---

**Author: stonegr1   Subject: Highlight   Date: 9/25/2023 13:15:58**

Line 71 - "cybersecurity risks"
   By definition a harm coupled with judgment on likelihood that harm will materialize.  Hence it is harm associated with a risk, as opposed to harm from a risk.

Line 71 - suggest change:
   From: "impacts to organizations from cybersecurity risks"
   To: "impacts to organizations associated with cybersecurity risks"

Line 72 - suggest change:
   From: "Cybersecurity risks also threaten"
   To: "Cybersecurity risks also include threats to"

---

**Author: stonegr1   Subject: Highlight   Date: 9/25/2023 13:17:00**

Line 74 - "CSF 2.0 provides guidance for reducing 74 cybersecurity risks"
   Rather than just 'reducing' which is measured by 'any amount less' suggest the purpose is to effectively manage.  Note that this aligns with current text in lines 93, 94, and 99.

Examples of associated changes in the document - examples, not complete list:

Line 74 - suggest change:
   From: "provides guidance for reducing cybersecurity risks"
   To: "provides guidance for effectively managing cybersecurity risks"

Line 76 - suggest change:
   From: "and the actions that will reduce them"
   To: "and the actions to effectively manage them"

Line 88 - suggest change:
   From: "terms of reducing cybersecurity risk"
   To: "terms of managing cybersecurity risk"

Line 98 - suggest change:
   From: "reduce its cybersecurity risk"
   To: "effectively manage its cybersecurity risk"

Line 116 - suggest change:
   From: "actions for reducing cybersecurity risk"
   To: "actions for effectively managing cybersecurity risk"

Line 286 & 287 suggest change:
   From: "cybersecurity posture"
   To: "risk management posture"

Line 289 suggest change:
   From: "cybersecurity outcomes"
   To: "cybersecurity risk management outcomes"
   To: "effectively manage"

Author: stonegr1    Subject: Highlight    Date: 9/25/2023 13:17:37
Line 108-113 - Missing assessing the threat environment and determining risks.

Line 111 - insert before:
  Assess current threat environment, including nature of threat sources and their capability, motivation to harm the organization, and intent to use cyberspace to accomplish or facilitate doing so.

  Determine existing cybersecurity risks as nature and degree of potential harm and judgment as to likelihood of this harm occurring.

Author: stonegr1    Subject: Highlight    Date: 9/25/2023 13:18:20

Line 174 - "The Framework Core provides a set of cybersecurity outcomes (arranged by Function, Category, 174 and Subcategory)"

  Suggest that from an organizational perspective and risk of harm to organization - the needed 'outcomes' are those that directly relay aspects of achieving management of risk and addressing organizational harm.

The needed outcomes are what must be achieved toward managing risk by whatever means or methods are employed.

  The needed outcomes should **not** be expressed as the employment of types of means or methods, since those are means to an end and should not themselves be stated as the end to be achieved.

Author: stonegr1    Subject: Highlight    Date: 9/25/2023 13:19:02

Line 190 - "The Framework Core Functions — GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, and 190 RECOVER"

  As indicated for line 174, the outcomes should be aspects of achieving management of risk.  However the GIPDRR set seems to be a different dimension.  For example, while PDRR may all be used, it is not essential that they all be.  Nor is there any one right answer as to how much P, how much D, how much R or how much R. PDRR represent a broad set of means/methods from which to choose in order to achieve risk management (along with G and I).

Bottom line: Do not see a calculus in the CSF for going from achieved (as stated) GIPDRR to achieved management of risk.  Need a framework for managing risk.  But seem to have a framework for 'doing stuff'.

Author: stonegr1    Subject: Highlight    Date: 9/15/2023 14:37:01

Line 192 - suggest that "Govern" is a primary element for an effective management of cybersecurity risks.  The others fall more into technical means that are applied and fall at a level below a frame work for effectively managing risk.

In other words - the essence of the framework is govern to effectively employ the means/methods - administrative, technical, managerial - toward achieving consistent effective risk management.  The content of the means/methods is at a level below.

Author: stonegr1     Subject: Highlight    Date: 9/15/2023 15:15:24
Line 208 - PROTECT - the prevention or reduction in cybersecurity risk = the totality of what is to be achieved.  Hence with this as the definition for 'Protect' - there is not need for DRR.

Suggest that as NIST SP 800-53 more often uses 'protect' as the broad term covering all that is done - so should the CSF.  Otherwise suggest use 'Protect' = Prevent in order to avoid 'stepping on' DRR. As DRR also serve to reduce cybersecurity risk.

Using "prevent or reduce", PROTECT can be proactive (means/measures that inherently do this - e.g., subnetting) or reactive (response to detected event).

Note that this means that there is an element of RESPOND within PROTECT.

Author: stonegr1     Subject: Highlight    Date: 9/25/2023 13:19:46
Line 215 - DETECT - Note that 'Detect' can be used to both prevent and to limit harm; for example an intrusion prevention system (IDS) detects-prevent while an intrusion detection system (IDS) detects-limit-harm (primarily).

And both RESPOND and RECOVER presume awareness of a reason to respond - hence a tie to DETECT

Bottom line: PROTECT, RESPOND, and RECOVER all have a dependence on DETECT

Author: stonegr1     Subject: Highlight    Date: 9/15/2023 15:15:14
Line 219 - RESPOND has dependencies on
DETECT

Author: stonegr1    Subject: Highlight    Date: 9/25/2023 13:20:19
Line 241 - "cybersecurity outcomes"
   As indicated previously, suggest need outcomes relaying what is achieved for risk management.  And not outcomes as an implemented means or method.

Author: stonegr1    Subject: Highlight   Date: 9/25/2023 13:20:53
Line 502 - "particularly how cybersecurity-related 502 uncertainties might"

Suggest change to reflect this is about 'risk management' and the issues related to risk:
From: "particularly how cybersecurity-related uncertainties might"
To: ""particularly how cybersecurity risk might"

Author: stonegr1    Subject: Highlight   Date: 9/18/2023 17:05:14
Line 506 - Suggest change:
From: "establish cybersecurity priorities and objectives based"
To: "establish cybersecurity risk management priorities and objectives based"

Author: stonegr1    Subject: Highlight   Date: 9/25/2023 13:23:32
Line 521 - "As controls are 521 implemented to manage risk to an acceptable level"
   Suggest that it is less" as controls are implemented" than it is that "risk is being managed".  That is, the outcome from the controls, not just their implementation. Moreover, if 'acceptable level' is being achieved, there is little decision making needed.  It is when the management is not effective enough (or too costly) that decisions are needed.

Suggest change:
From: "As controls are implemented to manage risk to an acceptable level"
To: "As risk is being managed"

Author: stonegr1    Subject: Highlight   Date: 9/25/2023 13:24:16

Line 536 - "Express its cybersecurity risk management requirements"

Suggest again not equating security controls with "risk management requirements".  Instead suggest developing, defining, and documenting the RM requirements that must be achieved by whatever controls are implemented.

Author: stonegr1    Subject: Highlight    Date: 9/25/2023 13:25:06

Line 585 - "IDENTIFY, PROTECT, DETECT, RESPOND, and RECOVER — provide a source for the organization to consider as a basis for supplier cybersecurity requirements"

Again - Suggest that IPDRR represent buckets into which controls (and portions of controls) can be placed.  And as such represent a taxonomy for controls and not a list of 'must dos'.  Moreover, there will be in general many (many!) different sets of bucket contents that can achieve RM requirements

And it should not a be set of bucket contents that is the RM requirement, but rather what the set of buckets must achieve toward requirements defining what 'effective RM' looks like for an organization.

Effective RM is the outcome achieved from the set of buckets, not having that set.

Line 630 - "organizations integrate all of their risk management efforts at a high level by using enterprise risk management (ERM)"

Ultimately, suggest that integrating 'cybersecurity risk' into ERM is a mandatory part of effective RM.  And to do so requires defining the RM requirements as outcomes and not as an implementation of a set of means.  Purposefully maintain the distinction between outcomes that relay the definition of risk being managed and sets of means/methods for doing so.  Just implementing means should not be used in place of stating what the implementation must achieve in the context of risk that is managed to an acceptable level.

# Public Draft: The NIST Cybersecurity Framework 2.0

## National Institute of Standards and Technology

Released August 8, 2023

## Note to Reviewers

This is the public draft of the NIST Cybersecurity Framework (CSF or Framework) 2.0.

The Framework has been used widely to reduce cybersecurity risks since its initial publication in 2014. Many organizations have told NIST that CSF 1.1 remains an effective framework for addressing cybersecurity risks. There is also widespread agreement that changes are warranted to address current and future cybersecurity challenges and to make it easier for organizations to use the Framework. NIST is working with the community to ensure that CSF 2.0 is effective for the future while fulfilling the CSF's original goals and objectives.

NIST seeks feedback on whether this draft revision addresses organizations' current and anticipated future cybersecurity challenges, is aligned with leading practices and guidance resources, and reflects comments received so far. In addition, NIST requests ideas on the best way to present the modifications from CSF 1.1 to CSF 2.0 to support transition. NIST encourages concrete suggestions for improvements to the draft, including revisions to the narrative and Core.

This draft includes an updated version of the CSF Core, reflecting feedback on the April discussion draft. This publication does not contain Implementation Examples or Informative References of the CSF 2.0 Core, given the need to frequently update them. Draft, initial Implementation Examples have been released under separate cover for public comment. NIST seeks feedback on what types of Examples would be most beneficial to Framework users, as well as what existing sources of implementation guidance might be readily adopted as sources of Examples (such as the NICE Framework Tasks, for example). NIST also seeks feedback on how often Implementation Examples should be updated and whether and how to accept Implementation Examples developed by the community.

As the CSF 2.0 is finalized, the updated Implementation Examples and Informative References will be maintained online on the NIST Cybersecurity Framework website, leveraging the NIST Cybersecurity and Privacy Reference Tool (CPRT). Resource owners and authors who are interested in mapping their resources to the final CSF 2.0 to create Informative References should reach out to NIST.

**Feedback on this CSF 2.0 Public Draft, as well as the related Implementation Examples draft, may be submitted to cyberframework@nist.gov by Friday, November 4, 2023.**

All relevant comments, including attachments and other supporting material, will be made publicly available on the NIST CSF 2.0 website. Personal, sensitive, confidential, or promotional business information should not be included. Comments with inappropriate language will not be considered.

This draft will be discussed at the third CSF workshop, which will be held this fall. **NIST does not plan to release another draft of CSF 2.0 for comment. Feedback on this draft will inform development of the final CSF 2.0 to be published in early 2024.**

NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY | U.S. DEPARTMENT OF COMMERCE

The modifications between Version 1.1 and this version are based on community input through:

- The 57 responses to the [Discussion Draft of the NIST Cybersecurity Framework 2.0 Core](#)
- The [92 written responses](#) to the January 2023 [CSF 2.0 Concept Paper](#)
- The February 2023 [In-Person Working Sessions](#) (attended by approximately 250 participants)
- The "Journey to the NIST Cybersecurity Framework 2.0" February 2023 [Workshop #2](#) (attended virtually by more than 2,000 participants from 69 countries)
- The "Journey to the NIST Cybersecurity Framework 2.0" August 2022 [Workshop #1](#) (attended virtually by approximately 4,000 participants from 100 countries)
- The [134 written responses](#) to the February 2022 [NIST Cybersecurity RFI](#)
- Feedback from organizations that have leveraged the CSF over the years
- NIST participation at conferences, webinars, roundtables, and meetings around the world

Cherilyn Pascoe
NIST Cybersecurity Framework Program Lead
[cyberframework@nist.gov](mailto:cyberframework@nist.gov)

**Summary of selected Framework changes from version 1.1 to this draft:**

- **Recognize broad use of the Framework:**
  - Title changed to the commonly used name, "Cybersecurity Framework" from the original "Framework for Improving Critical Infrastructure Cybersecurity."
  - Scope of the Framework has been updated to reflect use by all organizations; the original emphasis on critical infrastructure application in the narrative and Core has been modified to focus on all organizations.
  - Original emphasis on securing U.S. critical infrastructure has been modified to focus on organizations all around the world to reflect the broad and international use of the Framework.

- **Relate CSF to other Frameworks and resources:**
  - NIST reviewed updates to resources published in recent years to identify changes to the narrative and Core; this includes new references to the NIST Privacy Framework, NICE Workforce Framework for Cybersecurity (SP 800-181), Secure Software Development Framework (SP 800-218), Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (SP 800-161r1), Performance Measurement Guide for Information Security (SP 800-55), Integrating Cybersecurity and Enterprise Risk Management (NIST IR 8286) series, and the Artificial Intelligence Risk Management Framework (AI 100-1).
  - While not included in this draft, in the future NIST will release an online tool on the NIST CSF website to host the CSF 2.0 Core, with human- and machine-readable formats. This new tool will allow organizations to see the relationships online between the Core and updatable Informative References.

- **Increase guidance on CSF implementation:**
  - Implementation Examples added to provide notional examples of action-oriented processes to achieve CSF Subcategories.
  - Framework Profiles guidance revised significantly and expanded to provide guidance on the steps for using Profiles and to illustrate several purposes for Profiles.
  - Notional templates developed that organizations can use or adapt for creating their Profiles and action plans.
- **Emphasize cybersecurity governance:**
  - New Function, Govern, added to cover organizational context; risk management strategy; cybersecurity supply chain risk management; roles, responsibilities, and authorities; policies, processes, and procedures; and oversight.
  - New guidance offered on integrating the Framework with the NIST Privacy Framework and with enterprise risk management as discussed in NIST IR 8286.
  - Focus on people, process, and technology expanded throughout the implementation of the Framework.
- **Emphasize cybersecurity supply chain risk management:**
  - New Category in Govern focused on cybersecurity supply chain risk management.
  - Content updated to reflect the latest NIST guidance and Framework practices related to cybersecurity supply chain risk management and secure software development.
- **Clarify understanding of cybersecurity measurement and assessment:**
  - Information on cybersecurity assessment updated, with new pointers to NIST SP 800-55.
  - Tiers clarified to focus on cybersecurity governance, risk management, and third-party considerations.
  - Importance of continuous improvement is emphasized through a new Improvement Category in the Identify Function, as well as improvements in guidance on developing and updating Profiles and action plans.

# The NIST Cybersecurity Framework 2.0

Initial Public Draft

National Institute of Standards and Technology

August 8, 2023

NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

1  **Abstract**

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

10  **Keywords**

14  **Acknowledgments**

## Table of Contents

## List of Tables

## 60    List of Figures

69 **Executive Summary**

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

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

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

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

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

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

96 **1. Introduction**

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

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

105   • **Understand and Assess**:

106   o Describe an organization's current or target cybersecurity posture within and across
107      organizations, sectors, or business units.

108   o Determine where an organization may have cybersecurity gaps, including with
109      respect to existing or emerging threats or technologies, and assess progress toward
110      addressing those gaps.

111   o Align policy, business, and technological approaches to managing cybersecurity risks
112      across an entire organization or in a more focused area, such as a portion of the
113      organization, a specific technology, or technology suppliers.

114   • **Prioritize:**

115   o Prioritize opportunities to improve cybersecurity risk management.

116   o Identify, organize, and prioritize actions for reducing cybersecurity risks that align
117      with the organization's mission, legal and regulatory requirements, and risk
118      management and governance expectations.

119   o Inform decisions about cybersecurity-related workforce needs and capabilities.

120   • **Communicate:**

121   o Provide a common language for communicating with internal and external parties
122      about cybersecurity risks, capabilities, needs, and expectations.

123   o Complement an organization's risk management process by presenting a concise way
124      for executives and others to distill the fundamental concepts of cybersecurity risk so
125      that they express at a high level risks to be managed and how their organization uses
126      cybersecurity standards, guidelines, and practices.

127 The Framework can be used by organizations whose cybersecurity programs are at different
128 stages of maturity. An organization with an existing cybersecurity program can leverage the
129 Framework to identify opportunities to strengthen and communicate its management of
130 cybersecurity risk while considering its existing practices and needed changes. An organization
131 without an existing cybersecurity program can use the Framework as a starting point and
132 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.

158

## 1.2. Document Structure

160   This document contains the following sections and appendices:

161   • Section 2 explains the basics of the Framework Core: Functions, Categories,
162      Subcategories, Implementation Examples, and Informative References.

163   • Section 3 provides an overview of common uses for the Framework, including through
164      Current and Target Profiles, as well as guidance on using the Framework to understand,
165      assess, prioritize, and communicate cybersecurity efforts and cybersecurity supply chain
166      risk management efforts.

167   • Section 4 discusses using the Framework to help integrate cybersecurity risk management
168      with other types of risk management.

169   • Section 5 briefly outlines next steps for readers who want to use the Framework.

170   • Appendix A offers notional templates for Framework Profiles and action plans.

171   • Appendix B describes the Framework Tiers.

172   • Appendix C provides the Framework Core.

## 2. Understanding the Framework Core

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

181  order of Functions, Categories, and Subcategories in the Core is not intended to imply the
182  sequence by which they should be implemented or their relative importance. The ordering of the
183  Core is intended to resonate most with those charged with operationalizing risk management
184  within an organization.

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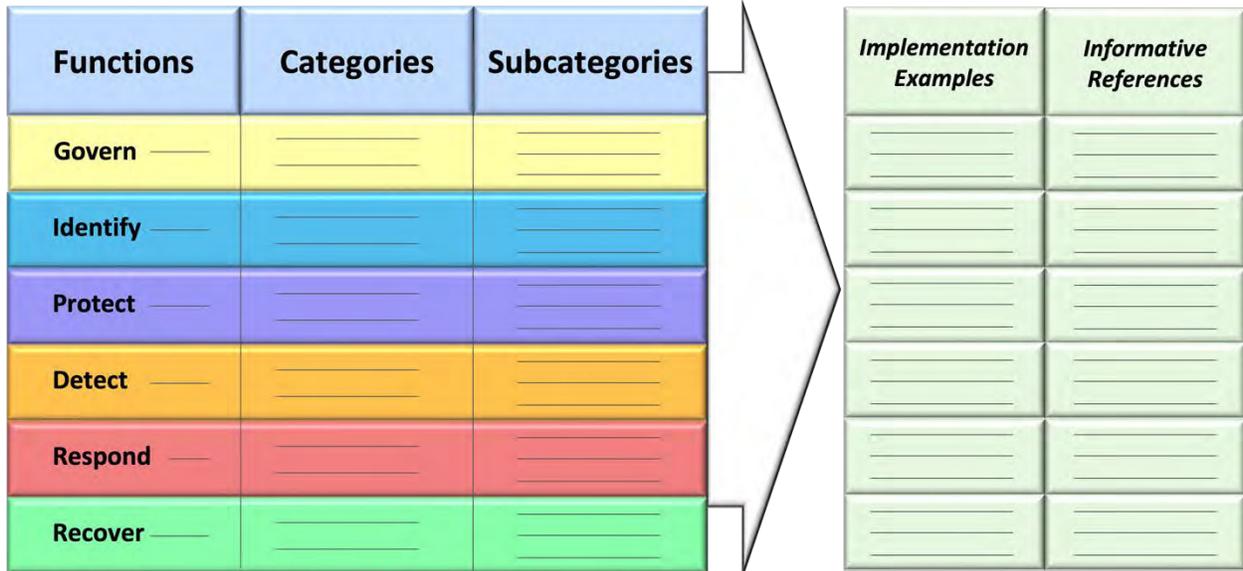


**Fig. 1. Cybersecurity Framework Core**

## 2.1. Functions, Categories, and Subcategories

190  The Framework Core **Functions** — GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, and
191  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 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.

208    • ***PROTECT (PR)*** – *Use safeguards to prevent or reduce cybersecurity risk.* Once assets and
209        risks are identified and prioritized, PROTECT supports the ability to secure those assets to
210        prevent or lower the likelihood and impact of adverse cybersecurity events. Outcomes
211        covered by this Function include awareness and training; data security; identity
212        management, authentication, and access control; platform security (i.e., securing the
213        hardware, software, and services of physical and virtual platforms); and the resilience of
214        technology infrastructure.

215    • ***DETECT (DE)*** – *Find and analyze possible cybersecurity attacks and compromises.*
216        DETECT enables timely discovery and analysis of anomalies, indicators of compromise,
217        and other potentially adverse cybersecurity events that may indicate that cybersecurity
218        attacks and incidents are occurring.

219    • ***RESPOND (RS)*** – *Take action regarding a detected cybersecurity incident.* RESPOND
220        supports the ability to contain the impact of cybersecurity incidents. Outcomes within this
221        Function cover incident management, analysis, mitigation, reporting, and
222        communication.

223    • ***RECOVER (RC)*** – *Restore assets and operations that were impacted by a cybersecurity*
224        *incident.* RECOVER supports timely restoration of normal operations to reduce the impact
225        of cybersecurity incidents and enable appropriate communication during recovery efforts.

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



232

**Fig. 2. Framework Functions**

233

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

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

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

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

## 2.2.   Implementation Examples and Informative References

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

247  - **Informative References** are standards, guidelines, regulations, and other resources to
248      help inform how an organization achieves the Functions, Categories, and Subcategories.
249      In some cases, the Informative Reference is more specific than a Subcategory, such as a
250      control from SP 800-53, *Security and Privacy Controls for Information Systems and*
251      *Organizations*. In that case, more than one control would be used to achieve the outcome
252      described in one Subcategory. In other cases, organizations may leverage higher-level
253      policies or requirements that address one or more Subcategories. Informative References
254      can also be sector- or technology-specific. In using the Framework, each organization
255      will identify applicable Informative References.

256  - **Implementation Examples** provide notional examples of concise, action-oriented steps
257      to help achieve the outcomes of the Subcategories in addition to the guidance provided by
258      Informative References. The examples are not a comprehensive list of all actions that
259      could be taken by an organization to achieve an outcome, nor do they represent a baseline
260      of required actions to address cybersecurity risk.

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

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

275   ## 3. Using the Framework

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

> 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.

283

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

285   - Create and use Framework Profiles to understand, assess, and communicate the
286     organization's current or target cybersecurity posture in terms of the Framework Core's
287     cybersecurity outcomes, and prioritize outcomes for achieving the target cybersecurity
288     posture. (Section 3.1)

289   - Assess the organization's achievement of cybersecurity outcomes. (Section 3.2)

290   - Characterize cybersecurity risk management outcomes with Framework Tiers. (Section
291     3.3)

292   - Improve cybersecurity communication with internal and external stakeholders. (Section
293     3.4)

294   - Manage cybersecurity risk throughout supply chains. (Section 3.5)

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

301   ### 3.1. Creating and Using Framework Profiles to Understand, Assess, Prioritize,
302   and Communicate

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

305   Profiles are used to understand, assess, prioritize, and tailor the sector- and technology-neutral
306   Core outcomes (i.e., Functions, Categories, and Subcategories) based on an organization's
307   mission objectives, stakeholder expectations, threat environment, and requirements and leading

308    practices, including those for specific sectors or technologies, as Fig. 3 illustrates. Organizations
309    then can prioritize their actions to achieve specific outcomes and communicate that information
310    to internal and external stakeholders. Appendix A provides a notional Profile template.
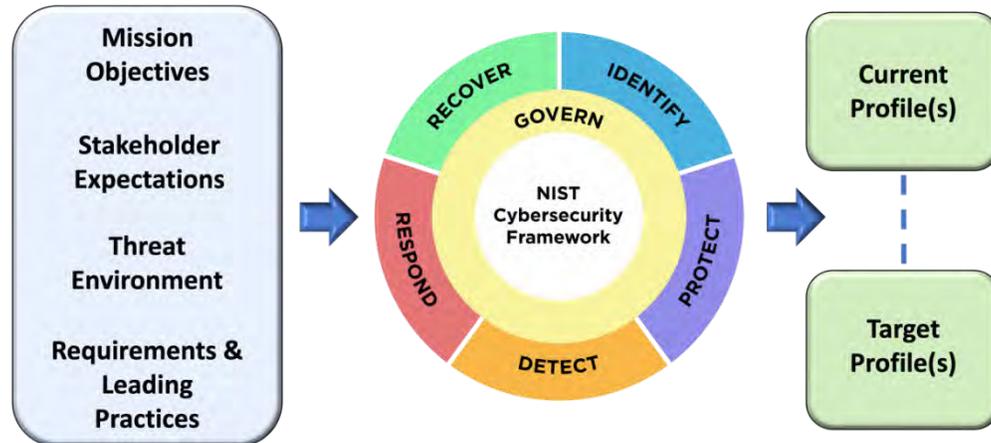
311
312                              **Fig. 3. Cybersecurity Framework Profiles**

313    There are two types of Profiles:

314        • A *Current Profile* covers the Core's outcomes that an organization is currently achieving
315          (or attempting to achieve) and characterizes how or to what extent each outcome is being
316          achieved.

317        • A *Target Profile* covers the desired outcomes that an organization has selected and
318          prioritized from the Core for achieving its cybersecurity risk management objectives. A
319          Target Profile takes into account anticipated changes to the organization's cybersecurity
320          posture, such as new requirements, new technology adoption, and cybersecurity threat
321          intelligence trends.

322    Some organizations prefer to create a Current Profile first — for example, an organization that
323    wants to review its current efforts first and then think about areas for improvement. Others prefer
324    to start with a Target Profile to work toward. For example, an organization that needs to meet a
325    set of new requirements might focus on developing its Target Profile first and in the course of
326    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.

327

### 328    3.1.1. Ways to Use Profiles

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

333    • Compare current cybersecurity practices to sector-specific standards and regulatory
334      requirements

335    • Document the Informative References (e.g., standards, guidelines, and policies) and the
336      practices (e.g., procedures and safeguards) currently in place and planned in the future

337    • Set cybersecurity goals for the organization, identify gaps between current practices and
338      the goals, and plan how to address the gaps in a cost-effective manner

339    • Prioritize cybersecurity outcomes

340    • Assess progress toward achieving the organization's cybersecurity goals

341    • Determine where the organization may have cybersecurity gaps with respect to an
342      emerging threat or a new technology

343    • Communicate about the cybersecurity capabilities an organization provides — for
344      example, to business partners or to prospective customers of the organization's
345      technology products and services

346    • Express the organization's cybersecurity requirements and expectations to suppliers,
347      partners, and other third parties

348    • Integrate cybersecurity and privacy risk management programs by analyzing gaps
349      between NIST Cybersecurity and Privacy Framework Profiles

### 350    3.1.2. Steps for Creating and Using Profiles

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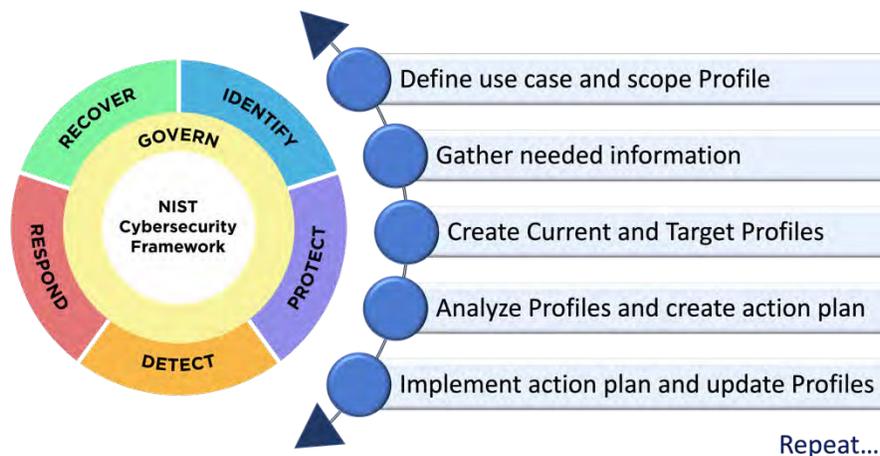


353
354    **Fig. 4. Steps for creating and using Cybersecurity Framework Profiles**

355   1. **Define the use case for the Profiles.** The use case defines the high-level facts and
356      assumptions on which the Profiles will be based, as a way of scoping the Profiles. This
357      can include:

358      • The reason for creating the Profiles

359      • The organization's divisions, information and technology assets, services, and other
360        elements that are in scope for these Profiles

361      • Those who will develop, review, and operationalize the Profiles

362      • The individuals who will set expectations for actions to achieve the cybersecurity
363        outcomes

364   2. **Gather the information needed to prepare the Profiles.** An organization can gather
365      relevant resources prior to preparing the Profiles, such as organizational policies, risk
366      management priorities and resources, cybersecurity requirements and standards followed
367      by the organization, and work roles. Understanding cybersecurity governance — such as
368      identifying the organization's mission, its stakeholders, and their needs and expectations,
369      as outlined in the GOVERN Function — is generally needed for preparing a Target Profile.

370   3. **Create Current and Target Profiles.** Determine what types of supporting information
371      (also known as *elements*) each Profile should include for each of the selected Framework
372      outcomes, and fill in the elements for each selected outcome. Consider the risk
373      implications of the current state to inform target state planning and prioritization.
374      Appendix A provides a notional template for Current and Target Profiles and examples of
375      common elements that organizations can choose to use. Examples of elements in a Profile
376      for each outcome Category or Subcategory include the outcome's priority compared to
377      other outcomes; current status in achieving the outcome; policies, processes, and
378      procedures; practices, including tools and responsibilities; metrics and measurements;
379      informative references; and any other supporting information that an organization
380      considers helpful. Organizations documenting responsibilities may employ the
381      [Workforce Framework for Cybersecurity (NICE Framework)](#), which provides a common
382      lexicon for describing cybersecurity work.

383   4. **Analyze the Profiles and create an action plan.** Identifying and analyzing the
384      differences between the Current and Target Profiles enables an organization to identify
385      gaps and develop a prioritized action plan for addressing those gaps to improve
386      cybersecurity. This plan should consider mission drivers, benefits, risks, and necessary
387      resources (e.g., staffing, funding). Using Profiles in this manner helps an organization
388      make better-informed decisions about how to improve cybersecurity risk management in
389      a cost-effective manner. Appendix A provides a notional action plan template.

390   5. **Implement the action plan and update the Profiles.** The organization follows the
391      action plan to adjust its cybersecurity practices to address gaps and move toward the
392      Target Profile. Improving an organization's cybersecurity program is a continuous effort,
393      and implementing an action plan can take months or years. At frequencies defined by the
394      organization, the Current Profile should be updated to assess progress and the Target
395      Profile should be updated to reflect changes in the organization and its cybersecurity risk.
396      Over time, changes in either or both Profiles will require revising the action plan and

397       repeating these steps. Given the importance of continual improvement, an organization
398       can repeat the steps as often as needed.

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

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

413       • An entire enterprise

414       • Each of an organization's major business units

415       • Business partners or suppliers

416       • Each of an organization's most critical systems

417       • Products or services with cybersecurity requirements

## 3.2. Assessing and Prioritizing Cybersecurity Outcomes With the Framework

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

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

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

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

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

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

### 3.3.   Using Framework Tiers to Characterize Cybersecurity Risk Management Outcomes

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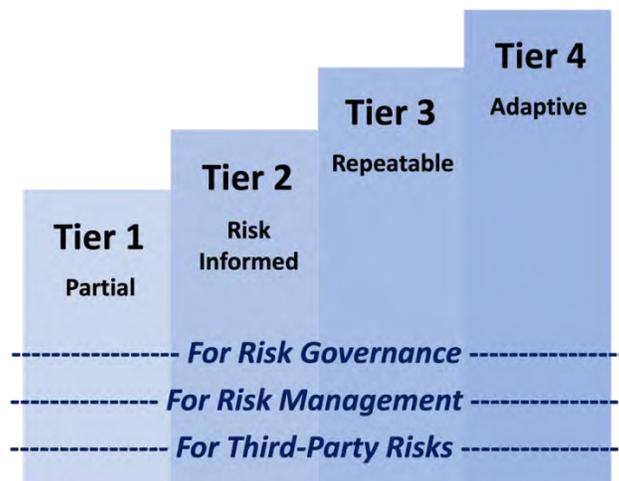


**Fig. 5. Cybersecurity Framework Tiers**

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

458    Tiers should be used to complement an organization's cybersecurity risk management
459    methodology rather than take its place. For example, an organization can use the Tiers to
460    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.

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

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

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

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

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

### 3.4.1.  Improving Communication Across the Organization

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

**National**
Provide Framework and guidance; share threat information; encourage international standards and alignment

**Senior Executive**
Set mission, cybersecurity, and enterprise risk appetite and priorities; oversee cybersecurity program

**Business Process**
Develop cybersecurity program; manage enterprise risk management

**Implementation/Operations**
Implement cybersecurity program

*Shared Organizational Responsibilities*

Stakeholder interests
Cybersecurity risks
Communications
Cybersecurity objectives
Framework Profile(s)
Budgets
Implementation

498
499    **Fig. 6. Using the Cybersecurity Framework to improve communication**

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

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

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

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

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

### 3.4.2. Improving Communication With External Stakeholders

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

536 • Express its cybersecurity risk management requirements to an external service provider
537   (e.g., a service provider with which it is exchanging data) through a Target Profile

538 • Report on the status of cybersecurity requirements (e.g., to a government regulator),
539   which makes it easier to review requirements as part of a broader risk management
540   strategy

541 • Better understand its cybersecurity posture in light of systemic risks

542 • Identify cybersecurity priorities for a sector

543 • Determine the extent to which risk management processes, integration, and information
544   sharing fulfill stakeholders' expectations

545 • Share high-level information on cybersecurity practices with prospective customers,
546   business partners, and others who may need to understand the organization's
547   cybersecurity posture before engaging with the organization

548 • Define shared responsibility models with cloud service providers

### 3.5. Managing Cybersecurity Risk in Supply Chains With the Framework

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

559 Given the complex and interconnected relationships in this ecosystem, supply chain risk
560 management (SCRM) is critical for organizations. Cybersecurity SCRM (C-SCRM) is a
561 systematic process for managing exposure to cybersecurity risk throughout supply chains and
562 developing appropriate response strategies, policies, processes, and procedures. See SP 800-
563 161r1 (Revision 1), *Cybersecurity Supply Chain Risk Management Practices for Systems and*
564 *Organizations*, for in-depth information on C-SCRM.

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

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

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

593     • **Identify**: Identifying, validating, and recording vulnerabilities associated with the
594        supplier's product or service [ID.RA-01]

595     • **Protect:** Authenticating users, services, and hardware [PR.AA-03]; applying appropriate
596        configuration management practices [PR.PS-01]; generating log records and having the
597        logs available for continuous monitoring [PR.PS-04]; and integrating secure software
598        development practices into the supplier's software development life cycles [PR.PS-07]

599     • **Detect**: Monitoring computing hardware and software for potentially adverse events
600        [DE.CM-09]

601     • **Respond**: Executing incident response plans when compromised products or services are
602        involved [RS.MA-01]

603     • **Recover**: Executing the recovery portion of the organization's incident response plan
604        when compromised products or services are involved [RC.RP-01], and restoring
605        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.

606

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

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

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

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

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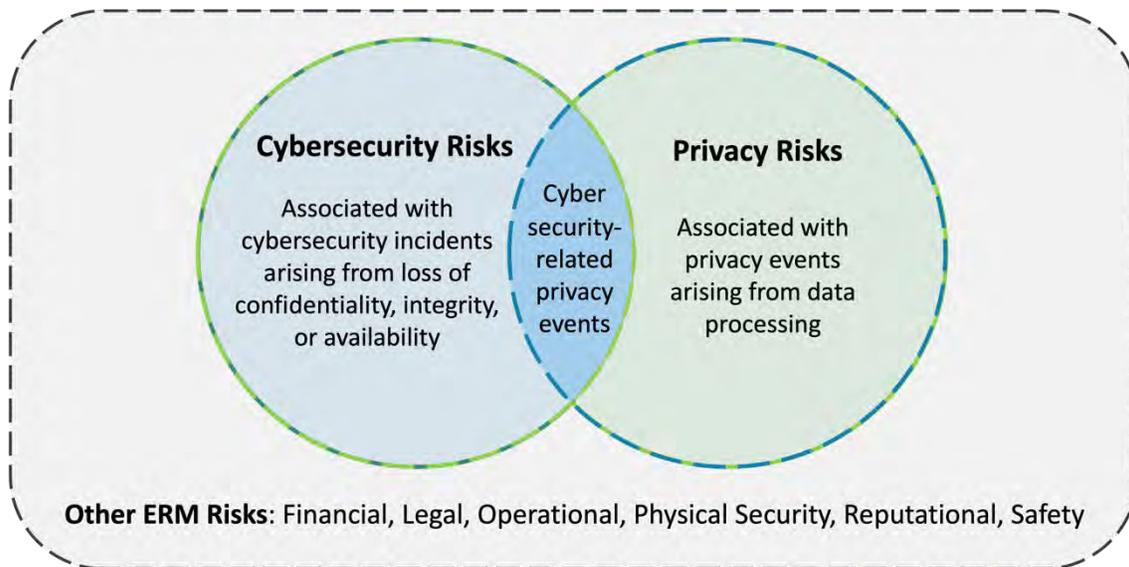
**Fig. 7. Integrating cybersecurity and privacy risks**

## 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 over-collection 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, and loss of trust.

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.

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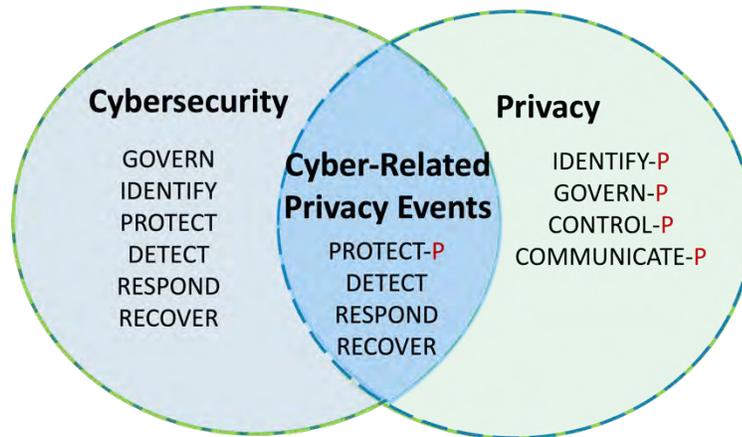


663
664                    **Fig. 8. Cybersecurity Framework and Privacy Framework alignment**

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

667   •   Use both the Cybersecurity and Privacy Frameworks to consider the full spectrum of
668       privacy risks associated with its cybersecurity program, including identity management
669       and access control

670   •   Ensure that individuals with cybersecurity-related privacy responsibilities report to
671       appropriate management and are appropriately trained

672   •   Comply with applicable privacy statutes and regulations

673   •   Identify outcomes and activities in the Privacy Framework Core that can be integrated
674       into cybersecurity workforce awareness and training

675   •   Inform providers of cybersecurity-related products and services about the organization's
676       applicable privacy policies

677   •   Conduct privacy reviews of an organization's asset monitoring and detection of adverse
678       cybersecurity events and incidents, as well as its cybersecurity incident mitigation efforts

679   •   Put processes in place to assess and address whether, when, how, and the extent to which
680       individuals' data is shared outside of the organization as part of cybersecurity
681       information-sharing activities

682   ## 4.2.   Integrating the Cybersecurity Framework With Enterprise Risk Management

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

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

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

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

701    • Ensuring that assets that are important to the enterprise are considered when defining the
702      Framework use case (step 1)

703    • Including ERM-related input (e.g., enterprise risk categories, priorities, integrated risk
704      registers) when gathering information needed to prepare the Profiles (step 2)

705    • Considering tangible and assessable representation of risks (risk scenarios) from
706      throughout the enterprise when evaluating the risk implications of the current state and
707      defining the desired state that will address important risks (step 3)

708    • Ensuring that expectations from those in ERM roles (e.g., enterprise risk steering
709      committee, senior executives, and officers) are included in the analysis and prioritization
710      to create an action plan (step 4)

711    • Communicating results from action plan implementation (step 5) to those in ERM roles
712      to help monitor cybersecurity risk strategy results, adjust that strategy to pursue
713      opportunities, and reduce exposure throughout the enterprise. ERM stakeholders may
714      also recommend adjustments to the desired tier (and associated governance, management,
715      and third-party risk management activities) to improve achievement of enterprise goals.

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

## 5. Next Steps

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

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

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

737        • NIST Artificial Intelligence Risk Management Framework (AI RMF)

738        • SP 800-207, *Zero Trust Architecture*, and the NCCoE's Implementing a Zero Trust
739          Architecture project

740        • NIST Cybersecurity for IoT Program

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

## Appendix A. Templates for Profiles and Action Plans

743

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

### A.1. Notional Organizational Profile Template

747

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

750      • **Selected Framework Outcomes:** The Functions, Categories, or Subcategories of the
751        Framework being included in the Profile. Profiles may be at any outcome level.
752        Organizations may downselect outcomes or add their own Functions, Categories, or
753        Subcategories to address specific needs or unique organizational risks.

754      • **Current Profile:** Elements chosen by the organization to characterize its current
755        cybersecurity risk management posture.

756      • **Target Profile:** Elements chosen by the organization to characterize its cybersecurity
757        risk management goals and its plans for achieving those goals.

758      • **Notes:** A space for additional comments on each selected outcome.

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

761                          **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 Responsi-bilities | Target Selected Informative References | Notes |
|---|---|---|---|---|---|---|---|
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

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

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

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

772  • **Priority**: The relative importance of an outcome compared to other outcomes.
773     Organizations can choose a simple prioritization schema (e.g., Prioritized/Not Prioritized)
774     or a multi-level schema (e.g., High, Moderate, Implement Later) to provide more insights
775     when creating a gap analysis or action plan.

776  • **Policies, Processes, and Procedures**: Information on the organization's policies,
777     processes, and procedures related to a particular outcome. For example, a policy might
778     state that access to resources requires a certain degree of authorization and a supporting
779     procedure might specify the correct access control rules for requesting and approving
780     access to a specific software component.

781  • **Internal Practices**: Information on how the organization implements its policies,
782     processes, and procedures for a particular outcome, as well as any other organizational
783     activities. The Internal Practices element could be divided into more granular elements,
784     such as the hardware and software tools and the methodologies used to perform the
785     practices.

786  • **Roles and Responsibilities**: People, teams, or other organizations who help achieve the
787     outcome or who are responsible for ensuring that the outcome is achieved. This includes
788     shared responsibility models, such as specifying which aspects of an outcome an
789     outsourcer and the organization are each responsible for. This element could also include
790     Work Roles, Tasks, and Knowledge and Skills needed for achieving each outcome, such
791     as from SP 800-181r1, *NIST Workforce Framework for Cybersecurity (NICE*
792     *Framework)*.

793  • **Selected Informative References:** Applicable standards, guidance, requirements,
794     organizational policies, and other references selected by the organization.

795  • **Measurements:** Selected measurements. See Section 3.2 for more information on
796     measuring cybersecurity risk outcomes.

797  • **Artifacts and Evidence:** Information on artifacts that contain evidence of achieving
798     particular outcomes. The Profile could include pointers to files, databases, and other
799     resources that contain the artifacts, or the Profile could characterize the artifacts and
800     provide a point of contact for each one.

## A.2.   Notional Action Plan Template

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

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

810

**Table 2. Notional action plan template**

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

811     **Appendix B.  Framework Tier Descriptions**

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

814                                                                **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.<br><br>Prioritization is ad hoc and not formally based on objectives or threat environment. | There is limited awareness of cybersecurity risks at the organizational level.<br><br>The organization implements cybersecurity risk management on an irregular, case-by-case basis.<br><br>The organization may not have processes that enable cybersecurity information to be shared within the organization. | The organization is generally unaware of the cybersecurity risks of the products and services it provides and uses.<br><br>The organization does not understand its role in the larger ecosystem with respect to either its dependencies or dependents.<br><br>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.<br><br>Prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, 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.<br><br>Consideration of cybersecurity in organizational objectives 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.<br><br>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.<br><br>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. |

| Tier | Cybersecurity Risk Governance | Cybersecurity Risk Management | Third-Party Cybersecurity Risks |
|---|---|---|---|
| Tier 3: Repeatable | The organization's risk management practices are formally approved and expressed as policy.<br><br>Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed.<br><br>Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements, threats, and technological landscape. | There is an organization-wide approach to managing cybersecurity risks.<br><br>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.<br><br>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.<br><br>An organization-wide approach to managing 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 managing 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 the organizational risk tolerances. | 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.<br><br>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). |

| Tier | Cybersecurity Risk Governance | Cybersecurity Risk Management | Third-Party Cybersecurity Risks |
|------|-------------------------------|-------------------------------|---------------------------------|
|      | 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. |  |  |

815 ## Appendix C. Framework Core

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

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

820 **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 |

821 The remaining tables in this appendix show the CSF 2.0 Core Functions, Categories, and
822 Subcategories with one table for each Function. Each table also identifies when a CSF 1.1
823 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, 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, 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, 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, and services that the organization depends on are determined and communicated (formerly ID.BE-01, ID.BE-04) |

| Category | Subcategory |
|---|---|
| **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 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 (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 |

| Category | Subcategory |
|---|---|
| | **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, and enforced (formerly ID.AM-06, ID.GV-02, DE.DP-01) |
| | **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, and enforced (formerly ID.GV-01) | |

| Category | Subcategory |
|---|---|
| | **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, and adjust 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 |

| Category | Subcategory |
|---|---|
|  | **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 |

| Category | Subcategory |
|---|---|
| | **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) |

| Category | Subcategory |
|---|---|
|  | **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.IM-02) |
|  | **ID.IM-04:** Cybersecurity plans that affect operations are communicated, maintained, and improved (formerly PR.IP-09) |

**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)* |

| Category | Subcategory |
|---|---|
| | *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)* |

| Category | Subcategory |
|---|---|
| | 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) |

| Category | Subcategory |
|---|---|
| | *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, and 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 maintained, replaced, and removed commensurate with risk (formerly PR.IP-12, PR.MA-02) |
| | **PR.PS-03:** Hardware is 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 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) |

**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, 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) |

| Category | Subcategory |
|---|---|
| | **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 |

| Category | Subcategory |
|---|---|
| **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 |

| Category | Subcategory |
|---|---|
| | *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 post-incident 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 |

| Category | Subcategory |
|---|---|
| | **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)* |