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.

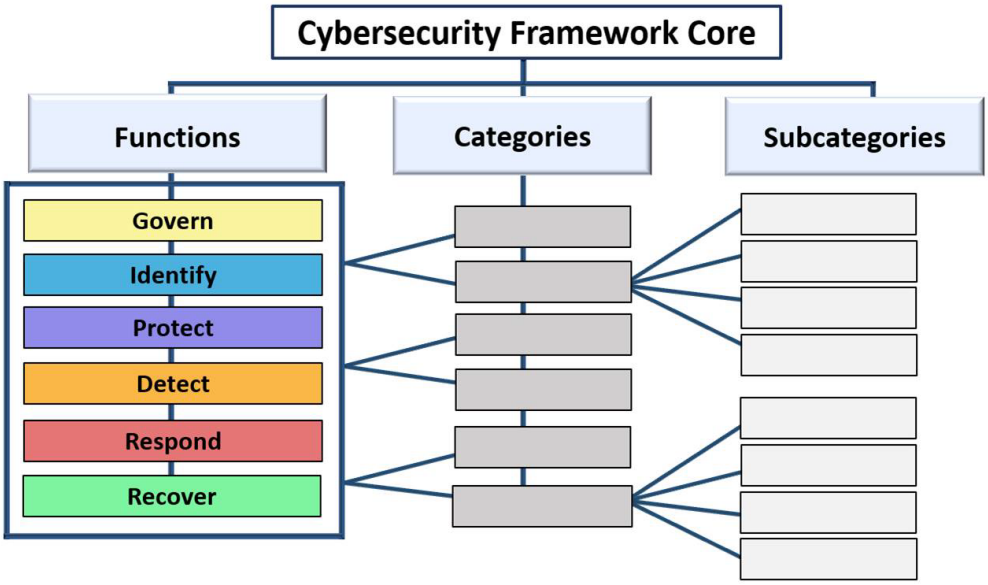

Fig. 1. CSF Core structure

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.

3. Introduction to CSF Profiles and Tiers

This section defines the concepts of CSF Profiles and Tiers.

3.1. CSF Profiles

A *CSF Organizational Profile* describes an organization's current and/or target cybersecurity posture in terms of the Core's outcomes. Organizational Profiles are used to understand, tailor, assess, prioritize, and communicate the Core's outcomes by considering an organization's mission objectives, stakeholder expectations, threat landscape, and requirements. An organization can then prioritize its actions to achieve specific outcomes and communicate that information to stakeholders.

Every Organizational Profile includes one or both of the following:

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

> A *Community Profile* is a baseline of CSF outcomes that is created and published to address shared interests and goals among a number of organizations. A Community Profile is typically developed for a particular sector, subsector, technology, threat type, or other use case. An organization can use a Community Profile as the basis for its own Target Profile. Examples of Community Profiles can be found on the NIST CSF website.

The steps shown in Fig. 3 and summarized below illustrate one way that an organization could use an Organizational Profile to help inform continuous improvement of its cybersecurity.

Fig. 3. Steps for creating and using a CSF Organizational Profile

1. **Scope the Organizational Profile.** Document the high-level facts and assumptions on which the Profile will be based to define its scope. An organization can have as many Organizational Profiles as desired, each with a different scope. For example, a Profile could address an entire organization or be scoped to an organization's financial systems or to countering ransomware threats and handling ransomware incidents involving those financial systems.
2. **Gather the information needed to prepare the Organizational Profile.** Examples of information may include organizational policies, risk management priorities and resources, enterprise risk profiles, business impact analysis (BIA) registers, cybersecurity requirements and standards followed by the organization, practices and tools (e.g., procedures and safeguards), and work roles.
3. **Create the Organizational Profile.** Determine what types of information the Profile should include for the selected CSF outcomes, and document the needed information. Consider the risk implications of the Current Profile to inform Target Profile planning and prioritization. Also, consider using a Community Profile as the basis for the Target Profile.
4. **Analyze the gaps between the Current and Target Profiles, and create an action plan.** Conduct a gap analysis to identify and analyze the differences between the Current and Target Profiles, and develop a prioritized action plan (e.g., risk register, risk detail report, Plan of Action and Milestones [POA&M]) to address those gaps.
5. **Implement the action plan, and update the Organizational Profile.** Follow the action plan to address the gaps and move the organization toward the Target Profile. An action plan may have an overall deadline or be ongoing.

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

There are additional uses for Organizational Profiles. For example, a Current Profile can be used to document and communicate the organization's cybersecurity capabilities and known opportunities for improvement with external stakeholders, such as business partners or prospective customers. Also, a Target Profile can help express the organization's cybersecurity risk management requirements and expectations to suppliers, partners, and other third parties as a target for those parties to achieve.

3.2. CSF Tiers

An organization can choose to use the Tiers to inform its Current and Target Profiles. *Tiers* characterize the rigor of an organization's cybersecurity risk governance and management practices, and they provide context for how an organization views cybersecurity risks and the processes in place to manage those risks. The Tiers, as shown in Fig. 4 and notionally illustrated in Appendix B, reflect an organization's practices for managing cybersecurity risk as Partial (Tier 1), Risk Informed (Tier 2), Repeatable (Tier 3), and Adaptive (Tier 4). The Tiers describe a progression from informal, ad hoc responses to approaches that are agile, risk-informed, and

continuously improving. Selecting Tiers helps set the overall tone for how an organization will manage its cybersecurity risks.

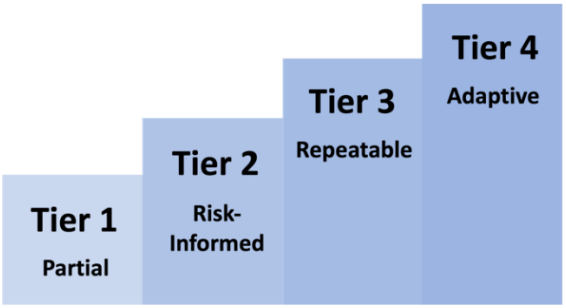

Fig. 4. CSF Tiers for cybersecurity risk governance and management

Tiers should complement an organization's cybersecurity risk management methodology rather than replace it. For example, an organization can use the Tiers to communicate internally as a benchmark for an organization-wide[1] approach to managing cybersecurity risks. Progression to higher Tiers is encouraged when risks or mandates are greater or when a cost-benefit analysis indicates a feasible and cost-effective reduction of negative cybersecurity risks.

The NIST CSF website provides additional information on using Profiles and Tiers. It includes pointers to NIST-hosted Organizational Profile templates and a repository of Community Profiles in a variety of machine-readable and human-usable formats.

[1] For the purposes of this document, the terms "organization-wide" and "enterprise" have the same meaning.

4. Introduction to Online Resources That Supplement the CSF

NIST and other organizations have produced a suite of online resources that help organizations understand, adopt, and use the CSF. Since they are hosted online, these additional resources can be updated more frequently than this document, which is updated infrequently to provide stability to its users, and be available in machine-readable formats. This section provides an overview of three types of online resources: Informative References, Implementation Examples, and Quick Start Guides.

Informative References are mappings that indicate relationships between the Core and various standards, guidelines, regulations, and other content. Informative References help inform how an organization may achieve the Core's outcomes. Informative References can be sector- or technology-specific. They may be produced by NIST or another organization. Some Informative References are narrower in scope than a Subcategory. For example, a particular control from SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, may be one of many references needed to achieve the outcome described in one Subcategory. Other Informative References may be higher-level, such as a requirement from a policy that partially addresses numerous Subcategories. When using the CSF, an organization can identify the most relevant Informative References.

Implementation Examples provide notional examples of concise, action-oriented steps to help achieve the outcomes of the Subcategories. Verbs used to express Examples include share, document, develop, perform, monitor, analyze, assess, and exercise. The Examples are not a comprehensive list of all actions that could be taken by an organization to achieve an outcome, nor do they represent a baseline of required actions to address cybersecurity risks.

Quick-Start Guides (QSGs) are brief documents on specific CSF-related topics and are often tailored to specific audiences. QSGs can help an organization implement the CSF because they distill specific portions of the CSF into actionable "first steps" that an organization can consider on the path to improving their cybersecurity posture and management of associated risks. The guides are revised in their own time frames, and new guides are added as needed.

Suggestions for new Informative References for CSF 2.0 can always be shared with NIST at olir@nist.gov. Suggestions for other resources to reference on the NIST CSF website, including additional QSG topics, should be directed to cyberframework@nist.gov.

5. Improving Cybersecurity Risk Communication and Integration

The CSF's use will vary based on an organization's unique mission and risks. With an understanding of stakeholder expectations and risk appetite and tolerance (as outlined in GOVERN), an organization can prioritize cybersecurity activities to make informed decisions about cybersecurity expenditures and actions. An organization may choose to handle risk in one or more ways — including mitigating, transferring, avoiding, or accepting negative risks and realizing, sharing, enhancing, or accepting positive risks — depending on the potential impacts and likelihoods. Importantly, an organization can use the CSF both internally to manage its cybersecurity capabilities and externally to oversee or communicate with third parties.

Regardless of the CSF's utilization, an organization may benefit from using the CSF as guidance to help it understand, assess, prioritize, and communicate cybersecurity risks and the actions that will manage those risks. The selected outcomes can be used to focus on and implement strategic decisions to improve cybersecurity postures and maintain continuity of mission-essential functions while taking priorities and available resources into account.

5.1. Improving Risk Management Communication

The CSF provides a basis for improved communication regarding cybersecurity expectations, planning, and resources. The CSF fosters bidirectional information flow (as shown in the top half of Fig. 5) between executives who focus on the organization's priorities and strategic direction and managers who manage specific cybersecurity risks that could affect the achievement of those priorities. The CSF also supports a similar flow (as shown in the bottom half of Fig. 5) between managers and the practitioners who implement and operate the technologies. The left side of the figure indicates the importance of practitioners sharing their updates, insights, and concerns with managers and executives.

Fig. 5. Using the CSF to improve risk management communication

Preparing to create and use Organizational Profiles involves gathering information about organizational priorities, resources, and risk direction from executives. Managers then collaborate with practitioners to communicate business needs and create risk-informed Organizational Profiles. Actions to close any gaps identified between the Current and Target Profiles will be implemented by managers and practitioners and will provide key inputs into system-level plans. As the target state is achieved throughout the organization — including through controls and monitoring applied at the system level — the updated results can be shared through risk registers and progress reports. As part of ongoing assessment, managers gain insights to make adjustments that further reduce potential harms and increase potential benefits.

The GOVERN Function supports organizational risk communication with **executives**. Executives' discussions involve strategy, particularly how cybersecurity-related uncertainties might affect the achievement of organizational objectives. These governance discussions support dialogue and agreement about risk management strategies (including cybersecurity supply chain risk); roles, responsibilities, and authorities; policies; and oversight. As executives establish cybersecurity priorities and objectives based on those needs, they communicate expectations about risk appetite, accountability, and resources. Executives are also responsible for integrating cybersecurity risk management with ERM programs and lower-level risk management programs (see Sec. 5.2). The communications reflected in the top half of Fig. 5 can include considerations for ERM and the lower-level programs and, thus, inform managers and practitioners.

The overall cybersecurity objectives set by executives are informed by and cascade to **managers**. In a commercial entity, these may apply to a line-of-business or operating division. For government entities, these may be division- or branch-level considerations. When implementing the CSF, managers will focus on how to achieve risk targets through common services, controls, and collaboration, as expressed in the Target Profile and improved through the actions being tracked in the action plan (e.g., risk register, risk detail report, POA&M).

Practitioners focus on implementing the target state and measuring changes in operational risk to help plan, carry out, and monitor specific cybersecurity activities. As controls are implemented to manage risk at an acceptable level, practitioners provide managers and executives with the information (e.g., key performance indicators, key risk indicators) they need to understand the organization's cybersecurity posture, make informed decisions, and maintain or adjust the risk strategy accordingly. Executives can also combine this cybersecurity risk data with information about other types of risk from across the organization. Updates to expectations and priorities are included in updated Organizational Profiles as the cycle repeats.

5.2. Improving Integration with Other Risk Management Programs

Every organization faces numerous types of ICT risk (e.g., privacy, supply chain, artificial intelligence) and may use frameworks and management tools that are specific to each risk. Some organizations integrate ICT and all other risk management efforts at a high level by using ERM, while others keep the efforts separate to ensure adequate attention on each. Small

organizations by their nature may monitor risk at the enterprise level, while larger companies may maintain separate risk management efforts integrated into the ERM.

Organizations can employ an ERM approach to balance a *portfolio* of risk considerations, including cybersecurity, and make informed decisions. Executives receive significant input about current and planned risk activities as they integrate governance and risk strategies with results from previous uses of the CSF. The CSF helps organizations to translate their terminology for cybersecurity and cybersecurity risk management into general risk management language that executives will understand.

NIST resources that describe the mutual relationship between cybersecurity risk management and ERM include:

- *NIST Cybersecurity Framework 2.0 – Enterprise Risk Management Quick-Start Guide*
- NIST Interagency Report (IR) 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*
- IR 8286A, *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management*
- IR 8286B, *Prioritizing Cybersecurity Risk for Enterprise Risk Management*
- IR 8286C, *Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight*
- IR 8286D, *Using Business Impact Analysis to Inform Risk Prioritization and Response*
- SP 800-221, *Enterprise Impact of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio*
- SP 800-221A, *Information and Communications Technology (ICT) Risk Outcomes: Integrating ICT Risk Management Programs with the Enterprise Risk Portfolio*

An organization may also find the CSF beneficial for integrating cybersecurity risk management with individual ICT risk management programs, such as:

- **Cybersecurity risk management and assessment:** The CSF can be integrated with established cybersecurity risk management and assessment programs, such as SP 800-37, *Risk Management Framework for Information Systems and Organizations*, and SP 800-30, *Guide for Conducting Risk Assessments* from the NIST Risk Management Framework (RMF). For an organization using the NIST RMF and its suite of publications, the CSF can be used to complement the RMF's approach to selecting and prioritizing controls from SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*.
- **Privacy risks:** While cybersecurity and privacy are independent disciplines, their objectives overlap in certain circumstances, as illustrated in Fig. 6.

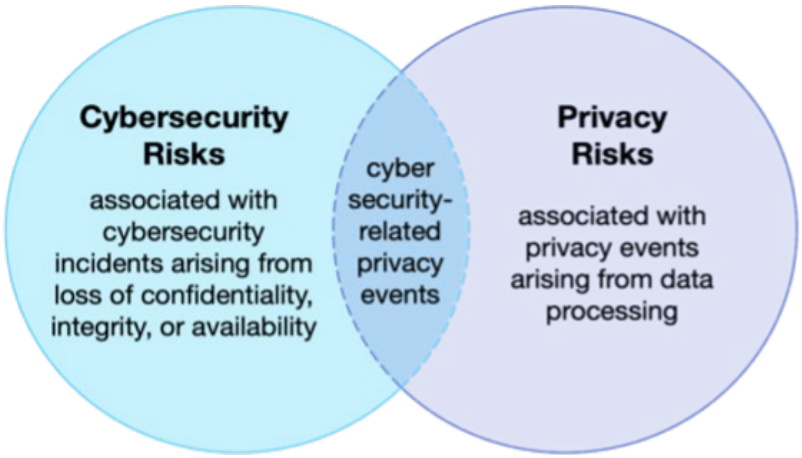

Fig. 6. Cybersecurity and privacy risk relationship

Cybersecurity risk management is essential for addressing privacy risks related to the loss of the confidentiality, integrity, and availability of individuals' data. For example, data breaches could lead to identity theft. However, privacy risks can also arise by means that are unrelated to cybersecurity incidents.

An organization processes data to achieve mission or business purposes, which can sometimes give rise to *privacy events* whereby individuals may experience problems as a result of the data processing. These problems can be expressed in various ways, but NIST describes them as ranging from dignity-type effects (e.g., embarrassment or stigma) to more tangible harms (e.g., discrimination, economic loss, or physical harm). The NIST Privacy Framework and Cybersecurity Framework can be used together to address the different aspects of cybersecurity and privacy risks. Additionally, NIST's Privacy Risk Assessment Methodology (PRAM) has a catalog of example problems for use in privacy risk assessments.

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

  Given the complex and interconnected relationships in this ecosystem, supply chain risk management (SCRM) is critical for organizations. Cybersecurity SCRM (C-SCRM) is a systematic process for managing exposure to cybersecurity risk throughout supply chains and developing appropriate response strategies, policies, processes, and procedures. The Subcategories within the CSF C-SCRM Category [GV.SC] provide a connection between outcomes that focus purely on cybersecurity and those that focus

on C-SCRM. SP 800-161r1 (Revision 1), *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, provides in-depth information on C-SCRM.

- **Risks from emerging technologies:** As new technologies and new applications of technology become available, new risks become clear. A contemporary example is artificial intelligence (AI), which has cybersecurity and privacy risks, as well as many other types of risk. The NIST Artificial Intelligence Risk Management Framework (AI RMF) was developed to help address these risks. Treating AI risks alongside other enterprise risks (e.g., financial, cybersecurity, reputational, and privacy) will yield a more integrated outcome and organizational efficiencies. Cybersecurity and privacy risk management considerations and approaches are applicable to the design, development, deployment, evaluation, and use of AI systems. The AI RMF Core uses Functions, Categories, and Subcategories to describe AI outcomes and help manage risks related to AI.