connecting Organizational Approach to Framework.

Organization 1 Internal Controls Approach			
Function	Category	Subcategory	Profiles
			Current
PROTECT (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	• Dial-in access for vendor maintenance is enabled as required and access is disabled when maintenance window completes • Remote access only authorized via encrypted VPN service • Remote access activity logged and monitored • Access to VPN service restricted to organization approved devices • All unauthorized connection attempts to VPN are logged • Immediate disabling of VPN account upon employee termination

Organization 2 Standards Based Approach			
Function	Category	Subcategory	Profiles Current
PROTECT (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	• NIST SP 800-53 Rev 4 AC-17 • NIST SP 800-53 Rev 4 AC-17 (1) • NIST SP 800-53 Rev 4 AC-17 (2) • NIST SP 800-53 Rev 4 AC-19 • NIST SP 800-53 Rev 4 AC-20 • NIST SP 800-53 Rev 4 AC-20 (1)
Organization 3 Exception Approach			
Function	Category	Subcategory	Profiles Current
PROTECT (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	• Not Applicable - No remote access available for in-scope assets and systems

Even though the Framework gives organizations a broad overview of the cybersecurity and risk management domains, it is not all-inclusive, and the organization may have already utilized standards, tools, methods, and guidelines that achieve outcomes not defined by or referenced in the Framework. The Current Profile should identify these practices as well. When appropriate, organizations should consider sharing these practices with NIST to help strengthen and expand the Framework.

Step 4: Conduct a Risk Assessment

Organizations conduct cybersecurity risk assessments to identify cybersecurity risks, evaluate and analyze these risks, and gauge which risks are outside of current tolerances. The results of cybersecurity risk assessment activities allow the organization to develop its Target Profile and identify a Target Implementation Tier, which occurs in Step 5. For organizations that already have a risk management program in place, this activity will be part of regular business practice, and necessary records and information to make this determination may already exist.

Step 5: Create a Target Profile

In creating a Target Profile, the organization should consider:

- Current risk management practices;
- Current risk environment;
- Legal and regulatory requirements;
- Business and mission objectives; and
- Organizational constraints.

The Target Profile outlines the key Category and Subcategory outcomes and associated cybersecurity and risk management standards, tools, methods, and guidelines that will protect against cybersecurity risks in proportion to the risks facing organizational and critical infrastructure security objectives. As highlighted in Step 3, the Framework gives organizations a broad overview of the cybersecurity and risk management domains, but is not all-inclusive. An organization may find it necessary to use standards, tools, methods, and guidelines that achieve outcomes not defined by the Framework. Including these practices in the Target Profile is also beneficial for coordination and future engagement.

Table 7 gives an overview of a hypothetical Target Profile for a specific Subcategory outcome (PR.AC-3) for three organizations using three different approaches. The bold text in the Target Profile highlights where the organization has identified additional practices it desires to use in order to successfully achieve an outcome based on its current risk environment and business and critical infrastructure objectives. Organization 1 has determined that the existing practices it uses for managing remote access are insufficient for addressing its unique risk environment and that additional practices are required. Organization 2 arrives at the same conclusion and identifies additional standards it would like to deploy across the in-scope organization. Organization 3 demonstrates an organization whose Current Profile is identical to the Target Profile for this Subcategory outcome. Such instances will occur when the standards, tools, methods, and guidelines currently deployed by the organization sufficiently fulfill its cybersecurity and risk management requirements. However, this alignment of the Current Profile and Target Profile may only last over the short term since an organization's cybersecurity and risk management requirements will evolve as its risk and operational environments change over time. For instance, an organization may determine that a current practice is no longer necessary or is inadequate and, therefore, omit it from the Target Profile.

In developing a Target Profile, organizations may opt to use a broad approach—considering more effective and efficient risk management approaches across the entire in-scope organizations—rather than examining individual Categories and Subcategories.

In addition to the Target Profile, the organization selects a Target Implementation Tier that applies to the in-scope risk management process. The organization examines each Tier and selects its target (the "desired" state) using the same list of considerations above for the Target Profile. Once a Target Implementation Tier is selected, the organization identifies the cybersecurity practices and risk management activities necessary to achieve that target—considering their ability to meet organizational goals, feasibility to implement, and their ability to reduce cybersecurity risks to acceptable levels for critical assets and resources (i.e., those most important to achieving the organization's business and critical infrastructure objectives).

Using its collection of cybersecurity and risk management standards, tools, methods, and guidelines, the organization documents these desired outcomes in the Target Profile and Target Implementation Tier.

TABLE 7.—Creating a Target Profile.

<table>
<tr><td colspan="5">Organization 1
Internal Controls Approach</td></tr>
<tr><td rowspan="2">Function</td><td rowspan="2">Category</td><td rowspan="2">Subcategory</td><td colspan="2">Profiles</td></tr>
<tr><td>Current</td><td>Target</td></tr>
<tr><td>PROTECT (PR)</td><td>Access Control (PR.AC)</td><td>PR.AC-3: Remote access is managed</td><td>• Dial-in access for vendor maintenance is enabled as required and disabled when maintenance window completes
• Remote access only authorized via encrypted VPN service
• Remote access activity logged and monitored
• Access to VPN service restricted to organization approved devices
• All unauthorized connection attempts to VPN are logged
• Immediate disabling of VPN account upon employee termination</td><td>• Dial-in access for vendor maintenance is enabled as required and disabled when maintenance window completes
• Remote access only authorized via encrypted VPN service
• Remote access activity logged and monitored
• Access to VPN service restricted to organization approved devices
• All unauthorized connection attempts to VPN are logged
• Immediate disabling of VPN account upon employee termination
• Supervisor signature required before VPN account issued
• Biannual review of authorized VPN account list</td></tr>
<tr><td colspan="5">Organization 2
Standards Based Approach</td></tr>
<tr><td rowspan="2">Function</td><td rowspan="2">Category</td><td rowspan="2">Subcategory</td><td colspan="2">Profiles</td></tr>
<tr><td>Current</td><td>Target</td></tr>
<tr><td>PROTECT (PR)</td><td>Access Control (PR.AC)</td><td>PR.AC-3: Remote access is managed</td><td>• NIST SP 800-53 Rev 4 AC-17
• NIST SP 800-53 Rev 4 AC-17 (1)
• NIST SP 800-53 Rev 4 AC-17 (2)
• NIST SP 800-53 Rev 4 AC-19
• NIST SP 800-53 Rev 4 AC-20
• NIST SP 800-53 Rev 4 AC-20 (1)</td><td>• NIST SP 800-53 Rev 4 AC-17
• NIST SP 800-53 Rev 4 AC-17 (1)
• NIST SP 800-53 Rev 4 AC-17 (2)
• NIST SP 800-53 Rev 4 AC-17 (3)
• NIST SP 800-53 Rev 4 AC-17 (4)
• NIST SP 800-53 Rev 4 AC-19
• NIST SP 800-53 Rev 4 AC-19 (5)
• NIST SP 800-53 Rev 4 AC-20
• NIST SP 800-53 Rev 4 AC-20 (1)
• NIST SP 800-53 Rev 4 AC-20 (2)</td></tr>
</table>

Organization 3 Exception Approach				
Function	Category	Subcategory	Profiles	
			Current	Target
PROTECT (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	• Not Applicable - No remote access available for in-scope assets and systems	• Not applicable - No remote access available for in-scope assets and systems

Bold text highlights the differences between the current and target approaches.

Step 6: Determine, Analyze, and Prioritize Gaps

For this step, an organization evaluates its Current Profile and Implementation Tier against its Target Profile and Target Implementation Tier and identifies any potential gaps. It is important to ensure that a broad and holistic outreach to all stakeholder sets is completed in order enable the proper consideration and incorporation of risks across the organization.

A gap exists when there is a desired Category or Subcategory outcome in the Target Profile or program characteristic in the Target Implementation Tier that is not currently satisfied by current cybersecurity and risk management approaches, as well as situations wherein existing practices do not achieve the outcome to the degree of satisfaction required by the organization's risk management strategy. The Gaps column in Table 8 provides a few basic examples of how organizations may choose to accomplish such efforts.

After identifying gaps in both the Profile and Tier, the organization identifies the potential consequences of failing to address such issues. At this point, the organization should assign a mitigation priority to all identified gaps. Prioritization of gaps should include examination of existing risk management practices, the current risk environment, legal and regulatory requirements, business and mission objectives, and any other applicable organizational limitations or considerations.

Once each gap is assigned a mitigation priority, the organization determines potential mitigation efforts and performs a cost-benefit analysis (CBA) on each option. The organization creates a plan of prioritized mitigation actions—based on available resources, business needs, and current risk environment—to move from the existing state to the desired or target state. If the organization is at its target state, it would seek to maintain its security posture in the face of ongoing changes to the risk environment.

TABLE 8.—Identifying Implementation Gaps.

Organization 1 Internal Controls Approach					
Function	Category	Subcategory	Profiles		
			Current	Target	Gaps
PROTECT (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	• Dial-in access for vendor maintenance is enabled as required and disabled when maintenance window completes • Remote access only authorized via encrypted VPN service • Remote access activity logged and monitored • Access to VPN service restricted to organization approved devices • All unauthorized connection attempts to VPN are logged • Immediate disabling of VPN account upon employee termination	• Dial-in access for vendor maintenance is enabled as required and disabled when maintenance window completes • Remote access only authorized via encrypted VPN service • Remote access activity logged and monitored • Access to VPN service restricted to organization approved devices • All unauthorized connection attempts to VPN are logged • Immediate disabling of VPN account upon employee termination • **Supervisor signature required before VPN account issued** • **Biannual review of authorized VPN account list**	• Supervisor signature required before VPN account issued • Biannual review of authorized VPN account list

Organization 2 Standards Based Approach					
Function	Category	Subcategory	Profiles		
			Current	Target	Gaps
PROTECT (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	• NIST SP 800-53 Rev 4 AC-17 • NIST SP 800-53 Rev 4 AC-17 (1) • NIST SP 800-53 Rev 4 AC-17 (2) • NIST SP 800-53 Rev 4 AC-19 • NIST SP 800-53 Rev 4 AC-20 • NIST SP 800-53 Rev 4 AC-20 (1)	• NIST SP 800-53 Rev 4 AC-17 • NIST SP 800-53 Rev 4 AC-17 (1) • NIST SP 800-53 Rev 4 AC-17 (2) • **NIST SP 800-53 Rev 4 AC-17 (3)** • **NIST SP 800-53 Rev 4 AC-17 (4)** • NIST SP 800-53 Rev 4 AC-19 • **NIST SP 800-53 Rev 4 AC-19 (5)** • NIST SP 800-53 Rev 4 AC-20 • NIST SP 800-53 Rev 4 AC-20 (1) • **NIST SP 800-53 Rev 4 AC-20 (2)**	• NIST SP 800-53 Rev 4 AC-17 (3) • NIST SP 800-53 Rev 4 AC-17 (4) • NIST SP 800-53 Rev 4 AC-19 (5) • NIST SP 800-53 Rev 4 AC-20 (2)

Organization 3 Exception Approach					
Function	Category	Subcategory	Profiles		
			Current	Target	Gaps
PROTECT (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	• Not Applicable - No remote access available for in-scope assets and systems	• Not Applicable - No remote access available for in-scope assets and systems	• None

Step 7: Implement Action Plan

The organization executes the implementation plan and tracks its progress over time, ensuring that gaps are closed and risks are monitored. As noted above, the identified Framework Category and Subcategory outcomes may not cover all of an organization's cybersecurity risks. However, the Target Profile should include all applicable cybersecurity approaches—including tools, standards, and guidelines—that the organization will use to address cybersecurity risk commensurate with the risk to organizational and critical infrastructure objectives, even if those go beyond the outcomes identified in the Framework.

Informing Existing Sector Efforts

This Implementation Guidance was developed to be intrinsically backwards compatible, meaning it can be used to enhance the success of existing sector-specific programs and inform sector-level goals and guidelines. The resources below can also be used to increase knowledge and enhance cybersecurity practices.

- **Critical Infrastructure Cyber Community (C³) Voluntary Program:** The C³ Voluntary Program is a public-private partnership aligning business enterprises as well as SLTT governments to existing resources that will assist their efforts to use the Framework to manage their cyber risks as part of an all-hazards approach to enterprise risk management. Currently, there are many programs and resources available to critical infrastructure sectors and organizations that are looking to improve their cyber risk resilience. These resources are provided by many DHS and government-wide agencies and offices. The C³ Voluntary Program provides the central place to access that information. The C³ Voluntary Program is the coordination point within the Federal government to leverage and enhance existing capabilities and resources to promote use of the Framework. While the Framework is based on existing guidelines and standards, organizations may still need assistance in understanding its purpose and how it may apply to them. The C³ Voluntary Program will provide assistance to organizations of all types interested in using the Framework.
- **Commercial Facilities Sector-Specific Plan:** The *Commercial Facilities Sector-Specific Plan* (SSP) is designed to guide the sector's efforts to improve security and resilience and describes how the Commercial Facilities Sector manages risks and contributes to national critical infrastructure security and resilience, as set forth in Presidential Policy Directive 21 (PPD-21). The SSP reflects the overall strategic direction for the Commercial Facilities Sector and represents the progress made in addressing the sector's evolving risk, operating, and policy environments. As an annex to the *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (NIPP 2013), this SSP tailors the NIPP's strategic guidance to the unique operating conditions and risk landscape of the Commercial Facilities Sector.

Table 9 provides specific information on how Framework use can help sector stakeholders address previously identified Commercial Facilities Sector priorities, as described in the resources above.

TABLE 9.—How the Framework Addresses Commercial Facilities Sector Priorities.

Sector Resource	Sector Strategy	How Framework Use Can Support the Strategy
Commercial Facilities SSP	States that it is a sector priority to conduct cyber and physical risk assessments and develop risk reduction strategies for evolving threats in collaboration with cross-sector, Federal, regional, and local security stakeholders.	The Framework encourages cyber risk assessments and the development of cybersecurity risk management strategies. For example, the Framework's Identify Function includes the categories Risk Assessment and Risk Management Strategy, which includes cybersecurity activities and outcomes for organizations to identify risks by assessing threats, vulnerabilities, likelihoods, and impacts (ID.RA-1, 2, and 5). It also has references for organizations to develop risk management strategies and communicate findings with stakeholders (ID.RA-3 and ID.RM-1).

Sector Resource	Sector Strategy	How Framework Use Can Support the Strategy
Commercial Facilities SSP	Acknowledges that the sector is "positioned to conduct a sector-wide cyber risk assessment" leveraging the critical functions and services identified in the Cyber-Dependent Infrastructure Identification (CDII).	The Framework introduces a seven-step process organizations can use to create or improve their cybersecurity programs. The fourth step of this process, "Conduct a Risk Assessment," determines the likelihood of a cybersecurity event and potential impacts. Additionally, the Framework Core's Identify function is divided into Subcategories that address cyber risk assessments (ID.RA-1, 5, and 6) and cyber infrastructure identification (ID.AM-1-7).
	Acknowledges that "[r]isks associated with cyberattacks continue to grow, as Commercial Facilities Sector reliance on cyber systems, such as for online financial transactions and building management, rises" and identifies cyber risks as one of six major notable trends and emerging issues.	The Framework can help address risk by making stakeholders more aware of increasing cyber risks at a time when more organizations rely on cyber systems to conduct business. Further, it provides stakeholders a menu of tools and approaches to more effectively address risks.
	Sets a goal for Commercial Facilities Sector stakeholders to cost-effectively reduce cyber risks and enhance resilience.	The Framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses. Regarding resilience, the Framework's Recover Function includes Categories and Subcategories dedicated to resilience activities.
	Calls for efforts to improve Commercial Facilities cybersecurity knowledge, tools, capabilities, risk assessments, and practices to secure critical physical and cyber assets linked to cyber systems.	The Framework Core is divided into Categories and Subcategories of cybersecurity outcomes closely tied to programmatic needs and particular activities. Many of these outcomes align to this SSP priority. Indeed, there are Subcategories for ensuring that organizations make sure employees understand their cybersecurity roles/responsibilities and are aware of expected data flows for users and systems (e.g., ID.GV-2, PR.AT-1, and DE.AE-1); carefully assess risks to physical and cyber assets (e.g., ID.RA-1-6); and adopt or improve asset management practices, including routine inventorying of hardware, devices, data, and software (e.g., ID.AM-1 and 2).

Sector Resource	Sector Strategy	How Framework Use Can Support the Strategy
Commercial Facilities SSP	Encourages activities to enhance coordination with interdependent critical infrastructure sectors and community response partners to improve resilience and enhance decision-making.	The Framework's Implementation Tier 3 is defined, in part, as a level of cybersecurity sophistication at which an organization "understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events." The Framework Core includes a Subcategory to ensure that an organization's place in critical infrastructure and its industry sector is identified and communicated (ID.BE-2). Moreover, the Core includes other Subcategories to ensure better coordination with internal and external partners in responding to and recovering from cybersecurity events (e.g., RS.CO-1-5).
	Sets a priority for Commercial Facilities organizations to share security and resilience best practices and case studies to enable owners and operators to leverage lessons learned in all risk mitigation activities.	The Framework incorporates Subcategories that encourage cyber-related information sharing among internal and external stakeholders, including information about emerging threats and vulnerabilities (see ID.RA-2) and about the effectiveness of protection technologies (see PR.IP-8). There are also Subcategories emphasizing a lessons-learned approach for improving response and recovery practices (RS.IM and RC.IM-1). In fact, this approach of continuous learning and adaptation underlies the entire Framework document as a whole. As the Framework's Executive Summary explains: "The Framework is a living document [that] will continue to be updated and improved as industry provides feedback on implementation. As the Framework is put into practice, lessons learned will be integrated into future versions. This will ensure it is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and solutions."
	Promotes the work of the Commercial Facilities Cyber Working Group, which was established to help stakeholders gain insight into private sector cybersecurity needs and practices.	The Framework encourages stakeholders at all levels to collaborate on and coordinate development of cybersecurity standards, guidelines, and practices.

Sector Resource	Sector Strategy	How Framework Use Can Support the Strategy
Commercial Facilities SSP	Encourages Commercial Facilities Sector organizations to continue working with DHS Office of Cybersecurity and Communications (CS&C) to improve cyber risk management efforts at the sector and individual facility level, including efforts to develop a long-term work plan related to cyber risk assessments.	The Framework's Profiles can serve as a good starting point for organizations seeking to develop new or update existing cybersecurity processes and practices, including risk assessment activities. Comparison of Profiles (e.g., the Current Profile and Target Profile) may reveal gaps to be addressed to meet cybersecurity risk management objectives, which could possibly compel an organization to write an action plan and/or roadmap to address these gaps. This risk-based approach enables an organization to gauge resource estimates (e.g., staffing and funding) to achieve cybersecurity goals in a cost-effective, prioritized manner.
	Establishes a number of sector research and development (R&D) priorities, including a priority to improve the ability of Commercial Facilities organizations to detect cyber threats and to identify and better understand potential impacts of a variety of cybersecurity failures.	The Framework's Core Functions, Categories, and Subcategories describe cybersecurity outcomes that address this particular R&D priority, including RS.AN-2 and DE.AE-4. To mitigate impacts, the Framework suggests that organizations consider investments in response/recovery planning and exercises.

Conclusion

This document serves as a foundation for how Commercial Facilities Sector organizations, both nascent and mature, can leverage existing resources to increase their overall cybersecurity awareness using the NIST Cybersecurity Framework. Specifically, the information provided in this document can help an organization assess its current cybersecurity practices, identify tools to help determine gaps, and determine its cybersecurity goals. The C^3 Voluntary Program is a compilation of various resources organized by the five Core Functions of the Framework. For any questions related to this Implementation Guidance and/or the C^3 Voluntary Program, please e-mail CCubedVP@hq.dhs.gov.

Appendix A: Notional Use-Case Study—Commercial Facilities Organization A

Goal Level

Commercial Facilities Organization A seeks to use the Framework with a **strict** interpretation of the Implementation Guidance to improve its cybersecurity and risk management practices. The Framework is partially implemented, as Organization A adheres to range of requirements from Federal and State laws.

Primary Actor, Stakeholders, and Interests

Commercial Facilities Organization A is a regional organization that operates three satellite locations with 300 employees. Stakeholders of the organization include employees, shareholders, and government regulators. Commercial Facilities Organization A is concerned with the resilience of its control systems. The security of the systems and information are essential to maintaining reliable operations. These security programs must have strong board and senior management level support, integration of security activities and controls throughout the organization's business processes, and clear accountability for carrying out security responsibilities.

Current Condition

In order to understand the implementation of the Framework, Commercial Facilities Organization A contacts the Commercial Facilities Sector Coordinating Council and the DHS C^3 Voluntary Program for Framework guidance and assistance to establish connections with public and private sector organizations.

Commercial Facilities Organization A assesses its current cybersecurity profile. The assessment shows that Commercial Facilities Organization A is only loosely aligned to the Framework's functions. As a result, the organization uses its risk management process and adherence to numerous information security-focused regulations to create its target profile that reflects the desired strict interpretation for each selected Framework Category. The Target Profile is based on the selection of the Functions, Categories, and Subcategories that are aligned with the organization's business requirements, risk tolerance, and resources.

Implementation

Commercial Facilities Organization A follows the recommended steps on how an organization can use the Framework to create a new cybersecurity program or improve an existing cybersecurity program.

- **Step 1: Identify**. Critical Manufacturing Organization A identifies its mission objectives, describes cybersecurity risks, and determines which organizational components will use the Framework.
- **Step 2**: **Orient.** Critical Manufacturing Organization A identifies the systems, assets, requirements, and risk management approaches and determines how to evaluate current risk management and cybersecurity posture.
- **Step 3: Create a Current Profile**. Beginning with the Categories specified in the Framework Core, Commercial Facilities Organization A develops a "Current Profile" that reflects its understanding of its present-day cybersecurity activities.
- **Step 4: Conduct a Risk Assessment**. Commercial Facilities Organization A analyzes the operational environment and determines that a cyberattack against its cyber infrastructure is likely over the long term based on the Cyber Information Sharing and Collaboration Program, which it connected with through the C^3 Voluntary Program. Based on its risk assessment, Commercial Facilities Organization A identifies various vulnerabilities and determines the consequence if those vulnerabilities are exploited.

- **Step 5: Create a Target Profile**. Commercial Facilities Organization A creates a Target Profile that focuses on the assessment of the Framework elements (e.g., Categories and Subcategories) describing the organization's desired cybersecurity outcomes.
- **Step 6: Determine, Analyze, and Prioritize Gaps**. Commercial Facilities Organization A compares the Current Profile and Target Profile to determine gaps and the resources necessary to address the gaps. Commercial Facilities Organization A creates a prioritized Action Plan that draws upon mission drivers, cost/benefit analysis, and understanding of risk to achieve Target Profile outcomes. Identifying gaps between the Current Profile and Target Profile allows for the creation of an Action Plan that Commercial Facilities Organization A implements to reduce its cybersecurity risk.
- **Step 7: Implement Action Plan**. The organization implements the steps defined in the Action Plan and monitors its current cybersecurity practices against the Target Profile.

Continuing to Adjust and Adapt

After implementing its plan, Commercial Facilities Organization A performs a self-evaluation against the Framework Implementation Tier 2 level before third-party validation of implementation. This self-evaluation includes determining the organization's defined, institutionalized, risk-informed, and management-approved processes and procedures. Although it is determined that Commercial Facilities Organization A complies with existing cybersecurity regulations, Commercial Facilities Organization A expresses its ultimate goal of being consistently secure throughout all of its processes.

Commercial Facilities Organization A also partners with a third-party to evaluate the organization's management and execution of risk management activities. To move forward in a comprehensive manner, the organization leverages activities in Framework Core Functions mentioned in the Preconditions section.

Commercial Facilities Organization A strives to meet the Tier 3, which includes regular and repeatable risk management processes to respond to a changing cybersecurity landscape. Tier 3 achievement is accomplished by overlaying the Framework and Commercial Facilities Organization A's risk management activities, gap identification, and mitigation. Risk management processes include risk-informed policies, processes, and procedures that are defined, implemented as intended, and validated.

[OPTION 1] The organization identifies areas for improvement based on Current Profile, Target Profile, and industry stakeholder input to focus on improving critical areas of cybersecurity and risk management:

- Authentication
- Data Analytics
- Cybersecurity Workforce
- Privacy Standards
- Supply Chain Risk Management

[OPTION 2] The organization identifies key areas to consider for improvement within the Framework Core Functions, noted in **bold** below:

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy	• Awareness and Training • Data Security • Information Protection Processes and Procedures • ***Protective Technology***	• ***Anomalies and Events*** • ***Security Continuous Monitoring*** • ***Detection Processes***	• ***Response Planning*** • ***Communications*** • Analysis • ***Mitigation*** • ***Improvements***	• ***Recovery Planning*** • ***Improvements*** • ***Communications***

Appendix B: Glossary

Aside from the term "organization," the following glossary is excerpted verbatim from the Cybersecurity Framework.

Term	Definition
Category	The subdivision of a Function into groups of cybersecurity outcomes, closely tied to programmatic needs and particular activities. Examples of Categories include "Asset Management," "Access Control," and "Detection Processes."
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters.
Cybersecurity	The process of protecting information by preventing, detecting, and responding to attacks.
Cybersecurity Event	A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).
Detect (Function)	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
Framework	A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. Also known as the "Cybersecurity Framework."
Framework Core	A set of cybersecurity activities and references that are common across critical infrastructure sectors and are organized around particular outcomes. The Framework Core comprises four types of elements: Functions, Categories, Subcategories, and Informative References.
Framework Implementation Tier	A lens through which to view the characteristics of an organization's approach to risk—how an organization views cybersecurity risk and the processes in place to manage that risk.
Framework Profile	A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories.
Function	One of the main components of the Framework. Functions provide the highest level of structure for organizing basic cybersecurity activities into Categories and Subcategories. The five functions are Identify, Protect, Detect, Respond, and Recover.
Identify (Function)	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
Informative Reference	A specific section of standards, guidelines, and practices common among critical infrastructure sectors that illustrates a method to achieve the outcomes associated with each Subcategory.

Term	Definition
Mobile Code	A program (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics.
Organization	An operational entity of any size that uses the same cybersecurity risk management program within its different components, and may individually use the Framework.
Protect (Function)	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
Privileged User	A user that is authorized (and, therefore, trusted) to perform security relevant functions that ordinary users are not authorized to perform.
Recover (Function)	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.
Respond (Function)	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Risk Management	The process of identifying, assessing, and responding to risk.
Subcategory	The subdivision of a Category into specific outcomes of technical and/or management activities. Examples of Subcategories include “External information systems are catalogued,” “Data-at-rest is protected,” and “Notifications from detection systems are investigated.”

Homeland
Security