Preface

The Cybersecurity Framework (CSF) 2.0 is designed to help organizations of all sizes and sectors — including industry, government, academia, and nonprofit — to manage and reduce their cybersecurity risks. It is useful regardless of the maturity level and technical sophistication of an organization’s cybersecurity programs. Nevertheless, the CSF does not embrace a one-size-fits-all approach. Each organization has both common and unique risks, as well as varying risk appetites and tolerances, specific missions, and objectives to achieve those missions. By necessity, the way organizations implement the CSF will vary.

Ideally, the CSF will be used to address cybersecurity risks alongside other risks of the enterprise, including those that are financial, privacy, supply chain, reputational, technological, or physical in nature.

The CSF *describes* desired outcomes that are intended to be understood by a broad audience, including executives, managers, and practitioners, regardless of their cybersecurity expertise. Because these outcomes are sector-, country-, and technology-neutral, they provide an organization with the flexibility needed to address their unique risks, technologies, and mission considerations. Outcomes are mapped directly to a list of potential security controls for immediate consideration to mitigate cybersecurity risks.

Although not prescriptive, the CSF assists its users in learning about and selecting specific outcomes. Suggestions for how specific outcomes may be achieved are provided in an expanding suite of online resources that complement the CSF, including a series of Quick Start Guides (QSGs). Also, various tools offer downloadable formats to help organizations that choose to automate some of their processes. The QSGs suggest initial ways to use the CSF and invite the reader to explore the CSF and related resources in greater depth. Available through the NIST CSF website, the CSF and these supplementary resources from NIST and others should be viewed as a “CSF portfolio” to help manage and reduce risks. Regardless of how it is applied, the CSF prompts its users to consider their cybersecurity posture in context and then adapt the CSF to their specific needs.

Building on previous versions, CSF 2.0 contains new features that highlight the importance of *governance* and *supply chains*. Special attention is paid to the QSGs to ensure that the CSF is relevant and readily accessible by smaller organizations as well as their larger counterparts. NIST now provides *Implementation Examples* and *Informative References*, which are available online and updated regularly. Creating current and target state *Organizational Profiles* helps organizations to compare where they are versus where they want or need to be and allows them to implement and assess security controls more quickly.

Cybersecurity risks are expanding constantly, and managing those risks must be a continuous process. This is true regardless of whether an organization is just beginning to confront its cybersecurity challenges or whether it has been active for many years with a sophisticated, well-resourced cybersecurity team. The CSF is designed to be valuable for any type of organization and is expected to provide appropriate guidance over a long time.

1. Cybersecurity Framework (CSF) Overview

This document is version 2.0 of the NIST Cybersecurity Framework (*Framework* or *CSF*). It includes the following components:

- ***CSF Core***, the nucleus of the CSF, which is a taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks. The CSF Core components are a hierarchy of Functions, Categories, and Subcategories that detail each outcome. These outcomes can be understood by a broad audience, including executives, managers, and practitioners, regardless of their cybersecurity expertise. Because the outcomes are sector-, country-, and technology-neutral, they provide an organization with the flexibility needed to address its unique risks, technologies, and mission considerations.
- ***CSF Organizational Profiles***, which are a mechanism for describing an organization's current and/or target cybersecurity posture in terms of the CSF Core's outcomes.
- ***CSF Tiers***, which can be applied to CSF Organizational Profiles to characterize the rigor of an organization's cybersecurity risk governance and management practices. Tiers can also provide context for how an organization views cybersecurity risks and the processes in place to manage those risks.

This document describes *what* desirable outcomes an organization can aspire to achieve. It does not *prescribe* outcomes nor *how* they may be achieved. Descriptions of *how* an organization can achieve those outcomes are provided in a suite of online resources that complement the CSF and are available through the NIST CSF website. These resources offer additional guidance on practices and controls that could be used to achieve outcomes and are intended to help an organization understand, adopt, and use the CSF. They include:

- *Informative References* that point to sources of guidance on each outcome from existing global standards, guidelines, frameworks, regulations, policies, etc.
- *Implementation Examples* that illustrate potential ways to achieve each outcome
- *Quick-Start Guides* that give actionable guidance on using the CSF and its online resources, including transitioning from previous CSF versions to version 2.0
- *Community Profiles* and *Organizational Profile Templates* that help an organization put the CSF into practice and set priorities for managing cybersecurity risks

An organization can use the CSF Core, Profiles, and Tiers with the supplementary resources to understand, assess, prioritize, and communicate cybersecurity risks.

- **Understand and Assess:** Describe the current or target cybersecurity posture of part or all of an organization, determine gaps, and assess progress toward addressing those gaps.

- **Prioritize:** Identify, organize, and prioritize actions for managing cybersecurity risks that align with the organization's mission, legal and regulatory requirements, and risk management and governance expectations.
- **Communicate:** Provide a common language for communicating inside and outside the organization about cybersecurity risks, capabilities, needs, and expectations.

The CSF is designed to be used by organizations of all sizes and sectors, including industry, government, academia, and nonprofit organizations, regardless of the maturity level of their cybersecurity programs. The CSF is a foundational resource that may be adopted voluntarily and through governmental policies and mandates. The CSF's taxonomy and referenced standards, guidelines, and practices are not country-specific, and previous versions of the CSF have been leveraged successfully by many governments and other organizations both inside and outside of the United States.

The CSF should be used in conjunction with other resources (e.g., frameworks, standards, guidelines, leading practices) to better manage cybersecurity risks and inform the overall management of information and communications technology (ICT) risks at an enterprise level. The CSF is a flexible framework that is intended to be tailored for use by all organizations regardless of size. Organizations will continue to have unique risks — including different threats and vulnerabilities — and risk tolerances, as well as unique mission objectives and requirements. Thus, organizations' approaches to managing risks and their implementations of the CSF will vary.

The remainder of this document is structured as follows:

- Section 2 explains the basics of the CSF Core: Functions, Categories, and Subcategories.
- Section 3 defines the concepts of CSF Profiles and Tiers.
- Section 4 provides an overview of selected components of the CSF's suite of online resources: Informative References, Implementation Examples, and Quick Start Guides.
- Section 5 discusses how an organization can integrate the CSF with other risk management programs.
- Appendix A is the CSF Core.
- Appendix B contains a notional illustration of the CSF Tiers.
- Appendix C is a glossary of CSF terminology.

2. Introduction to the CSF Core

Appendix A is the CSF Core — a set of cybersecurity outcomes arranged by Function, then Category, and finally Subcategory, as depicted in Fig. 1. These outcomes are not a checklist of actions to perform; specific actions taken to achieve an outcome will vary by organization and use case, as will the individual responsible for those actions. Additionally, the order and size of Functions, Categories, and Subcategories in the Core does not imply the sequence or importance of achieving them. The structure of the Core is intended to resonate most with those charged with operationalizing risk management within an organization.

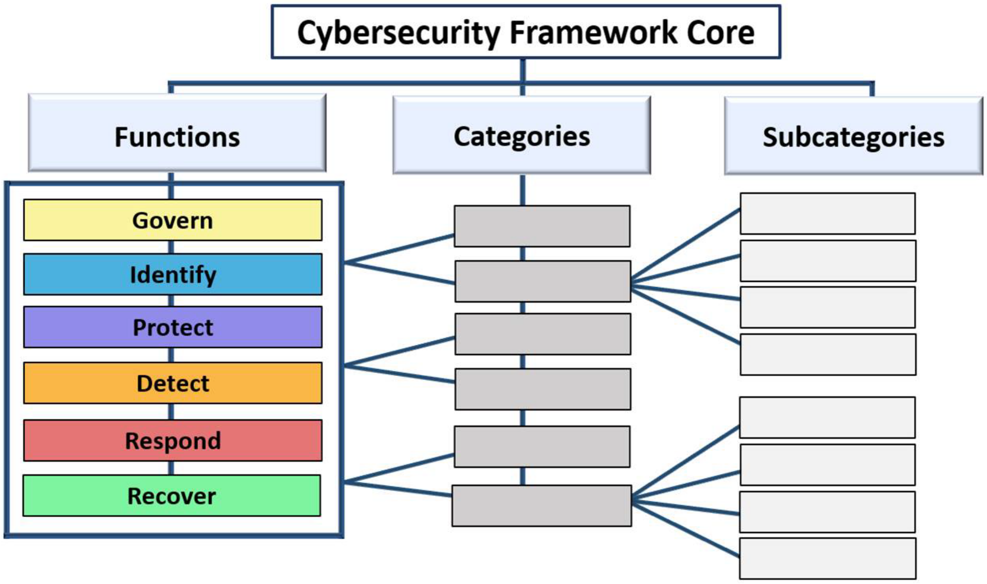

Fig. 1. CSF Core structure

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

- **GOVERN (GV)** — *The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.* The GOVERN Function provides outcomes to inform what an organization may do to 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 (ERM) strategy. GOVERN addresses an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and the oversight of cybersecurity strategy.

- **IDENTIFY (ID)** — *The organization's current cybersecurity risks are understood.* Understanding the organization's assets (e.g., data, hardware, software, systems, facilities, services, people), suppliers, and related cybersecurity risks enables an organization to prioritize its efforts consistent with its risk management strategy and the mission needs identified under GOVERN. This Function also includes the identification of improvement opportunities for the organization's policies, plans, processes, procedures, and practices that support cybersecurity risk management to inform efforts under all six Functions.

- **Protect (PR)** — *Safeguards to manage the organization's cybersecurity risks are used.* Once assets and risks are identified and prioritized, Protect supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events, as well as to increase the likelihood and impact of taking advantage of opportunities. Outcomes covered by this Function include identity management, authentication, and access control; awareness and training; data security; platform security (i.e., securing the hardware, software, and services of physical and virtual platforms); and the resilience of technology infrastructure.
- **Detect (DE)** — *Possible cybersecurity attacks and compromises are found and analyzed.* Detect enables the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring. This Function supports successful incident response and recovery activities.
- **Respond (RS)** — *Actions regarding a detected cybersecurity incident are taken.* Respond supports the ability to contain the effects of cybersecurity incidents. Outcomes within this Function cover incident management, analysis, mitigation, reporting, and communication.
- **Recover (RC)** — *Assets and operations affected by a cybersecurity incident are restored.* Recover supports the timely restoration of normal operations to reduce the effects of cybersecurity incidents and enable appropriate communication during recovery efforts.

While many cybersecurity risk management activities focus on preventing negative events from occurring, they may also support taking advantage of positive opportunities. Actions to reduce cybersecurity risk might benefit an organization in other ways, like increasing revenue (e.g., first 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 risks).

Figure 2 shows the CSF Functions as a wheel because all of the Functions relate to one another. For example, an organization will categorize assets under Identify and take steps to secure those assets under Protect. Investments in planning and testing in the Govern and Identify Functions will support timely detection of unexpected events in the Detect Function, as well as enabling incident response and recovery actions for cybersecurity incidents in the Respond and Recover Functions. Govern is in the center of the wheel because it informs how an organization will implement the other five Functions.

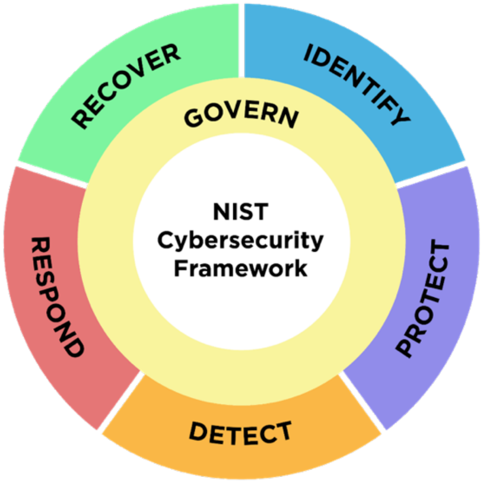

Fig. 2. CSF Functions

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

Each Function is named after a verb that summarizes its contents. Each Function is divided into *Categories*, which are related cybersecurity outcomes that collectively comprise the Function. *Subcategories* further divide each Category into more specific outcomes of technical and management activities. The Subcategories are not exhaustive, but they describe detailed outcomes that support each Category.

The Functions, Categories, and Subcategories apply to all ICT used by an organization, including information technology (IT), the Internet of Things (IoT), and operational technology (OT). They also apply to all types of technology environments, including cloud, mobile, and artificial intelligence systems. The CSF Core is forward-looking and intended to apply to future changes in technologies and environments.