From:	Juan Carlos Angarita Castellanos
To:	cyberframework
Subject:	Comments to CSF 2.0 Public Draft
Date:	Thursday, November 9, 2023 10:06:32 PM
Attachments:	Comments to NIST-CSWP-29-ipd.docx

Good night,

I am pleased to contribute my comments on the Public Draft: The NIST Cybersecurity Framework 2.0.

With best regards,

Juan Carlos Angarita C.
[redacted]
CEO – IMS GLOBAL
TX, USA – Colombia – México – Brasil
http://imsglobals.com/

Public Draft: The NIST Cybersecurity Framework 2.0

National Institute of Standards and Technology

Released August 8, 2023

Abstract

The NIST Cybersecurity Framework 2.0 provides guidance to industry, government agencies, and other organizations to manage and reduce cybersecurity risks. It offers a taxonomy of high-level cybersecurity outcomes that can be used by any organization — regardless of its size, sector, complexity, or maturity — to better understand, assess, prioritize, and communicate its cybersecurity efforts. The Framework does not prescribe how outcomes should be achieved. Rather, it maps to resources that provide additional guidance on practices and controls that could be used to achieve those outcomes. This document explains Cybersecurity Framework 2.0 and its components and describes some of the many ways that it can be used.

Keywords

cybersecurity; Cybersecurity Framework; cybersecurity risk governance; cybersecurity risk management; cybersecurity supply chain risk management; enterprise risk management; Privacy Framework; Profiles.

Acknowledgments

This Framework is the result of a collaborative effort across industry, academia, and government in the United States and around the world. NIST acknowledges and thanks all of those who have contributed to this revised Framework. Information on the Framework development process, including workshops and drafts, can be found on the NIST Cybersecurity Framework website.

Lessons learned on the use of the Framework can always be shared with NIST through cyberframework@nist.gov.

Commented [JA1]: It is suggested to include the two words in red to ensure a more comprehensive cybersecurity management

Table of Contents

List of Tables

List of Figures

Executive Summary

Cybersecurity risks are a fundamental type of risk for all organizations to manage. Potential impacts to organizations from cybersecurity risks include higher costs, lower revenue, loss of money, reputational damage, and the impairment of innovation and competitivity. Cybersecurity risks also threaten individuals' privacy and access to essential services and can result in life-or-death consequences.

The NIST Cybersecurity Framework (Framework or CSF) 2.0 provides guidance for managing and reducing cybersecurity risks by helping organizations to understand, assess, prioritize, and communicate about those risks and the actions that will reduce them.

Commented [JA2]: It is suggested to include the two words in red to improve the concept of cybersecurity risk.

Those actions are intended to address cybersecurity outcomes described within the CSF Core. These high-level outcomes can be understood by a broad audience, including executives, government officials, and others who may not be cybersecurity professionals. The outcomes are sector- and technology-neutral, so they provide organizations with the flexibility needed to address their unique risk, technology, and mission considerations. These outcomes can be used to focus on and implement strategic decisions that improve cybersecurity postures (or state) while also considering organizational priorities and available resources.

The CSF Core also includes examples of how each outcome can be achieved along with references to additional guidance. Together these help an organization address its cybersecurity priorities. The CSF also describes the concepts of Profiles and Tiers, which are tools to help organizations put the CSF into practice and set priorities for where they need or want to be in terms of reducing cybersecurity risks.

The CSF is a foundational resource that is adopted voluntarily and through governmental policies and mandates. Its enduring and flexible nature transcends sectors, technologies, and national borders. The updates in CSF 2.0 address changes in technologies and cybersecurity risk.

The CSF should be used in conjunction with other resources (e.g., frameworks, standards, guidelines, and leading practices) to better manage cybersecurity risks and to inform overall management of cybersecurity and other risks at an enterprise level. Supplemental guidance to this Framework will be developed and available on the NIST Cybersecurity Framework website.

1. Introduction

The NIST Cybersecurity Framework (Framework or CSF) describes essential cybersecurity outcomes that can help an organization manage and reduce its cybersecurity risk. The voluntary Framework is not a one-size-fits-all approach to managing cybersecurity risks. Organizations will continue to have unique or specific risks - including different assets, vulnerabilities, threats, and risk tolerances, as well as unique mission objectives and requirements across sectors. Thus, organizations' implementations of the Framework, and approaches to managing risk, will vary.

Commented [JA3]: It is suggested to include the two words in red to ensure the alignment with the introduction (in terms of risk management) and the reference to the assets (information and technology) which are in the sight of cyber-criminals.

This collection of cybersecurity outcomes creates a taxonomy and structure that can be used to understand, assess, prioritize, and communicate about cybersecurity risks.

- **Understand and Assess**:
  - Describe an organization's current or target cybersecurity posture within and across organizations, sectors, or business units.
  - Determine where an organization may have cybersecurity gaps, including with respect to existing or emerging threats or technologies, and assess progress toward addressing those gaps.
  - Align policy, business, and technological approaches to managing cybersecurity risks across an entire organization or in a more focused area, such as a portion of the organization, a specific technology, or technology suppliers.
- **Prioritize:**
  - Prioritize opportunities to improve cybersecurity risk management.
  - Identify, organize, and prioritize actions for reducing cybersecurity risks that align with the organization's mission, legal and regulatory requirements, and risk management and governance expectations.
  - Inform decisions about cybersecurity-related workforce needs and capabilities.
- **Communicate:**
  - Provide a common language for communicating with internal and external parties about cybersecurity risks, capabilities, needs, and expectations.
  - Complement an organization's risk management process by presenting a concise way for executives and others to distill the fundamental concepts of cybersecurity risk so that they express at a high level risks to be managed and how their organization uses cybersecurity standards, guidelines, and practices.

The Framework can be used by organizations whose cybersecurity programs are at different stages of maturity. An organization with an existing cybersecurity program can leverage the Framework to identify opportunities to strengthen and communicate its management of cybersecurity risk while considering its existing practices and needed changes. An organization without an existing cybersecurity program can use the Framework as a starting point and reference to establish one.

While many cybersecurity risk management activities focus on conditions that may prevent mission objectives from being achieved, it is important to also note conditions that may enable or accentuate mission achievement. Actions to reduce cybersecurity risk might benefit the organization in other ways, like increasing revenue (e.g., offering excess facility space to a commercial hosting provider for hosting their own and other organizations' data centers, then moving a major financial system from the organization's in-house data center to the hosting provider to reduce cybersecurity risk).

The Framework should be used in conjunction with other resources to better manage cybersecurity risks. The outcomes are based on and are mapped to existing global standards, guidelines, and practices. Organizations can use the Framework to efficiently scale their cybersecurity programs, address the dynamic and global nature of cybersecurity risks, and adapt to technological advances and business and legal requirements. The Framework applies to all information and communications technology (ICT), including information technology (IT), the Internet of Things (IoT), and operational technology (OT) used by an organization. It also applies to all types of technology environments, including cloud, mobile, and artificial intelligence systems. The Framework is forward-looking and is intended to apply to future changes in technologies and environments.

1.1. Audience

The Framework is designed to be used by organizations of all sizes and sectors, including industry, government, academia, and non-profit organizations. The Framework's taxonomy and referenced standards, guidelines, and practices are not country-specific, and previous versions of the Framework have been successfully leveraged by many governments and other organizations outside of the United States.

The primary audience for the Framework consists of those responsible for developing and leading a cybersecurity program. The Framework can also be used by others involved in managing risk — including executives, boards of directors, acquisition professionals, technology professionals, risk managers, lawyers, human resources specialists, and cybersecurity and risk management auditors — to guide their cybersecurity-related decisions.

Additionally, the Framework can be useful to policymakers (such as associations, professional organizations, and regulators) to set and communicate priorities for cybersecurity risk management.

Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, issued in February 2013, directed NIST "to lead the development of a framework to reduce cyber risks to critical infrastructure." The Cybersecurity Enhancement Act of 2014 directed NIST to "on an ongoing basis, facilitate and support the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure." NIST published Framework Version 1.0 in 2014 and updated the Framework to 1.1 in 2018.

Since then, Congress has explicitly directed NIST to consider small business concerns (in the NIST Small Business Cybersecurity Act) and the needs of institutions of higher education (in the CHIPS and Science Act) in the Framework. While Version 2.0 can be used by any organization, NIST will continue to build additional resources to help implement the Framework, including an updated NIST Special Publication (SP) 1271, *Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide*. All resources will be publicly available on the NIST Cybersecurity Framework website.

1.2. Document Structure

This document contains the following sections and appendices:

- Section 2 explains the basics of the Framework Core: Functions, Categories, Subcategories, Implementation Examples, and Informative References.
- Section 3 provides an overview of common uses for the Framework, including through Current and Target Profiles, as well as guidance on using the Framework to understand, assess, prioritize, and communicate cybersecurity efforts and cybersecurity supply chain risk management efforts.
- Section 4 discusses using the Framework to help integrate cybersecurity risk management with other types of risk management.
- Section 5 briefly outlines next steps for readers who want to use the Framework.
- Appendix A offers notional templates for Framework Profiles and action plans.
- Appendix B describes the Framework Tiers.
- Appendix C provides the Framework Core.

2. Understanding the Framework Core

The Framework Core provides a set of cybersecurity *outcomes* (arranged by Function, Category, and Subcategory), examples of how those outcomes might be achieved (Implementation Examples), and references to additional guidance on how to achieve those outcomes (Informative References), as depicted in Fig. 1. The cybersecurity outcome statements in the Core reflect activities across sectors and are technology-neutral. They are not a checklist of actions to perform; the specific actions taken to achieve a cybersecurity outcome will vary by organization and use case, as will the individual responsible for those actions. Additionally, the order of Functions, Categories, and Subcategories in the Core is not intended to imply the

sequence by which they should be implemented or their relative importance. The ordering of the Core is intended to resonate most with those charged with operationalizing risk management within an organization.

This section explains the basics of the Framework Core. See Appendix C for the Framework Core's descriptions of the Functions, Categories, and Subcategories.

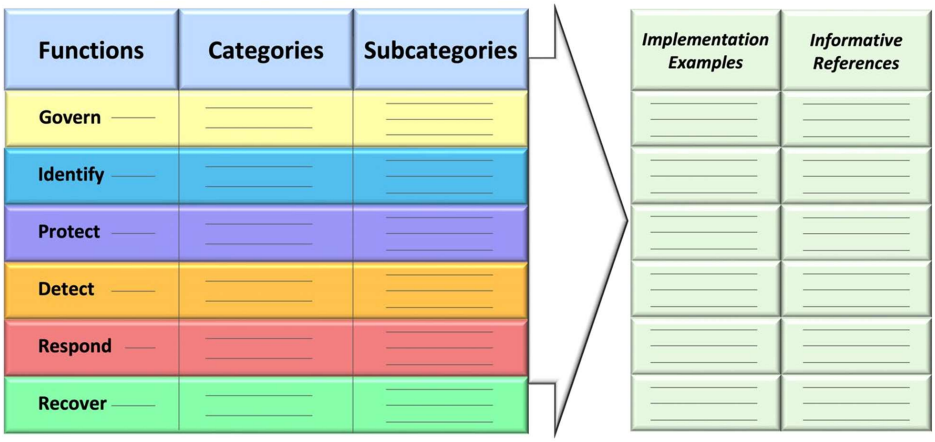

Fig. 1. Cybersecurity Framework Core

2.1. Functions, Categories, and Subcategories

The Framework Core **Functions** — GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, and RECOVER — organize cybersecurity outcomes at their highest level.

- ***GOVERN (GV)*** *– Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy.* The GOVERN Function is cross-cutting and provides outcomes to inform how an organization will achieve and prioritize the outcomes of the other five Functions in the context of its mission, the applicable requirements, and stakeholder expectations. Governance activities are critical for incorporating cybersecurity into an organization's broader enterprise risk management strategy. GOVERN directs an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policies, processes, and procedures; and the oversight of cybersecurity strategy.

- ***IDENTIFY (ID)*** *– Help determine the current cybersecurity risk to the organization.* Understanding its assets (e.g., data, hardware, software, systems, facilities, services, people) and the related cybersecurity risks enables an organization to focus and prioritize its efforts in a manner consistent with its risk management strategy and the mission needs identified under GOVERN. This Function also includes the identification of improvements needed for the organization's policies, processes, procedures, and practices supporting cybersecurity risk management to inform efforts under all six Functions.

Commented [JA4]: Governance must include the perspective of compliance (as a part of the context).

- ***PROTECT (PR)*** – *Use safeguards to prevent or reduce cybersecurity risk.* Once assets and risks are identified and prioritized, PROTECT supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events. Outcomes covered by this Function include awareness and training; data security; identity management, authentication, and access control; platform security (i.e., securing the hardware, software, and services of physical and virtual platforms); and the resilience of technology infrastructure.
- ***DETECT (DE)*** – *Find and analyze possible cybersecurity attacks and compromises.* DETECT enables timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse cybersecurity events that may indicate that cybersecurity attacks and incidents are occurring.
- ***RESPOND (RS)*** – *Take action regarding a detected cybersecurity incident.* RESPOND supports the ability to contain the impact of cybersecurity incidents. Outcomes within this Function cover incident management, analysis, mitigation, reporting, and communication.
- ***RECOVER (RC)*** – *Restore assets and operations that were impacted by a cybersecurity incident.* RECOVER supports timely restoration of normal operations to reduce the impact of cybersecurity incidents and enable appropriate communication during recovery efforts.

Fig. 2 shows the CSF Functions as a wheel because all Framework Functions relate to one another. For example, an organization will categorize assets under IDENTIFY and take steps to secure those assets under PROTECT. Investments in planning and testing in the GOVERN and IDENTIFY Functions will support timely incident response and recovery actions for cybersecurity incidents in the RESPOND and RECOVER Functions. GOVERN is in the center of the wheel because it informs how an organization will implement the other five Functions.

Fig. 2. Framework Functions

To form and maintain a culture that addresses dynamic cybersecurity risk, the Functions should be addressed concurrently. Actions supporting GOVERN, IDENTIFY, PROTECT, and DETECT should

all happen continuously, and actions supporting RESPOND and RECOVER should be ready at all times and happen when cybersecurity incidents occur. All Functions have vital roles related to incidents; GOVERN, IDENTIFY, and PROTECT outcomes help prevent and prepare for cybersecurity incidents, while GOVERN, DETECT, RESPOND, and RECOVER outcomes help discover and manage cybersecurity incidents.

Categories are the subdivisions of a Function into groups of related cybersecurity outcomes.

Subcategories further divide a Category into specific outcomes of technical and management activities. They are not exhaustive, but they help to achieve the outcomes in each Category.

2.2. Implementation Examples and Informative References

The Framework Core also provides two types of additional resources with information to help achieve the outcomes described in the Core's Functions, Categories, and Subcategories.

- **Informative References** are standards, guidelines, regulations, and other resources to help inform how an organization achieves the Functions, Categories, and Subcategories. In some cases, the Informative Reference is more specific than a Subcategory, such as a control from SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*. In that case, more than one control would be used to achieve the outcome described in one Subcategory. In other cases, organizations may leverage higher-level policies or requirements that address one or more Subcategories. Informative References can also be sector- or technology-specific. In using the Framework, each organization will identify applicable Informative References.
- **Implementation Examples** provide notional examples of concise, action-oriented steps to help achieve the outcomes of the Subcategories in addition to the guidance provided by Informative References. The examples are not a comprehensive list of all actions that could be taken by an organization to achieve an outcome, nor do they represent a baseline of required actions to address cybersecurity risk.

While Informative References and Implementation Examples are considered part of the Core, they will be maintained separately in an online format on the NIST Cybersecurity Framework website (leveraging the NIST Cybersecurity and Privacy Reference Tool [CPRT]) to allow for more frequent updates. Informative References may be submitted at any time through the NIST National Online Informative References (OLIR) program.

The Framework Core can be used to identify opportunities for new or revised standards, guidelines, or practices where additional Informative References would help organizations address emerging needs. An organization implementing a given Subcategory might discover that there are few Informative References, if any, for a specific activity. In that case, the organization might collaborate with technology leaders and standards bodies to draft, develop, and coordinate standards, guidelines, or practices. Similarly, an organization might determine that additional Implementation Examples would help others better understand an emerging need. NIST encourages submissions of new Examples for consideration at any time. Suggestions may be sent to cyberframework@nist.gov.

3. Using the Framework

The Framework can be used in numerous ways. Its use will vary based on an organization's unique mission, assets, risks and the applicable requirements. With an understanding of stakeholder expectations and risk appetite and tolerance (as outlined in GOVERN), organizations can prioritize cybersecurity activities, enabling them to make informed decisions about cybersecurity expenditures and actions. Organizations may choose to handle risk in different ways — including mitigating, transferring, avoiding, or accepting the risks — depending on the potential impacts. Importantly, organizations can use the Framework both internally and to oversee third parties.

Commented [JA5]: Assets and requirements are key factors in how any framework or standard is applied to manage cybersecurity.

> The Cybersecurity Framework provides a flexible and risk-based implementation that can be used with a broad array of cybersecurity risk management processes, such as International Organization for Standardization (ISO) 31000:2018; ISO/International Electrotechnical Commission (IEC) 27005:2022; SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy;* and the *Electricity Subsector Cybersecurity Risk Management Process* (RMP) guideline.

This section explains several ways that organizations can use the Framework:

- Create and use Framework Profiles to understand, assess, and communicate the organization's current or target cybersecurity posture in terms of the Framework Core's cybersecurity outcomes, and prioritize outcomes for achieving the target cybersecurity posture. (Section 3.1)
- Assess the organization's achievement of cybersecurity outcomes. (Section 3.2)
- Characterize cybersecurity risk management outcomes with Framework Tiers. (Section 3.3)
- Improve cybersecurity communication with internal and external stakeholders. (Section 3.4)
- Manage cybersecurity risk throughout supply chains. (Section 3.5)

Regardless of the application of the Framework, organizations likely will find it helpful to think of the Framework as guidance to help them to understand, assess, prioritize, and communicate about those cybersecurity risks and the actions that will reduce those risks. The outcomes which are selected can be used to focus on and implement strategic decisions to improve an organization's cybersecurity posture (or state), taking into account its priorities and available resources.

3.1. Creating and Using Framework Profiles to Understand, Assess, Prioritize, and Communicate

The Framework's mechanism for describing an organization's current or target cybersecurity posture in terms of the Core's outcomes is called a *Framework Profile* (Profile).

Profiles are used to understand, assess, prioritize, and tailor the sector- and technology-neutral Core outcomes (i.e., Functions, Categories, and Subcategories) based on an organization's mission objectives, stakeholder expectations, threat environment, and requirements and leading practices, including those for specific sectors or technologies, as Fig. 3 illustrates. Organizations then can prioritize their actions to achieve specific outcomes and communicate that information to internal and external stakeholders. Appendix A provides a notional Profile template.

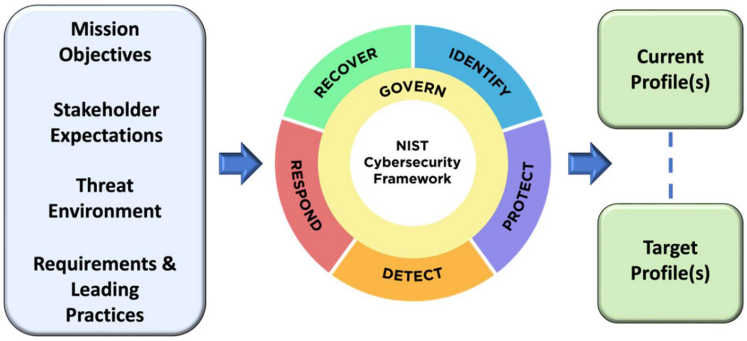

Fig. 3. Cybersecurity Framework Profiles

There are two types of Profiles:

- A *Current Profile* covers the Core's outcomes that an organization is currently achieving (or attempting to achieve) and characterizes how or to what extent each outcome is being achieved.
- A *Target Profile* covers the desired outcomes that an organization has selected and prioritized from the Core for achieving its cybersecurity risk management objectives. A Target Profile takes into account anticipated changes to the organization's cybersecurity posture, such as new requirements, new technology adoption, and cybersecurity threat intelligence trends.

Some organizations prefer to create a Current Profile first — for example, an organization that wants to review its current efforts first and then think about areas for improvement. Others prefer to start with a Target Profile to work toward. For example, an organization that needs to meet a set of new requirements might focus on developing its Target Profile first and in the course of doing so, also determine its current cybersecurity posture for its Current Profile.

A *Community Profile* is a Target Profile created to address shared interests and goals among a group of organizations. Organizations can consider using it as the basis for their own Target Profile. An example of a Community Profile is one developed for a sector or subsector, or for a specific use case or technology. A Community Profile could be developed by organizations collaboratively, or it could be developed by one organization for others to use. Examples of CSF 1.1 Community Profiles can be found on the NIST Cybersecurity Framework website, which NIST will update as new Community Profiles are developed for CSF 2.0.

3.1.1. Ways to Use Profiles

Organizations can create and use Profiles to utilize the full capabilities of the Framework (as discussed in Section 1). While organizations can use the Framework without Profiles, they provide the opportunity to develop a prioritized roadmap to achieve the cybersecurity outcomes of the Framework. There are many ways to use Profiles, including to:

- Compare current cybersecurity practices to sector-specific standards and regulatory requirements
- Document the Informative References (e.g., standards, guidelines, and policies) and the practices (e.g., procedures and safeguards) currently in place and planned in the future
- Set cybersecurity goals for the organization, identify gaps between current practices and the goals, and plan how to address the gaps in a cost-effective manner
- Prioritize cybersecurity outcomes
- Assess progress toward achieving the organization's cybersecurity goals
- Determine where the organization may have cybersecurity gaps with respect to an emerging threat or a new technology
- Communicate about the cybersecurity capabilities an organization provides — for example, to business partners or to prospective customers of the organization's technology products and services
- Express the organization's cybersecurity requirements and expectations to suppliers, partners, and other third parties
- Integrate cybersecurity and privacy risk management programs by analyzing gaps between NIST Cybersecurity and Privacy Framework Profiles

3.1.2. Steps for Creating and Using Profiles

The steps described below and summarized in Fig. 4 illustrate one way an organization could use Current and Target Profiles to help inform continuous improvement of its cybersecurity:

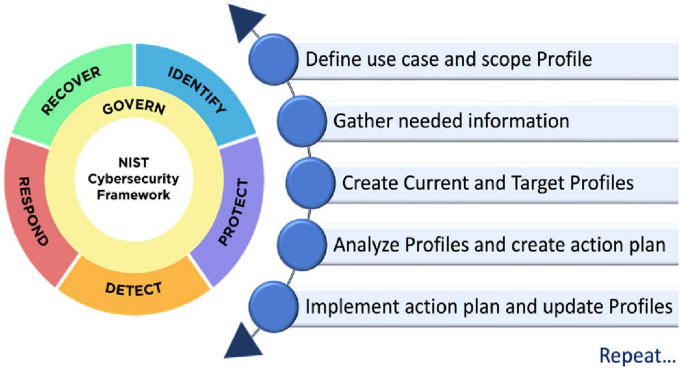

Fig. 4. Steps for creating and using Cybersecurity Framework Profiles

1. **Define the use case for the Profiles.** The use case defines the high-level facts and assumptions on which the Profiles will be based, as a way of scoping the Profiles. This can include:
   - The reason for creating the Profiles
   - The organization's divisions, information and technology assets, services, and other elements that are in scope for these Profiles
   - Those who will develop, review, and operationalize the Profiles
   - The individuals who set expectations for actions to achieve cybersecurity outcomes
2. **Gather the information needed to prepare the Profiles.** An organization can gather relevant resources prior to preparing the Profiles, such as (i) organizational policies, (ii) risk management priorities and resources, (iii) information, technology, infrastructure, and cybersecurity requirements and standards followed by the organization, and work roles. Understanding cybersecurity governance — such as identifying the organization's mission, its stakeholders, and their needs and expectations, as outlined in the GOVERN Function — is generally needed for preparing a Target Profile.
3. **Create Current and Target Profiles.** Determine what types of supporting information (also known as *elements*) each Profile should include for each of the selected Framework outcomes, and fill in the elements for each selected outcome. Consider the risk implications of the current state to inform target state planning and prioritization. Appendix A provides a notional template for Current and Target Profiles and examples of common elements that organizations can choose to use. Examples of elements in a Profile for each outcome Category or Subcategory include the outcome's priority compared to other outcomes; current status in achieving the outcome; policies, processes, and procedures; practices, including tools and responsibilities; metrics and measurements; informative references; and any other supporting information that an organization considers helpful. Organizations documenting responsibilities may employ the Workforce Framework for Cybersecurity (NICE Framework), which provides a common lexicon for describing cybersecurity work.
4. **Analyze the Profiles and create an action plan.** Identifying and analyzing the differences between the Current and Target Profiles enables an organization to identify gaps and develop a prioritized action plan for addressing those gaps to improve cybersecurity. This plan should consider mission drivers, benefits, risks, and necessary resources (e.g., staffing, funding). Using Profiles in this manner helps an organization make better-informed decisions about how to improve cybersecurity risk management in a cost-effective manner. Appendix A provides a notional action plan template.
5. **Implement the action plan and update the Profiles.** The organization follows the action plan to adjust its cybersecurity practices to address gaps and move toward the Target Profile. Improving an organization's cybersecurity program is a continuous effort, and implementing an action plan can take months or years. At frequencies defined by the organization, the Current Profile should be updated to assess progress and the Target Profile should be updated to reflect changes in the organization and its cybersecurity risk.

Commented [JCAC6]: A common mistake is only observe direct cybersecurity requirements; however, there are an important set of requirements related to the secure and sage management of information, technology and infrastructure that should be observed for a comprehensive cybersecurity solution.

Over time, changes in either or both Profiles will require revising the action plan and repeating these steps. Given the importance of continual improvement, an organization can repeat the steps as often as needed.

Profile development can be improved through communication across an organization, including but not limited to key stakeholders from executive leadership, risk management, security, legal, human resources, acquisition, and operations. For example, Profile developers can reach out to leaders within the organization to confirm which resources (e.g., facilities, personnel, systems) are most relevant to achieving the objectives (e.g., for a business unit). Those leaders can then share their risk-related expectations for the selected resources with the implementers. By using Current and Target Profiles, cybersecurity planning and monitoring are tightly tied to organizational objectives, and mission-level planners can understand the residual risk of uncertainty in terms of likelihood and impact to the mission.

An organization may choose to develop multiple Profiles that each address a different use case and scope. This can enable better prioritization of activities and outcomes where there may be differing degrees of cybersecurity risk while still allowing an organization to use the overarching Framework structure for consistency across use cases. Examples include describing a cybersecurity outcome posture for:

- An entire enterprise
- Each of an organization's major business units
- Business partners or suppliers
- Each of an organization's most critical systems
- Processes, Technologies, Products or services with cybersecurity requirements

Commented [JCAC7]: A complete posture should include processes and technologies

3.2. Assessing and Prioritizing Cybersecurity Outcomes With the Framework

Step 3, "Create Current and Target Profiles" in Section 3.1 mentions that creating Profiles means filling in the elements for each selected Core outcome. Each organization needs to determine the values to enter into its own Profiles. The Framework does not prescribe specific standards, guidelines, or practices to meet the outcomes. Rather, it gives organizations the flexibility to assess their own cybersecurity outcomes in different ways and does not prescribe a single approach.

For organizations that already assess their cybersecurity risk management practices on a regular basis, the results from recent self-assessments or third-party assessments may provide much of the data needed to create Current Profiles, which capture the as-implemented state of Framework outcomes. Organizations that use the Framework are encouraged to begin with their existing cybersecurity risk assessments and risk management processes.

An organization may choose to conduct an assessment and document the results by comparing the Current and Target Profiles. Assessment results can help to determine if practices are in place and identify and prioritize opportunities for improvement in Profiles.

Organizations can identify metrics to help prioritize and demonstrate progress from Current to Target Profiles. Organizations are encouraged to innovate and customize how they incorporate measurement into their application of the Framework. See the NIST Cybersecurity Measurement

project page for more information, including a pointer to the latest version of SP 800-55, *Performance Measurement Guide for Information Security*.

The Framework offers an opportunity to explore or adjust methodologies for measurement and assessment.[1] For example, key stakeholders could discuss what to include in the organization's Current and Target Profiles, such as selected Informative References, roles and responsibilities, tools, and policies, processes, procedures, and practices. The stakeholders could also discuss what assessment and measurement approaches can be used for those topics, and how the approaches can provide information to support decisions about the organization's cybersecurity posture.

3.3. Using Framework Tiers to Characterize Cybersecurity Risk Management Outcomes

The selection of Framework Tiers (Tiers) helps set the overall tone for how cybersecurity risks will be managed within the organization, and determine the effort required to reach a selected Tier. Organizations can choose to use the Tiers found in Appendix B to inform their Current and Target Profiles. Tiers characterize the rigor of an organization's cybersecurity risk governance and management outcomes, and they provide context on how an organization views cybersecurity risks and the processes in place to manage those risks.

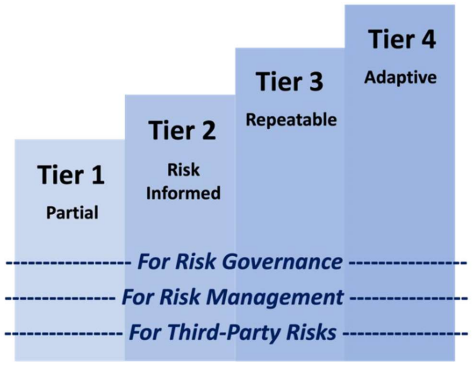

Fig. 5. Cybersecurity Framework Tiers

The Tiers capture an organization's outcomes over a range, from Partial (Tier 1) to Adaptive (Tier 4), as Fig. 5 depicts. They reflect a progression from informal, ad hoc responses to approaches that are agile, risk-informed, and continuously improving.

Tiers should be used to complement an organization's cybersecurity risk management methodology rather than take its place. For example, an organization can use the Tiers to communicate internally as a benchmark for a more organization-wide approach to managing

[1] Many cybersecurity risk assessment or analysis methodologies are available, such as the example detailed in NIST SP 800-30 Rev.1, *Guide for Conducting Risk Assessments*; the Open Group's Open Factor Analysis of Information Risk (OpenFAIR) standard; and others described in International Electrotechnical Commission (IEC) 31010, Risk management – Risk assessment techniques.

cybersecurity risks as necessary to progress to a higher Tier. Not all organizations need to be at a particular Tier (e.g., Tier 3 or 4). Progression to higher Tiers is encouraged when risks or mandates are greater or when a cost-benefit analysis indicates a feasible and cost-effective reduction of cybersecurity risks.

As Framework Profiles are created or updated, the Tier descriptions (as listed in Appendix B) can be considered for guidance. An organization may want to include Tier values (1 through 4) in its Current and Target Profiles. For example, if leadership has determined that the organization should be at Tier 3 (Repeatable), then the Current Profile will reflect how well the Tier 3 governance and management characteristics have been achieved. The Target Profile will reflect any additional outcomes needed to fully achieve the Tier 3 description. Selecting Tiers overall or at the Function or Category level instead of the Subcategory level will provide a better sense of the organization's current cybersecurity risk management practices. Alternatively, an organization can apply the Tiers exclusively to the GOVERN Function to describe the rigor of the organization's risk management as demonstrated by the risk management strategy, expectations, and policy since GOVERN is cross-cutting.

When selecting Tiers, the organization should consider its current risk management practices, threat environment, legal and regulatory requirements, information sharing practices, business and mission objectives, supply chain requirements, and organizational constraints, including assets and resources. The organization should ensure that the selection and use of Tiers help to meet organizational goals, are feasible to implement, and reduce cybersecurity risks to critical assets and resources to levels that are acceptable to the organization.

Commented [JCAC8]: Text in red should be included to ensure the complete understanding of cybersecurity risks.

3.4. Improving Communication With Internal and External Stakeholders Using the Framework

One of the most common benefits of using the Framework is improving communication regarding cybersecurity risks and posture with those inside and outside of an organization. This section explains how to use the Framework to facilitate communication and discusses many of the entities that may benefit.

3.4.1. Improving Communication Across the Organization

The Framework provides a basis for improved communication regarding cybersecurity expectations, planning, and resources among executives, business process managers, and implementation and operations practitioners across an organization. The Framework is best used to foster bi-directional information flows (as shown in Fig. 6) between those who understand the mission objectives and those who understand the specific cybersecurity risks that could hamper the achievement of those objectives. This includes top-down dialogue (fostering understanding of priorities and strategic direction based on stakeholder needs and expectations) and bottom-up reporting (informing decisions about and reporting on results of actions taken to implement the Framework).

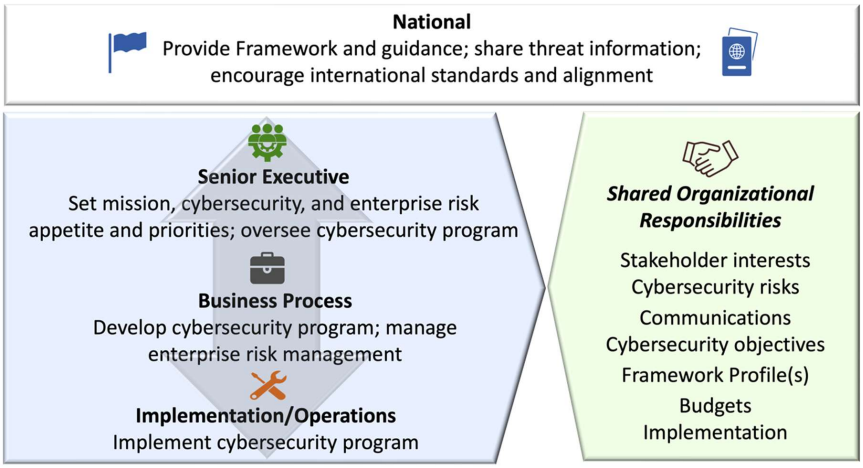

Fig. 6. Using the Cybersecurity Framework to improve communication

When implementing the Framework, the **senior executive** level will focus on organizational risk, with actions to express mission priorities under the GOVERN Function and approve Framework Tier selection. Discussions at this level involve strategy, particularly how cybersecurity-related uncertainties might affect achieving the enterprise's mission and objectives. From a cybersecurity perspective, this entails understanding the needs of internal stakeholders (e.g., shareholders, employees, business managers) and external stakeholders (e.g., customers, regulators, citizens). As executives establish cybersecurity priorities and objectives based on those needs, they develop a risk strategy that considers risk appetite and addresses expectations, accountability, and resources.

The overall cybersecurity objectives set at the senior executive level are informed by and cascade to specific **business process** level objectives. In a commercial entity, these may apply to a line-of-business, a facility, or operating division. For government entities these may be division- or branch-level considerations. When implementing the Framework, business process managers will focus on cybersecurity risk management, with actions to develop Framework Profiles and nominate Framework Tiers. As risk priorities and appetite are translated into mission-level objectives, business process managers can express their own cybersecurity expectations and performance criteria in terms of how uncertainty created by risk may impact the business.

Commented [JCAC9]: Different facilities have diverse assets, processes, risks, and they can be managed specifically.

At the **implementation or operations** level, the focus in implementing the Framework includes securing systems with the action to implement the Framework Profiles. Practitioners both inform and fulfill expectations from the other levels and provide valuable information for planning, carrying out, and monitoring specific cybersecurity activities. Understanding organizational-level priorities, strategies, and processes enables system-specific implementation. As controls are implemented to manage risk to an acceptable level, implementation- and operations-level practitioners provide business process managers and senior executives with the information they need to understand the organization's cybersecurity posture, make informed decisions, and maintain or adjust the risk strategy accordingly.

The Framework encourages and supports discussions about how well the organization's cybersecurity activities address various risks to mission objectives. Section 4.2 describes how organizations can combine cybersecurity risk data with information about other risks to help support better mission alignment across the organization.

At all levels, Framework Profiles are used to support effective enterprise decision-making. The Framework enables those who make strategic decisions to convey expectations and those at the business process and implementation/operations levels to share information with leaders.

3.4.2. Improving Communication With External Stakeholders

The Framework helps facilitate communications about cybersecurity with external parties, including throughout an organization's supply chain. An organization can use the Framework to:

- Express its cybersecurity risk management requirements to an external service provider (e.g., a service provider with which it is exchanging data) through a Target Profile
- Report on the status of cybersecurity requirements (e.g., to a government regulator), which makes it easier to review requirements as part of a broader risk management strategy
- Better understand its cybersecurity posture in light of systemic risks
- Identify cybersecurity priorities for a sector
- Determine the extent to which risk management processes, integration, and information sharing fulfill stakeholders' expectations
- Share high-level information on cybersecurity practices with prospective customers, business partners, and others who may need to understand the organization's cybersecurity posture before engaging with the organization, as well as information related to security incidents.
- Define shared responsibility models with cloud service providers.
- Guide conformity evaluators/auditors, ensuring homogeneity in the interpretation of results

Commented [JCAC10]: When an information security and cybersecurity event or incident happens, the report, collaboration and integration with authorities, law enforcement, information holders, among others, must be included as a component of communication in cases of emergency

Commented [JCAC11]: The evaluation component should be part of the communication process to support the continuous improvement.

3.5. Managing Cybersecurity Risk in Supply Chains With the Framework

The Framework can be used to foster an organization's oversight and communications related to cybersecurity risks with stakeholders across supply chains. All types of technology rely on a complex, globally distributed, extensive, and interconnected supply chain ecosystem with geographically diverse routes and multiple levels of outsourcing. This ecosystem is composed of public- and private-sector entities (e.g., acquirers, suppliers, developers, system integrators, external system service providers, and other technology-related service providers) that interact to research, develop, design, manufacture, acquire, deliver, integrate, operate, maintain, dispose of, and otherwise utilize or manage technology products and services. These interactions are shaped and influenced by technologies, laws, policies, procedures, and practices.

Given the complex and interconnected relationships in this ecosystem, supply chain risk management (SCRM) is critical for organizations. Cybersecurity SCRM (C-SCRM) is a systematic process for managing exposure to cybersecurity risk throughout supply chains and developing appropriate response strategies, policies, processes, and procedures. See SP 800161r1

(Revision 1), *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, for in-depth information on C-SCRM.

Today, nearly all organizations depend on supply chains. As such, it is increasingly important that they develop capabilities and implement practices to identify, assess, and respond to cybersecurity risks throughout the supply chain. The primary objective of C-SCRM is to extend appropriate first-party cybersecurity risk management considerations to third parties, supply chains, and products and services an organization acquires, based on supplier criticality and risk assessment. Examples of risks include products and services that may potentially contain or become a vector for malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the supply chain. Effective C-SCRM requires stakeholders to actively collaborate, communicate, and take actions to secure favorable C-SCRM outcomes. It also requires an enterprise-wide cultural shift to a state of heightened awareness and preparedness regarding the potential ramifications of cybersecurity risks throughout the supply chain.

The Framework Core addresses cybersecurity supply chain risk management in two ways. Within the GOVERN function, the Supply Chain Risk Management (GV.SC) Category and its Subcategories provide outcomes for establishing, managing, monitoring, and improving an organizational cybersecurity supply chain risk management capability or program. The GV.SC Category and Subcategories are specific to C-SCRM and address outcomes such as establishing a cybersecurity supply chain risk management program [GV.SC-01], roles and responsibilities [GV.SC-02], and risk management processes [GV.SC-03] in a manner that is integrated with other related capabilities.

The Categories and Subcategories within the other Functions — IDENTIFY, PROTECT, DETECT, RESPOND, and RECOVER — provide a source for the organization to consider as a basis for supplier cybersecurity requirements, both for direct suppliers and as flow-down requirements for lower-tier suppliers [GV.SC-05]. Which Categories or Subcategories are selected for inclusion in contractual requirements depends on the supplier criticality [GV.SC-04] and supplier risk assessments [GV.SC-07]. Overall, cybersecurity risk in supply chains should be taken into consideration as an organization performs all the Framework Functions. The following provide a few examples across the Functions:

- **Identify**: Identifying, validating, and recording vulnerabilities associated with the supplier's product or service [ID.RA-01]
- **Protect:** Authenticating users, services, and hardware [PR.AA-03]; applying appropriate configuration management practices [PR.PS-01]; generating log records and having the logs available for continuous monitoring [PR.PS-04]; and integrating secure software development practices into the supplier's software development life cycles [PR.PS-07]
- **Detect**: Monitoring computing hardware and software for potentially adverse events [DE.CM-09]
- **Respond**: Executing incident response plans when compromised products or services are involved [RS.MA-01]

- **Recover**: Executing the recovery portion of the organization's incident response plan when compromised products or services are involved [RC.RP-01], and restoring compromised products or services and verifying their integrity [RC.RP-05]

Secure software development is an area that heavily overlaps with supply chain considerations. C-SCRM includes software and software-based services that an organization acquires from third parties, including open-source software, as well as software that an organization creates or integrates for its customers to use. Organizations that acquire or develop software may follow secure software development practices, such as those described in SP 800-218, *Secure Software Development Framework (SSDF)*. Organizations that develop software solely for their own use may benefit from adopting other C-SCRM practices, in effect treating their software development units as part of their supply chain.

An organization can use Framework Profiles to delineate cybersecurity standards and practices to incorporate into contracts with suppliers and provide a common language to communicate those requirements to suppliers. Profiles can also be used by suppliers to express their cybersecurity posture and related standards and practices.

Target Profiles can be used to inform decisions about buying products and services based on requirements to address gaps. This often entails some degree of trade-off with other requirements, comparing multiple products or services and considering other needs such as cost, functionality, and supplier and supply chain risks. Once a product or service is purchased, the Profile can be used to track and address residual cybersecurity risk. For example, if the service or product does not meet all of the cybersecurity objectives described in the Target Profile, the residual risk can be addressed through other actions. The Profile also provides the organization with a method for assessing whether the product meets cybersecurity outcomes through periodic review and testing. A Profile can sharpen the organization's focus on desired cybersecurity outcomes throughout the supply chain.

4. Integrating Cybersecurity Risk Management With Other Risk Management Domains Using the Framework

In addition to cybersecurity risks, every organization faces numerous other types of risk and may use frameworks and management tools that are specific to them. Sometimes two types of risk have commonalities, as Fig. 7 depicts through overlapping cybersecurity and privacy risks. Cybersecurity and privacy risk management have some of the same objectives, so integrating their approaches helps ensure that all risks are considered and that efforts are not duplicated. Section 4.1 discusses an example of integrating risk management approaches — using the Cybersecurity Framework and the Privacy Framework together.

Some organizations integrate all of their risk management efforts at a high level by using enterprise risk management (ERM). Section 4.2 discusses using the Cybersecurity Framework as part of ERM. (See NIST IR 8286, *Integrating Cybersecurity and Enterprise Risk Management*.) The outer border of Fig. 7 indicates an organization's full range of ERM risks, with examples of risks including financial, legal, operational, physical security, reputational, and safety — in addition to cybersecurity and privacy risks.

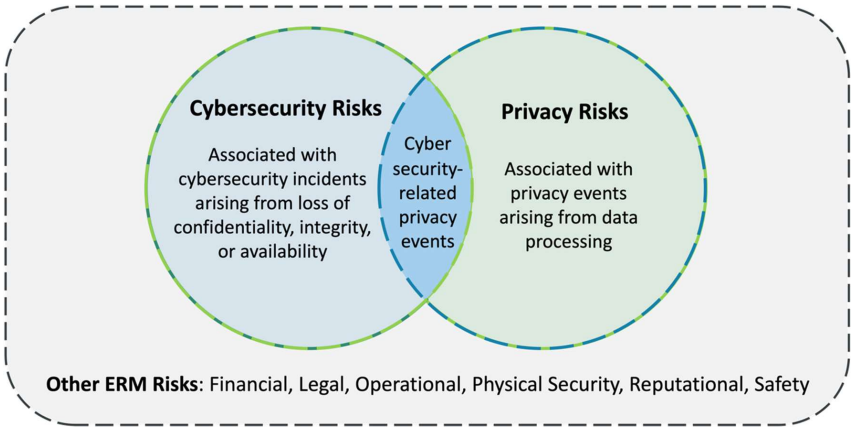

Fig. 7. Integrating cybersecurity and privacy risks

4.1. Integrating the Cybersecurity Framework With the Privacy Framework

Cybersecurity and privacy are independent disciplines, but in certain circumstances their objectives overlap, as illustrated by Fig. 7. Cybersecurity risk management is essential for addressing privacy risks related to the loss of confidentiality, integrity, and availability of individuals' data. For example, data breaches could lead to identity theft. However, privacy risks can also be unrelated to cybersecurity incidents.

Organizations process data to achieve mission or business purposes, which can give rise to *privacy events* whereby individuals may experience problems as a result of the data processing. NIST describes these problems as ranging from dignity-type effects, such as embarrassment or stigma, to more tangible harms, such as discrimination, economic loss, or physical harm.[2] Consequently, when organizations are processing data to conduct cybersecurity activities, they can create privacy risks. For example, some types of incident detection or monitoring activities — particularly those conducted in a manner disproportionate to the intended purpose — may lead individuals to feel surveilled. Additionally, cybersecurity activities can result in the overcollection or over-retention of personal information or the disclosure or use of personal information unrelated to cybersecurity activities. These activities can lead to problems such as embarrassment, discrimination, loss of trust, and the damage to fundamental rights of the owners.

Commented [JCAC12]: In terms of privacy, the guarantee of fundamental rights of the owners (as a requirement) is an aspect that can be affected in cybersecurity incidents.

The NIST Cybersecurity Framework and the NIST Privacy Framework can be used together to collectively address cybersecurity and privacy risks, as illustrated by Fig. 8. As the right side of the Venn diagram depicts, organizations using the Cybersecurity Framework to manage cybersecurity risks can leverage the Privacy Framework Identify-P, Govern-P, Control-P, and Communicate-P Functions to identify and manage privacy risks unrelated to cybersecurity incidents, such as those described above. The Cybersecurity Framework DETECT, RESPOND, and

[2] NIST has created an illustrative catalog of problems for use in privacy risk assessment. See *NIST Privacy Risk Assessment Methodology*. Other organizations may have created other categories of problems, or may refer to them as adverse consequences or harms.

RECOVER Functions and the Privacy Framework Protect-P Function can be collectively leveraged to support the management of overlapping cybersecurity and privacy risks.

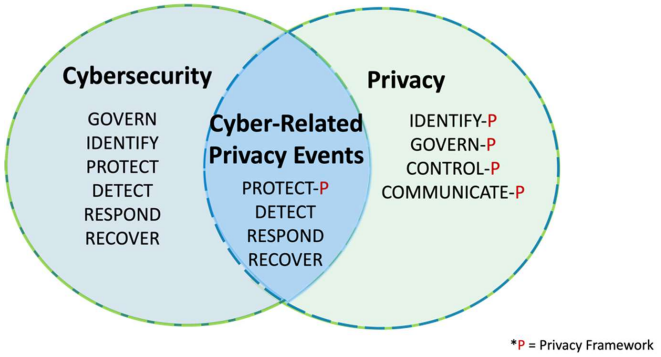

Fig. 8. Cybersecurity Framework and Privacy Framework alignment

When reviewing cybersecurity programs for privacy risks, an organization can consider taking actions such as the following:

- Use both the Cybersecurity and Privacy Frameworks to consider the full spectrum of privacy risks associated with its cybersecurity program, including identity management and access control
- Ensure that individuals with cybersecurity-related privacy responsibilities report to appropriate management and are appropriately trained
- Comply with applicable privacy statutes and regulations
- Identify outcomes and activities in the Privacy Framework Core that can be integrated into cybersecurity workforce awareness and training
- Inform providers of cybersecurity-related products and services about the organization's applicable privacy policies
- Conduct privacy reviews of an organization's asset monitoring and detection of adverse cybersecurity events and incidents, as well as its cybersecurity incident mitigation efforts
- Put processes in place to assess and address whether, when, how, and the extent to which individuals' data is shared outside of the organization as part of cybersecurity information-sharing activities

4.2. Integrating the Cybersecurity Framework With Enterprise Risk Management

Organizations can employ an enterprise risk management (ERM) approach to balance multiple risk considerations, including cybersecurity. They can benefit from using the Framework to better harmonize cybersecurity risk management activities with other risk management domains (e.g., financial, legal, legislative, operational, privacy, reputational, safety). Enterprise leaders receive significant input about current and planned risk activities as they integrate governance and risk strategy with results from previous Framework cycles. Integrated data about a broad set

of risks, including cybersecurity risk data, helps leaders understand potential risk changes so that they can make informed decisions about the direction of the enterprise. Fig. 6 illustrates this iterative cycle of risk communication at all organizational levels.

NIST IR 8286, *Integrating Cybersecurity and Enterprise Risk Management*, describes an example approach. That report is part of a series of publications that describes the use of cybersecurity risk management activities, in conjunction with the Cybersecurity Framework, to keep leaders informed about cybersecurity risks in context with other risks. Specific activities for integrating the CSF into ERM are described in the main report and provide additional details to Cybersecurity Framework users.

Section 3.1 of this document presents five steps that an organization could take using Framework Profiles to help inform continuous improvement of its cybersecurity posture. Organizations can expand and enhance those steps to integrate ERM considerations, such as:

- Ensuring that assets that are important to the enterprise are considered when defining the Framework use case (step 1)
- Including ERM-related input (e.g., enterprise risk categories, priorities, integrated risk registers) when gathering information needed to prepare the Profiles (step 2)
- Considering tangible and assessable representation of risks (risk scenarios) from throughout the enterprise when evaluating the risk implications of the current state and defining the desired state that will address important risks (step 3)
- Ensuring that expectations from those in ERM roles (e.g., enterprise risk steering committee, senior executives, and officers) are included in the analysis and prioritization to create an action plan (step 4)
- Communicating results from action plan implementation (step 5) to those in ERM roles to help monitor cybersecurity risk strategy results, adjust that strategy to pursue opportunities, and reduce exposure throughout the enterprise. ERM stakeholders may also recommend adjustments to the desired tier (and associated governance, management, and third-party risk management activities) to improve achievement of enterprise goals.

As these steps are iteratively applied, they provide enterprise leaders with information to help them understand what conditions might improve or impair the organization's ability to achieve its business objectives. The action plan should include metrics, such as key performance indicators (KPIs) and key risk indicators (KRIs) that help monitor, evaluate, and adjust the enterprise risk strategy. As actions occur, results can be recorded (e.g., through aggregated and normalized risk registers and profiles). Reviews of those results, expressed in terms of business and enterprise objectives, help to maintain and adjust organizational strategy. This monitorevaluate-adjust cycle, executed through the Framework steps, aids in aligning cybersecurity risk activity with management of the many other types of risk facing the enterprise.

5. Next Steps

Whether an organization is using the Cybersecurity Framework for the first time or it has used the Framework previously, it is important to remember that the CSF is designed to be used in conjunction with other cybersecurity frameworks, standards, and guidance.

NIST provides many resources that are specific to the Framework and its use on the Cybersecurity Framework website, as well as hundreds of cybersecurity publications and other resources hosted on the NIST Computer Security Resource Center (CSRC) website and the NIST National Cybersecurity Center of Excellence (NCCoE) website. While these resources are not part of the Framework Core, they provide detailed information on cybersecurity risk management that supports use of the Framework.

Since the Framework is technology-neutral, organizations should also look for resources that are specific to their technologies, such as:

- NIST Artificial Intelligence Risk Management Framework (AI RMF)
- SP 800-207, *Zero Trust Architecture*, and the NCCoE's Implementing a Zero Trust Architecture project
- NIST Cybersecurity for IoT Program

As organizations continue on their cybersecurity journey, NIST is committed to providing guidance to address current and future cybersecurity challenges.

Appendix A. Templates for Profiles and Action Plans

This appendix provides notional templates that organizations can choose to use and adapt for their own Profiles and action plans. Organizations should not feel compelled to follow these templates in terms of format, structure, or data representation.

A.1. Notional Organizational Profile Template

Table 1 depicts an excerpt of a blank template for an organization's Profiles, as described in Section 3.1. This notional template uses four groupings for its elements:

- **Selected Framework Outcomes:** The Functions, Categories, or Subcategories of the Framework being included in the Profile. Profiles may be at any outcome level. Organizations may downselect outcomes or add their own Functions, Categories, or Subcategories to address specific needs or unique organizational risks.
- **Current Profile:** Elements chosen by the organization to characterize its current cybersecurity risk management posture.
- **Target Profile:** Elements chosen by the organization to characterize its cybersecurity risk management goals and its plans for achieving those goals.
- **Notes:** A space for additional comments on each selected outcome.

As the notional template demonstrates, the Current Profile and the Target Profile do not need to include the same elements.

Table 1. Notional organizational profile template

Selected Framework Outcomes (Functions, Categories, or Subcategories)	Current Policies, Processes, and Procedures	Current Internal Practices	Target Priority	Target Policies, Processes, and Procedures	Target Roles and Responsibilities	Target Selected Informative References	Notes

Some organizations choose to express the desired outcomes as a series of interim milestones, such as quarterly, annual, and five-year targets for improvement. In those cases, multiple interim Target Profiles could be included in one table, each describing progress toward defined goals.

The following list provides examples of possible elements that could be included within Profiles:

- **Status**: The current state or condition of an outcome, such as whether an organization is achieving it or the degree to which the organization is achieving it. This can use any status scheme, such as a simple status (e.g., Achieved, Not Achieved) or a more granular scheme that indicates the degree of progress (e.g., Not Evaluated, Planned, Partially Achieved, Fully Achieved). More detailed status values can provide more insights when creating a gap analysis or action plan. An organization may also include its Tier selection.

- **Priority**: The relative importance of an outcome compared to other outcomes. Organizations can choose a simple prioritization schema (e.g., Prioritized/Not Prioritized) or a multi-level schema (e.g., High, Moderate, Implement Later) to provide more insights when creating a gap analysis or action plan.
- **Policies, Processes, and Procedures**: Information on the organization's policies, processes, and procedures related to a particular outcome. For example, a policy might state that access to resources requires a certain degree of authorization and a supporting procedure might specify the correct access control rules for requesting and approving access to a specific software component.
- **Internal Practices**: Information on how the organization implements its policies, processes, and procedures for a particular outcome, as well as any other organizational activities. The Internal Practices element could be divided into more granular elements, such as the hardware and software tools and the methodologies used to perform the practices.
- **Roles and Responsibilities**: People, teams, or other organizations who help achieve the outcome or who are responsible for ensuring that the outcome is achieved. This includes shared responsibility models, such as specifying which aspects of an outcome an outsourcer and the organization are each responsible for. This element could also include Work Roles, Tasks, and Knowledge and Skills needed for achieving each outcome, such as from SP 800-181r1, *NIST Workforce Framework for Cybersecurity (NICE Framework)*.
- **Selected Informative References:** Applicable standards, guidance, requirements, organizational policies, and other references selected by the organization.
- **Measurements:** Selected measurements. See Section 3.2 for more information on measuring cybersecurity risk outcomes.
- **Artifacts and Evidence:** Information on artifacts that contain evidence of achieving particular outcomes. The Profile could include pointers to files, databases, and other resources that contain the artifacts, or the Profile could characterize the artifacts and provide a point of contact for each one.

A.2. Notional Action Plan Template

Table 2 illustrates an excerpt of a notional action plan template, as described in Section 3.1. Organizations that choose to use this template should customize it to meet their needs and priorities.

In this template, the action plan includes rows for the priority of each action item, a description of the action item, the responsible party or department, the target completion date, and the resources required to accomplish the action item (e.g., personnel, budget, tools). This template can be integrated with the Profiles or maintained separately. The action plan can be based on outcomes at the Function, Category, or Subcategory level or a combination of those levels.

Table 2. Notional action plan template

Selected Framework Outcomes	Priority	Action Item	Responsible Parties	Target Completion Date	Resources Required

Appendix B. Framework Tier Descriptions

Table 3 describes the Framework Tiers discussed in Section 3.2. The Tiers characterize the typical rigor of the cybersecurity risk governance and management practices throughout an organization, including third-party cybersecurity risks.

Table 3. Framework Tiers

Tier	Cybersecurity Risk Governance	Cybersecurity Risk Management	Third-Party Cybersecurity Risks
Tier 1: Partial	Application of organizational cybersecurity risk strategy is managed in an ad hoc manner. Prioritization is ad hoc and not formally based on objectives, requirements, assets importance, or threat environment.	There is limited awareness of cybersecurity risks and its relevance at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by case basis, generally on demand (in response to a requirement or regulation). The organization may not have processes that enable cybersecurity information to be shared within the organization and other interested parties.	The organization is generally unaware of the cybersecurity risks of the products and services it provides and uses. The organization does not understand its role in the larger ecosystem with respect to either its dependencies or dependents. The organization has not formalized its capabilities to internally manage cybersecurity risks in its supply chains or with its partners and may do these activities in a one-off manner.
Tier 2: Risk Informed	Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, its assets and their criticality, the threat environment, or business/mission requirements.	There is an awareness of cybersecurity risks at the organizational level, but an organization-wide approach to managing cybersecurity risks has not been established. Consideration of cybersecurity in organizational objectives, process, and programs may occur at some but not all levels of the organization. Cyber risk assessment of organizational and external assets occurs but is not typically repeatable or reoccurring. Cybersecurity information is shared within the organization on an informal basis.	The organization understands the cybersecurity risks in its supply chains that are associated with the products and services that either support the business and mission functions of the organization or are utilized in the organization's products or services. The organization is aware of the cybersecurity risks associated with the products and services it provides and uses, but does not act consistently or formally in response to those risks.

Commented [JCAC13]: Texts in red are elements to be included to improve how cybersecurity risks are managed in organizations.

Tier 3: Repeatable	The organization's risk management practices are formally approved and expressed as policy. Risk-informed policies, processes, and procedures are defined, implemented as intended, and continuously reviewed. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements, threats, assets, and technological landscape.	There is an organization-wide approach to managing cybersecurity risks. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. The organization consistently and accurately monitors cybersecurity risks of assets. Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risks. Senior executives ensure that cybersecurity is considered through all lines of operation in the organization.	The organization risk strategy is informed by cybersecurity risks associated with the products and services it provides and uses. Personnel formally act upon those risks, including through mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring. An organization-wide approach to manage cybersecurity risks in its supply chains is instantiated in the organization's enterprise risk management policies, processes, and procedures, which are in turn implemented consistently and as intended and continuously monitored and reviewed.
Tier 4: Adaptive	There is an organization-wide approach to manage cybersecurity risks that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The relationship between cybersecurity risks and organizational objectives is clearly understood and considered when making decisions. Senior executives monitor cybersecurity risks in the same context as financial and other organizational risks. The organizational budget is based on an understanding of the current and predicted risk environment and risk tolerance. Business units implement executive vision and analyze system-level risks in the context of organizational risk tolerances. Cybersecurity risk management is part of the organizational culture. It evolves from an awareness of previous activities and continuous awareness of activities on organizational systems and networks. The organization can quickly and efficiently account for changes to business/mission objectives in how risk is approached and communicated.	The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. Through a process of continuous improvement that incorporates advanced cybersecurity technologies and practices, the organization actively adapts to a changing technological landscape and responds in a timely and effective manner to evolving, sophisticated threats.	The organization uses real-time or near real-time information to understand and consistently act upon cybersecurity risks associated with the products and services it provides and uses. The organization has a governance structure (e.g., Risk Council) that manages the organizational risk silos as well as up and down the supply chain and addresses its supply chain security requirements in tandem with other risks. The organization collaborates with its suppliers and proactively manages its relationships with its suppliers and downstream dependents (e.g., customers).

Appendix C. Framework Core

This section presents the Functions, Categories, and Subcategories of the Framework Core. The Implementation Examples and Informative References of the Core will be maintained online on the NIST Cybersecurity Framework website to allow for more frequent updates.

Table 4 shows the CSF 2.0 Core Function and Category names and unique alphabetic identifiers.

Table 4. CSF 2.0 Core Function and Category Names and Identifiers

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI

Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

The remaining tables in this appendix show the CSF 2.0 Core Functions, Categories, and Subcategories with one table for each Function. Each table also identifies when a CSF 1.1 Category or Subcategory has been moved to one or more CSF 2.0 Subcategories for traceability.

824 The following are links to each of the CSF 2.0 Function tables:

Table 5. **GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy**
Table 6. **IDENTIFY (ID): Help determine the current cybersecurity risk to the organization**
Table 7. **PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk**
Table 8. **DETECT (DE): Find and analyze possible cybersecurity attacks and compromises**
Table 9. **RESPOND (RS): Take action regarding a detected cybersecurity incident**
Table 10. **RECOVER (RC): Restore assets and operations that were impacted by a cybersecurity incident**

Table 5. GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy

Category	Subcategory
Organizational Context (GV.OC): The circumstances — mission, stakeholder expectations, and legal, regulatory, technical, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood (formerly ID.BE)	
	GV.OC-01: The organizational mission is understood and informs cybersecurity risk management (formerly ID.BE-02, ID.BE-03)
	GV.OC-02: Internal and external stakeholders are determined, and their needs and expectations regarding cybersecurity risk management are understood
	GV.OC-03: Legal, regulatory, technical, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed (formerly ID.GV-03)
	GV.OC-04: Critical objectives, capabilities, infrastructure, and services that stakeholders depend on or expect from the organization are determined and communicated (formerly ID.BE-04, ID.BE-05)
	GV.OC-05: Outcomes, capabilities, technologies and infrastructure, and services that the organization depends on are determined and communicated (formerly ID.BE-01, ID.BE-04)

Commented [JCAC14]: Several texts in red are suggested to improve the description of categories and subcategories

Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions (formerly ID.RM)	
	GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders (formerly ID.RM-01)
	GV.RM-02: Risk appetite and risk tolerance statements are determined, communicated, and maintained (formerly ID.RM-02, ID.RM-03)
	GV.RM-03: Enterprise risk management processes include cybersecurity risk management activities and outcomes (formerly ID.GV-04)
	GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated
	GV.RM-05: Lines of communication across the organization and externally (to relevant interested parties) are established for cybersecurity risks, including risks from suppliers and other third parties
	GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated
	GV.RM-07: Strategic opportunities (i.e., positive risks) are identified and included in organizational cybersecurity risk discussions
Cybersecurity Supply Chain Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by	

organizational stakeholders (formerly ID.SC)	
	GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders (formerly ID.SC-01)
	GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally, ensuring a proper segregation of duties. (formerly ID.AM-06)
	GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes (formerly ID.SC-02)
	GV.SC-04: Suppliers are known and prioritized by criticality
	GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties (formerly ID.SC-03)
	GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships
	GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are identified, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship (formerly ID.SC-02, ID.SC-04)
	GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities (formerly ID.SC-05)
	GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle
	GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement

Roles, Responsibilities, and Authorities (GV.RR): Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated (formerly ID.GV-02)	
	GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving
	GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, enforced (formerly ID.AM-06, ID.GV-02, DE.DP-01) ensuring a proper segregation of duties.
	GV.RR-03: Adequate resources are allocated commensurate with cybersecurity risk strategy, roles and responsibilities, and policies
	GV.RR-04: Cybersecurity is included in human resources practices (formerly PR.IP-11)
Policies, Processes, and Procedures (GV.PO): Organizational cybersecurity policies, processes, and procedures are established, communicated, enforced, and improved (formerly ID.GV-01)	
	GV.PO-01: Policies, processes, and procedures for managing cybersecurity risks are established based on organizational context, cybersecurity strategy, and priorities and are communicated and enforced (formerly ID.GV-01)
	GV.PO-02: Policies, processes, and procedures for managing cybersecurity risks are reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission (formerly ID.GV-01)

Oversight (GV.OV): Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, adjust, and improve the risk management strategy	
	GV.OV-01: Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction
	GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks
	GV.OV-03: Organizational cybersecurity risk management performance is measured and reviewed to confirm and adjust strategic direction

Table 6. IDENTIFY (ID): Help determine the current cybersecurity risk to the organization

Category	Subcategory
Asset Management (ID.AM): Assets (e.g., data, hardware software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy	
	ID.AM-01: Inventories of hardware managed by the organization are maintained
	ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained
	ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained (formerly ID.AM-03, DE.AE-01)
	ID.AM-04: Inventories of services provided by suppliers are maintained
	ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission

	ID.AM-06: Dropped (moved to GV.RR-02, GV.SC-02)
	ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained
	ID.AM-08: Systems, hardware, software, and services are managed throughout their life cycle (formerly PR.DS-03, PR.IP-02, PR.MA-01, PR.MA-02)
Business Environment (ID.BE): Dropped (moved to GV.OC)	
	ID.BE-01: Dropped (moved to GV.OC-05)
	ID.BE-02: Dropped (moved to GV.OC-01)
	ID.BE-03: Dropped (moved to GV.OC-01)
	ID.BE-04: Dropped (moved to GV.OC-04, GV.OC-05)
	ID.BE-05: Dropped (moved to GV.OC-04)
Governance (ID.GV): Dropped (moved to GV)	
	ID.GV-01: Dropped (moved to GV.PO)
	ID.GV-02: Dropped (moved to GV.RR-02)
	ID.GV-03: Dropped (moved to GV.OC-03)
	ID.GV-04: Dropped (moved to GV.RM-03)
Risk Assessment (ID.RA): The organization understands the	

cybersecurity risk to the organization, assets, and individuals.	
	ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded (formerly ID.RA-01, PR.IP-12, DE.CM-08)
	ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources
	ID.RA-03: Internal and external threats to the organization are identified and recorded
	ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded
	ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk and inform risk prioritization
	ID.RA-06: Risk responses are chosen from the available options, prioritized, planned, tracked, and communicated (formerly ID.RA-06, RS.MI-03)
	ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked (formerly part of PR.IP-03)
	ID.RA-08: Processes for receiving, analyzing, and responding to vulnerability disclosures are established (formerly RS.AN-05)
	ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use (formerly PR.DS-08)
Risk Management Strategy (ID.RM): Dropped (moved to GV.RM)	
	ID.RM-01: Dropped (moved to GV.RM-01)
	ID.RM-02: Dropped (moved to GV.RM-02)
	ID.RM-03: Dropped (moved to GV.RM-02)

Supply Chain Risk Management (ID.SC): Dropped (moved to GV.SC)	
	ID.SC-01: Dropped (moved to GV.SC-01)
	ID.SC-02: Dropped (moved to GV.SC-03, GV.SC-07)
	ID.SC-03: Dropped (moved to GV.SC-05)
	ID.SC-04: Dropped (moved to GV.SC-07)
	ID.SC-05: Dropped (moved to GV.SC-08, ID.IM-02)
Improvement (ID.IM): Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all Framework Functions	
	ID.IM-01: Continuous evaluation is applied to identify improvements
	ID.IM-02: Security tests and exercises, including those done in coordination with suppliers and relevant third parties, are conducted to identify improvements (formerly ID.SC-05, PR.IP-10, DE.DP-03)
	ID.IM-03: Lessons learned during execution of operational processes, procedures, and activities are used to identify improvements (formerly PR.IP-07, PR.IP-08, DE.DP-05, RS.IM-01, RS.IM-02, RC.IM-01, RC.IM02)
	ID.IM-04: Cybersecurity plans that affect operations are communicated, maintained, and improved (formerly PR.IP-09)

Commented [JCAC15]: The entire category should be part of govern

Table 7. PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk

Category	Subcategory
Identity Management, Authentication, and Access Control (PR.AA): Access to physical and logical assets is limited to authorized users, services, and hardware, and is managed commensurate with the assessed risk of unauthorized access (formerly PR.AC)	
	PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization (formerly PR.AC-01)
	PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions (formerly PR.AC-06)
	PR.AA-03: Users, services, and hardware are authenticated (formerly PR.AC-03, PR.AC-07)
	PR.AA-04: Identity assertions are protected, conveyed, and verified
	PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties (formerly PR.AC-01, PR.AC-03, PR.AC-04)
	PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk (formerly PR.AC-02, PR.PT-04)
Identity Management, Authentication and Access Control (PR.AC): Dropped (moved to PR.AA)	
	PR.AC-01: Dropped (moved to PR.AA-01, PR.AA-05)
	PR.AC-02: Dropped (moved to PR.AA-06)

	PR.AC-03: Dropped (moved to PR.AA-03, PR.AA-05, PR.IR-01)
	PR.AC-04: Dropped (moved to PR.AA-05)
	PR.AC-05: Dropped (moved to PR.IR-01)
	PR.AC-06: Dropped (moved to PR.AA-02)
	PR.AC-07: Dropped (moved to PR.AA-03)
Awareness and Training (PR.AT): The organization's personnel are provided cybersecurity awareness and training so they can perform their cybersecurity-related tasks	
	PR.AT-01: Users are provided awareness and training so they possess the knowledge and skills to perform general tasks with security risks in mind (formerly PR.AT-01, PR.AT-03, RS.CO-01)
	PR.AT-02: Individuals in specialized roles are provided awareness and training so they possess the knowledge and skills to perform relevant tasks with security risks in mind (formerly PR.AT-02, PR.AT-03, PR.AT-04, PR.AT-05)
	PR.AT-03: Dropped (moved to PR.AT-01, PR.AT-02)
	PR.AT-04: Dropped (moved to PR.AT-02)
	PR.AT-05: Dropped (moved to PR.AT-02)
Data Security (PR.DS): Data is managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information	

	PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected (formerly PR.DS-01, PR-DS.05, PR.DS-06, PR.PT-02)
	PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected (formerly PR.DS-02, PR.DS-05)
	PR.DS-03: Dropped (moved to ID.AM-08)
	PR.DS-04: Dropped (moved to PR.IR-04)
	PR.DS-05: Dropped (moved to PR.DS-01, PR-DS-02, PR.DS-10)
	PR.DS-06: Dropped (moved to PR.DS-01, DE.CM-09)
	PR.DS-07: Dropped (moved to PR.IR-01)
	PR.DS-08: Dropped (moved to ID.RA-09, DE.CM-09)
	PR.DS-09: Data is managed throughout its life cycle, including destruction (formerly PR.IP-06)
	PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected (formerly PR.DS-05)
	PR.DS-11: Backups of data are created, protected, maintained, and tested (formerly PR.IP-04)
Information Protection Processes and Procedures (PR.IP): Dropped (moved to other Categories and Functions)	
	PR.IP-01: Dropped (moved to PR.PS-01)
	PR.IP-02: Dropped (moved to ID.AM-08)
	PR.IP-03: Dropped (moved to PR.PS-01, ID.RA-07)
	PR.IP-04: Dropped (moved to PR.DS-11)
	PR.IP-05: Dropped (moved to PR.IR-02)
	PR.IP-06: Dropped (moved to PR.DS-09)

	PR.IP-07: Dropped (moved to ID.IM-03)
	PR.IP-08: Dropped (moved to ID.IM-03)
	PR.IP-09: Dropped (moved to ID.IM-04)
	PR.IP-10: Dropped (moved to ID.IM-02)
	PR.IP-11: Dropped (moved to GV.RR-04)
	PR.IP-12: Dropped (moved to ID.RA-01, PR.PS-02)
Maintenance (PR.MA): Dropped (moved to ID.AM-08)	
	PR.MA-01: Dropped (moved to ID.AM-08, PR.PS-03)
	PR.MA-02: Dropped (moved to ID.AM-08, PR.PS-02)
Protective Technology (PR.PT): Dropped (moved to other Protect Categories)	
	PR.PT-01: Dropped (moved to PR.PS-04)
	PR.PT-02: Dropped (moved to PR.DS-01, PR.PS-01)
	PR.PT-03: Dropped (moved to PR.PS-01)
	PR.PT-04: Dropped (moved to PR.AA-07, PR.IR-01)
	PR.PT-05: Dropped (moved to PR.IR-04)

Platform Security (PR.PS): The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, availability	
	PR.PS-01: Configuration management practices are applied (formerly PR.IP-01, PR.IP-03, PR.PT-02, PR.PT-03)
	PR.PS-02: Software is designed, developed or acquired, maintained, replaced, and removed commensurate with risk (formerly PR.IP-12, PR.MA-02)
	PR.PS-03: Hardware is designed, developed or acquired, maintained, replaced, and removed commensurate with risk (formerly PR.MA-01)
	PR.PS-04: Log records are generated and made available for continuous monitoring (formerly PR.PT-01)
	PR.PS-05: Installation and execution of unauthorized software are prevented
	PR.PS-06: Secure software development practices are integrated, including strategies such as security and cybersecurity by design, and their performance is monitored throughout the software development life cycle
Technology Infrastructure Resilience (PR.IR): Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience	
	PR.IR-01: Networks and environments are protected from unauthorized logical access and usage (formerly PR.AC-03, PR.AC-05, PR.DS-07, PR.PT-04)
	PR.IR-02: The organization's technology assets are protected from environmental threats (formerly PR.IP-05)
	PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations (formerly PR.PT-05)
	PR.IR-04: Adequate resource capacity to ensure availability is maintained (formerly PR.DS-04)

Commented [JCAC16]: Several texts in red are suggested to improve the description of categories and subcategories

Table 8. DETECT (DE): Find and analyze possible cybersecurity attacks and compromises

Category	Subcategory
Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, new or modified vulnerabilities, and other potentially adverse events	
	DE.CM-01: Networks and network services are monitored to find potentially adverse events (formerly DE.CM-01, DE.CM-04, DE.CM-05, DE.CM-07)
	DE.CM-02: The physical environment is monitored to find potentially adverse events
	DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events (formerly DE.CM-03, DE.CM-07)
	DE.CM-04: Dropped (moved to DE.CM-01, DE.CM-09)
	DE.CM-05: Dropped (moved to DE.CM-01, DE.CM-09)
	DE.CM-06: External service provider activities and services are monitored to find potentially adverse events (formerly DE.CM-06, DE.CM-07)
	DE.CM-07: Dropped (moved to DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09)
	DE.CM-08: Dropped (moved to ID.RA-01)
	DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events (formerly PR.DS-06, PR.DS-08, DE.CM-04, DE.CM-05, DE.CM-07)

Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents (formerly DE.AE, DE.DP-02)	
	DE.AE-01: Dropped (moved to ID.AM-03)
	DE.AE-02: Potentially adverse events are analyzed to better understand associated activities
	DE.AE-03: Information is correlated from multiple sources
	DE.AE-04: The estimated impact and scope of adverse events are determined
	DE.AE-05: Dropped (moved to DE.AE-08)
	DE.AE-06: Information on adverse events is provided to authorized staff and tools (formerly DE.DP-04)
	DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis
	DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria (formerly DE.AE-05)
Detection Processes (DE.DP): Dropped (moved to other Categories and Functions)	
	DE.DP-01: Dropped (moved to GV.RR-02)
	DE.DP-02: Dropped (moved to DE.AE)
	DE.DP-03: Dropped (moved to ID.IM-02)
	DE.DP-04: Dropped (moved to DE.AE-06)
	DE.DP-05: Dropped (moved to ID.IM-03)

Table 9. RESPOND (RS): Take action regarding a detected cybersecurity incident

Category	Subcategory
Response Planning (RS.RP): Dropped (moved to RS.MA)	
	RS.RP-01: Dropped (moved to RS.MA-01)
Incident Management (RS.MA): Responses to detected cybersecurity incidents are managed (formerly RS.RP)	
	RS.MA-01: The incident response plan is executed once an incident is declared in coordination with relevant third parties (formerly RS.RP-01, RS.CO-04)
	RS.MA-02: Incident reports are triaged and validated (formerly RS.AN-01, RS.AN-02)
	RS.MA-03: Incidents are categorized and prioritized (formerly RS.AN-04, RS.AN-02)
	RS.MA-04: Incidents are escalated or elevated as needed (formerly RS.AN-02, RS.CO-04)
	RS.MA-05: The criteria for initiating incident recovery are applied
Incident Analysis (RS.AN): Investigation is conducted to ensure effective response and support forensics and recovery activities	
	RS.AN-01: Dropped (moved to RS.MA-02)
	RS.AN-02: Dropped (moved to RS.MA-02, RS.MA-03, RS.MA-04)
	RS.AN-03: Analysis is performed to determine what has taken place during an incident and the root cause of the incident

	RS.AN-04: Dropped (moved to RS.MA-03)
	RS.AN-05: Dropped (moved to ID.RA-08)
	RS.AN-06: Actions performed during an investigation are recorded and the records' integrity and provenance are preserved (formerly part of RS.AN-03)
	RS.AN-07: Incident data and metadata are collected, and their integrity and provenance are preserved
	RS.AN-08: The incident's magnitude is estimated and validated
Incident Response Reporting and Communication (RS.CO): Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies	
	RS.CO-01: Dropped (moved to PR.AT-01)
	RS.CO-02: Internal and external stakeholders are notified of incidents
	RS.CO-03: Information is shared with designated internal and external stakeholders (formerly RS.CO-03, RS.CO-05)
	RS.CO-04: Dropped (moved to RS.MA-01, RS.MA-04)
	RS.CO-05: Dropped (moved to RS.CO-03)
Incident Mitigation (RS.MI): Activities are performed to prevent expansion of an event and mitigate its effects	
	RS.MI-01: Incidents are contained
	RS.MI-02: Incidents are eradicated
	RS.MI-03: Dropped (moved to ID.RA-06)

Improvements (RS.IM): Dropped (moved to ID.IM)	
	RS.IM-01: Dropped (moved to ID.IM-03)
	RS.IM-02: Dropped (moved to ID.IM-03)

Table 10. RECOVER (RC): Restore assets and operations that were impacted by a cybersecurity incident

Category	Subcategory
Incident Recovery Plan Execution (RC.RP): Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents	
	RC.RP-01: The recovery portion of the incident response plan is executed once initiated from the incident response process
	RC.RP-02: Recovery actions are determined, scoped, prioritized, and performed
	RC.RP-03: The integrity of backups and other restoration assets is verified before using them for restoration
	RC.RP-04: Critical mission functions and cybersecurity risk management are considered to establish postincident operational norms
	RC.RP-05: The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed
	RC.RP-06: The criteria for determining the end of incident recovery are applied, and incident-related documentation is completed

Incident Recovery Communication (RC.CO): Restoration activities are coordinated with internal and external parties	
	RC.CO-01: Dropped (moved to RC.CO-04)
	RC.CO-02: Dropped (moved to RC.CO-04)
	RC.CO-03: Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders
	RC.CO-04: Public updates on incident recovery are properly shared using approved methods and messaging (formerly RC.CO-01, RC.CO-02)
Improvements (RC.IM): Dropped (moved to ID.IM)	
	RC.IM-01: Dropped (moved to ID.IM-03)
	RC.IM-02: Dropped (moved to ID.IM-03)