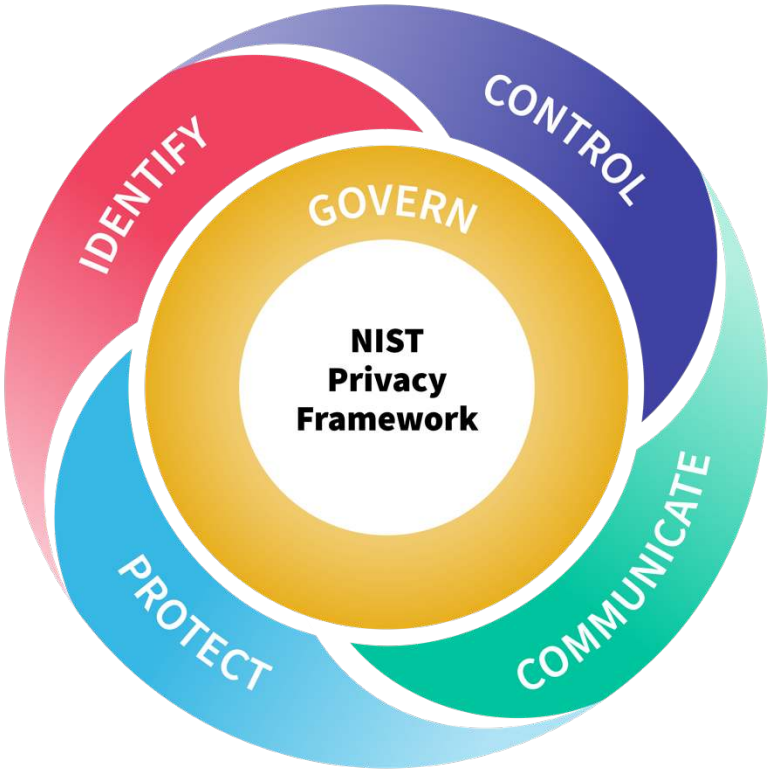
# NIST Cybersecurity White Paper
# CSWP 40 ipd (Initial Public Draft)

# NIST Privacy Framework 1.1

Initial Public Draft




National Institute of Standards and Technology

This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.40.ipd

April 14, 2025

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

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.



**Publication History**
Approved by the NIST Editorial Review Board on YYYY-MM-DD [Will be added to final publication.]

**How to Cite this NIST Technical Series Publication:**
National Institute of Standards and Technology (2025) NIST Privacy Framework 1.1. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 40 ipd. https://doi.org/10.6028/NIST.CSWP.40.ipd

**Author ORCID iDs**
Meghan Anderson: 0009-0004-2875-5672
Dylan Gilbert: 0009-0003-6061-3757
Nakia Grayson: 0000-0003-1062-4338

**Public Comment Period**
April 14, 2025 - June 13, 2025

**Submit Comments**
privacyframework@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

**Additional Information**
Additional information about this publication is available at https://csrc.nist.gov/publications/cswp, including related content, potential updates, and document history.

## Abstract

The NIST Privacy Framework 1.1 is a voluntary tool developed in collaboration with stakeholders intended to help organizations identify and manage privacy risk to build innovative products and services while protecting individuals' privacy. It provides high-level privacy risk management outcomes that can be used by any organization to better understand, assess, prioritize, and communicate its privacy activities. This document introduces the Privacy Framework and privacy risk management practices, highlights the Framework's basic elements, and offers examples of how it can be used.

## Keywords

framework; privacy; privacy framework; privacy risk; privacy risk management; profiles; risk management; tiers.

## Note to Reviewers

This NIST Privacy Framework 1.1 Initial Public Draft (IPD) has been developed in response to stakeholder desire for a Privacy Framework update that:

- Addresses current privacy risk management needs
- Realigns with the NIST Cybersecurity Framework (CSF) 2.0
- Enhances usability

NIST seeks stakeholder feedback on whether this IPD meets those goals. NIST also welcomes feedback on all aspects of the IPD including, but not limited to, content, structure and format, grammar and syntax, and usability. Please submit clear and actionable suggestions for improvements to this document, including rationale for each proposed change. Commentators are strongly encouraged to use the comment template available for download at the NIST Privacy Framework website.

In addition to general feedback on the PF 1.1 IPD, NIST is interested in answers to the following questions:

- **Implementation Examples:** Should NIST include Privacy Framework 1.1 Implementation Examples as supplemental material to the PF 1.1 Final Draft?
    - If so, would a mapping of Task Statements from the NIST Privacy Workforce Taxonomy to the Privacy Framework 1.1 Core be a useful approach to creating Implementation Examples? Why or why not?
- **Gaps in Subcategory Unique Identifiers:** Many Privacy Framework 1.1 IPD Subcategories are moved to other locations in the Core. This leads to gaps in the Subcategory Unique Identifiers (e.g., ID.RA-P2 has been withdrawn, creating a gap between ID.RA-P1 and ID.RA-P3).
    - Should NIST re-number Unique Identifiers in the Privacy Framework 1.1. Final Draft to avoid gaps in numbering?
    - If the answer to the above question is, no, why should NIST retain gaps in Subcategory Unique Identifiers?
- **Streamlining the Privacy Framework 1.1 PDF:** The Privacy Framework 1.1 IPD has replaced Section 3 with a high-level summary of ways to use the Framework. The remaining material has been moved to the Privacy Framework website, where it is structured for interactive engagement.
    - Should NIST further streamline the Privacy Framework 1.1 PDF by removing content from the PDF (e.g., Appendices) and relocating it?
        - If so, what content should be relocated?
        - What format or type of materials would best convey the relocated content (e.g., Quick Start Guide, interactive online resources, etc.)?

## Table of Contents



## List of Tables



## List of Figures

## Acknowledgments

This publication is the result of a collaborative effort between NIST and organizational and individual stakeholders in the public and private sectors, academia, and civil society. In developing Privacy Framework 1.1, NIST has relied upon a public workshop, public comments, and other stakeholder engagement.[1] NIST acknowledges and thanks all who have contributed to this publication.

[1] More information on Privacy Framework 1.1 development can be found at https://www.nist.gov/privacy-framework/new-projects/privacy-framework-version-11.

## Executive Summary

For more than two decades, the Internet and associated information technologies have driven unprecedented innovation, economic value, and improvement in social services. Many of these benefits are fueled by data about individuals that flow through a complex ecosystem. As a result, individuals may not realize the potential consequences for their privacy as they interact with systems, products, and services. At the same time, organizations may not realize the full extent of these consequences for individuals, for society, or for their enterprises, which can affect their brands, their finances, and their future prospects for growth.

Following a transparent, consensus-based process including both private and public stakeholders, the National Institute of Standards and Technology (NIST) has updated the Privacy Framework to Version 1.1 (Privacy Framework 1.1), to meet stakeholder privacy risk management needs, maintain alignment with the NIST Cybersecurity Framework 2.0 (Cybersecurity Framework or CSF 2.0), and provide information on artificial intelligence (AI) and privacy risk management. Privacy Framework 1.1 updates include:

- Targeted revisions and restructuring of the Core
- A new Section (1.2.2) on AI and privacy risk management
- Relocation of Section 3 guidelines from front matter to the NIST Privacy Framework website[2]

The Privacy Framework can support organizations in:

- Building customers' trust by supporting ethical decision-making in product and service design or deployment that optimizes beneficial uses of data while minimizing adverse consequences for individuals' privacy and society as a whole;[3]
- Fulfilling current compliance obligations, as well as future-proofing products and services to meet these obligations in a changing technological and policy environment; and
- Facilitating communication about privacy practices with individuals, business partners, assessors, and regulators.

Deriving benefits from data while simultaneously managing risks to individuals' privacy is not well-suited to one-size-fits-all solutions. Like building a house, where homeowners make layout and design choices while relying on a well-engineered foundation, privacy protection should allow for individual choices, as long as effective privacy risk mitigations are already engineered into products and services. The Privacy Framework—through a risk- and outcome-based approach—is flexible enough to address diverse privacy needs, enable more innovative and

[2] For more information on using the Privacy Framework 1.1, visit https://www.nist.gov/privacy-framework/using-privacy-framework-11.
[3] There is no objective standard for ethical decision-making; it is grounded in the norms, values, and legal expectations in a given society.

effective solutions that can lead to better outcomes for individuals and organizations, and stay current with technology trends.

Privacy Framework 1.1 follows the structure of CSF 2.0 [1] to facilitate the use of both frameworks together. Like the Cybersecurity Framework, the Privacy Framework is composed of three components: Core, Organizational Profiles, and Tiers. Each component reinforces privacy risk management through the connection between business and mission drivers, organizational roles and responsibilities, and privacy protection activities.

- The Core enables a dialogue—from the executive level to the implementation/operations level—about important privacy protection activities and desired outcomes.
- Organizational Profiles enable the prioritization of the outcomes and activities that best meet organizational privacy values, mission or business needs, and risks.
- Tiers support decision-making and communication about the sufficiency of organizational processes and resources to manage privacy risk.

In summary, the Privacy Framework is intended to help organizations build better privacy foundations by bringing privacy risk into parity with their broader enterprise risk portfolio.

## 1. Privacy Framework Introduction

For more than two decades, the Internet and associated information technologies have driven unprecedented innovation, economic value, and access to social services. Many of these benefits are fueled by *data* about *individuals* that flow through a complex ecosystem. As a result, individuals may not realize the potential consequences for their privacy as they interact with systems, products, and services. Organizations may not fully realize the consequences either. Failure to manage *privacy risks* can have direct adverse consequences at both the individual and societal levels, with follow-on effects on organizations' brands, bottom lines, and future prospects for growth. Finding ways to continue to derive benefits from *data processing* while simultaneously protecting individuals' privacy is challenging, and not well-suited to one-size-fits-all solutions.

Privacy is challenging because not only is it an all-encompassing concept that helps to safeguard important values such as human autonomy and dignity, but also the means for achieving it can vary.[4] For example, privacy can be achieved through seclusion, limiting observation, or individuals' control of facets of their identities (e.g., body, data, reputation).[5] Moreover, human autonomy and dignity are not fixed, quantifiable constructs; they are filtered through cultural diversity and individual differences. This broad and shifting nature of privacy makes it difficult to communicate clearly about privacy risks within and between organizations and with individuals. What has been missing is a common language and practical tool that is flexible enough to address various privacy needs.

NIST Privacy Framework 1.1 is a voluntary tool, intended to be widely usable by organizations of all sizes, and agnostic to any particular technology, sector, law, or jurisdiction. Using a common approach—adaptable to any organization's role(s) in the *data processing ecosystem*—the Privacy Framework's purpose is to help organizations manage privacy risks by:

- Taking privacy into account as they design and deploy systems, products, and services that affect individuals;
- Communicating about their privacy practices; and
- Encouraging cross-organizational workforce collaboration—for example, among executives, legal, and information technology (IT)—through the development of Profiles, selection of Tiers, and achievement of outcomes.

[4] Autonomy and dignity are concepts covered in the United Nations Universal Declaration of Human Rights at https://www.un.org/en/universal-declaration-human-rights/.

[5] There are many publications that provide an in-depth treatment on the background of privacy or different aspects of the concept. For two examples, see Solove D (2010) *Understanding Privacy* (Harvard University Press, Cambridge, MA). Available at https://ssrn.com/abstract=1127888; and Selinger E, Hartzog W (2017) Obscurity and Privacy, *Spaces for the Future: A Companion to Philosophy of Technology*, eds Pitt J, Shew A (Taylor & Francis, New York, NY), Chapter 12, 1st Ed. Available at https://doi.org/10.4324/9780203735657.

## 1.1. Overview of the Privacy Framework

As shown in **Figure 1**, the Privacy Framework is composed of three components: Core, Organizational Profiles, and Tiers. Each component reinforces how organizations manage privacy risk through the connection between business or mission drivers, organizational roles and responsibilities, and privacy protection activities. As further explained in Section 2:

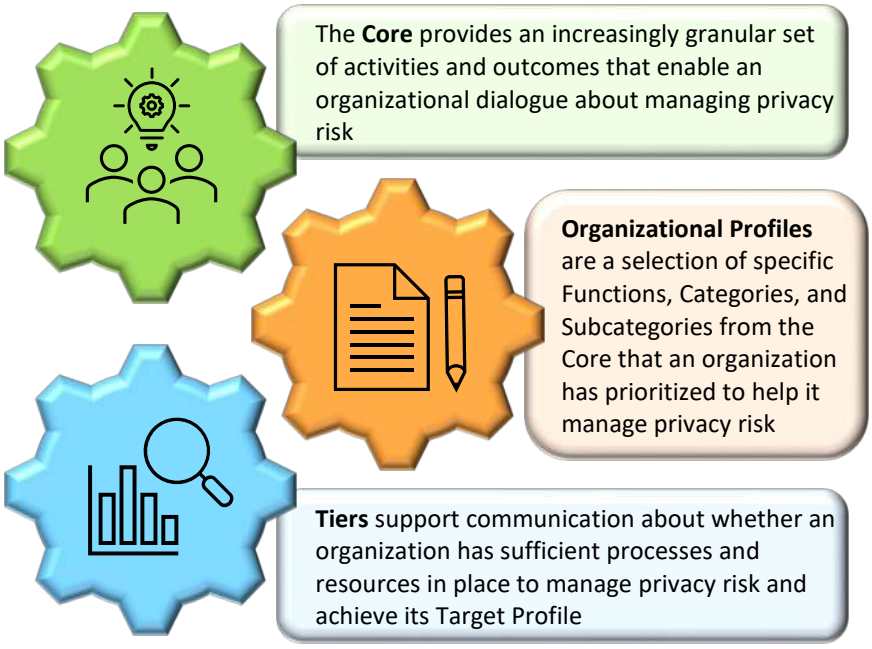



**Figure 1: Core, Organizational Profiles, and Tiers**

- The *Core* is a set of privacy protection activities and outcomes that allows for communicating prioritized privacy protection activities and outcomes across an organization from the executive level to the implementation/operations level. The Core is further divided into key Categories and Subcategories—which are discrete outcomes—for each Function.
- An Organizational *Profile* represents an organization's current privacy activities or desired outcomes. Groups of organizations can also create Community Profiles to address shared privacy risk management needs and priorities. To develop a Profile, an organization can review all the outcomes and activities in the Core to determine which are most important to focus on based on business or mission drivers, data processing ecosystem role(s), types of data processing, and individuals' privacy needs. An organization can create or add Functions, Categories, and Subcategories as needed. Profiles can be used to identify opportunities for improving privacy posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state). Profiles can be used to conduct self-assessments and to communicate within an organization or between organizations about how privacy risks are being managed.
- *Tiers* provide a point of reference on how an organization views privacy risk and whether it has sufficient processes and resources in place to manage that risk. Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk informed. When selecting Tiers, an organization should consider its Target Profile(s) and how achievement may be supported or hampered by factors such as its current risk management practices, the degree of integration of privacy risk into its enterprise risk management portfolio, its data processing ecosystem relationships, and its workforce composition and training program.

## 1.2. Privacy Risk Management

To promote broader understanding of *privacy risk management*, this section covers concepts and considerations that organizations may use to develop, improve, or communicate about privacy risk management. Appendix D provides additional information on key privacy risk management practices.

### 1.2.1. Cybersecurity and Privacy Risk Management

Since its release in 2014, the Cybersecurity Framework has helped organizations to communicate and manage cybersecurity risk. [1] While managing cybersecurity risk contributes to managing privacy risk, it is not sufficient, as privacy risks can also arise by means unrelated to *cybersecurity incidents*, as illustrated by **Figure 2.** Having a general understanding of the different origins of cybersecurity and privacy risks is important for determining the most effective solutions to address the risks.

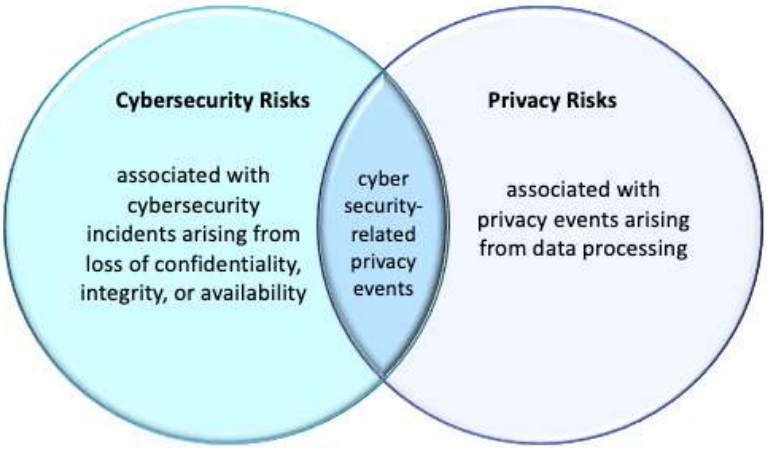



**Figure 2: Cybersecurity and Privacy Risk Relationship**

***Data Action***
A data life cycle operation, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal.

***Data Processing***
The collective set of data actions.

The Privacy Framework approach to privacy risk is to consider *privacy events* as potential problems individuals could experience arising from system, product, or service operations with data, whether in digital or non-digital form, through a complete life cycle from data collection through disposal.

The Privacy Framework describes these data operations in the singular as a *data action* and collectively as data processing. The problems individuals can experience as a result of data processing can be expressed in various ways, but NIST describes them as ranging from dignity-type effects such as embarrassment or stigmas to more tangible harms such as discrimination, economic loss, or physical harm.[6]

The basis for the problems that individuals may experience can vary. As depicted in **Figure 2**, problems arise as an adverse effect of data processing that organizations conduct to meet their

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

mission or business objectives. An example is the concerns that certain communities had about the installation of "smart meters" as part of the Smart Grid, a nationwide technological effort to increase energy efficiency.[7] The ability of these meters to collect, record, and distribute highly granular information about household electrical use could provide insight into people's behavior inside their homes.[8] The meters were operating as intended, but the data processing could lead to people feeling surveilled.

In an increasingly connected world, some problems can arise simply from individuals' interactions with systems, products, and services, even when the data being processed is not directly linked to identifiable individuals. For example, smart cities technologies could be used to alter or influence people's behavior such as where or how they move through the city.[9] Problems also can arise where there is a loss of *confidentiality*, *integrity*, or *availability* at some point in the data processing, such as data theft by external attackers or the unauthorized access or use of data by employees. **Figure 2** shows these types of cybersecurity-related privacy events as the overlap between privacy and cybersecurity risks.

Once an organization can identify the likelihood of any given problem arising from the data processing, which the Privacy Framework refers to as a *problematic data action*, it can assess the impact should the problematic data action occur. This impact assessment is where privacy risk and organizational *risk* intersect. Individuals, whether singly or in groups (including at a societal level) experience the direct impact of problems. As a result of the problems individuals experience, an organization may experience impacts such as noncompliance costs, revenue loss arising from customer abandonment of products and services, or harm to its external brand reputation or internal culture. Organizations commonly manage these types of impacts through enterprise risk management (ERM); by connecting problems that individuals experience to these well-understood organizational impacts, organizations can bring privacy risk into parity with other risks they are managing in their broader portfolio and drive more informed decision-making about resource allocation to strengthen privacy programs. **Figure 3** illustrates this relationship between privacy risk and enterprise risk.[10]

[7] See, for example, NIST Interagency or Internal Report (IR) 7628 Revision 1 Volume 1, Guidelines for Smart Grid Cybersecurity: Volume 1 – Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements at [3] p. 26.

[8] See NIST IR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems* at [4] p. 2. For additional types of privacy risks associated with adverse effects on individuals of data processing, see Appendix E of NIST IR 8062.

[9] See Newcombe T (2016) Security, Privacy, Governance Concerns About Smart City Technologies Grow. *Government Technology*. Available at http://www.govtech.com/Security-Privacy-Governance-Concerns-About-Smart-City-Technologies-Grow.html.

[10] See NIST SP 800-221, *Enterprise Impact of Information and Communications Technology Risk, Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio* at [5] for more information on enterprise risk.

304

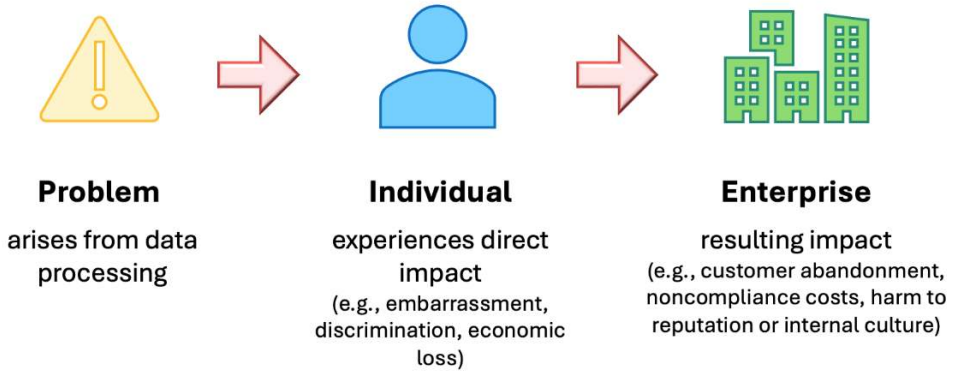



**Figure 3: Relationship Between Privacy Risk and Enterprise Risk**

305

306 ### 1.2.2. Artificial Intelligence and Privacy Risk Management

307 Artificial intelligence (AI) systems are engineered or machine-based systems that can, for a
308 given set of objectives, generate outputs such as predictions, recommendations, or decisions
309 influencing real or virtual environments. As a tool designed for all technologies, Privacy
310 Framework 1.1 can assist organizations with identifying and managing privacy risks that can
311 arise from data processing within AI systems throughout the AI lifecycle. Privacy risks can arise,
312 for example, when AI systems are trained on data that was collected without individuals'
313 consent or have missing or inadequate privacy safeguards.[11] An AI system could also reveal
314 information about individuals by estimating individuals' personal attributes or through privacy
315 attacks such as data reconstruction, prompt injection, or membership inference. This may
316 create privacy problems ranging from embarrassment and stigmatization to unanticipated
317 revelation. Systemic, computational and statistical, as well as human-cognitive biases can exist
318 and persist in AI systems that make important decisions and predictions about people.[12] In
319 some cases, AI technology may be the key enabler of privacy risk (e.g., use of generative AI to
320 create privacy-invasive images, video, or audio). These and other data processing activities
321 within AI systems may create privacy problems for individuals and groups, including at a
322 societal level, ranging from dignity effects to more concrete harms like physical harm and
323 economic loss. As discussed in Section 1.2.1 above, these impacts on the privacy of individuals
324 and groups can lead to significant organizational impacts, ranging from revenue losses to
325 reputational harms.

[11] Numerous publications analyze and characterize AI privacy risks. See, for example, Lee H, Yang Y, von Davier TS, Forlizzi J, Das S (2024) Deepfakes, Phrenology, Surveillance, and More! A Taxonomy of AI Privacy Risks. (Carnegie Mellon University, Pittsburgh PA, United States). Available at https://dl.acm.org/doi/pdf/10.1145/3613904.3642116; and Solove DJ (2024) Artificial Intelligence and Privacy. 77 Florida Law Review, GWU Legal Studies Research Paper No. 2024-36, GWU Law School Public Law Research Paper No. 2024-36. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4713111.

[12] For further discussion of bias in Artificial Intelligence, see Schwartz R, Vassilev A, Greene K, Perine L, Burt A, Hall P (2022) Towards a Standard for Identifying and Managing Bias in Artificial Intelligence. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication 1270. Available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf

Organizations can utilize the Privacy Framework 1.1 Core to identify and prioritize outcomes to effectively manage AI privacy risks and ensure that organizational privacy values are reflected in the development and use of AI systems. For example, organizations can leverage the new Roles, Responsibilities, and Authorities Category (GV.RR-P) to ensure roles and responsibilities for the AI workforce are established with respect to privacy to foster accountability and continuous improvement. Organizations can also prioritize outcomes in the Monitoring and Review Category (GV.MT-P) for regularly reviewing and updating policies to respond to emerging and rapidly evolving AI privacy risks. The Control-P and Communicate-P Functions can be utilized to consider how technical measures like de-identification techniques as well as mechanisms for enabling individuals' data processing preferences can meet an organization's identified AI privacy priorities like data minimization or user control over how their data are used in AI systems.

Managing privacy risks associated with AI can make AI systems more trustworthy and support responsible AI practices. AI risks, however, go beyond privacy risks to implicate other risks such as cybersecurity. The relationship between AI and privacy risk is complex, and AI risk may affect privacy risk differently depending on the specific use case and context. This poses challenges for managing AI and privacy risks together. For example, differentially private synthetic data could be used to train machine learning models while enhancing the privacy protections for the original data. Yet, the synthetic generation process may skew distributions and introduce other biases, which can propagate to downstream applications.

The NIST AI Risk Management Framework (AI RMF) can help organizations manage AI risks and promote trustworthy and responsible development and use of AI systems.[13] The AI RMF can be used with Privacy Framework 1.1 as well as other NIST risk management frameworks such as CSF 2.0. Treating AI risks together with other enterprise risks (e.g., privacy, cybersecurity) supports integrated outcomes and organizational efficiencies. NIST also develops integrated NIST frameworks Community Profiles to assist organizations seeking to effectively use NIST frameworks together and to understand and manage the complex relationship and dependencies among AI and other risks.[14]

### 1.2.3. Privacy Risk Assessment

Privacy risk management is a cross-organizational set of processes that helps organizations to understand how their systems, products, and services may create problems for individuals and how to develop effective solutions to manage such risks. *Privacy risk assessment* is a sub-process for identifying and analyzing specific privacy risks. In general, privacy risk assessments produce the information that can help organizations to weigh the benefits of the data processing against the risks and to determine the appropriate response—sometimes referred to as

[13] See NIST Artificial Intelligence (AI) Risk Management Framework (AI RMF 1.0), NIST AI 100-1 at [6].
[14] See, e.g., NIST Data Governance and Management Profile. Available at https://www.nist.gov/privacy-framework/new-projects/data-governance-and-management-profile.

proportionality.[15] Organizations may choose to prioritize and respond to privacy risk in different ways, depending on the potential impact to individuals and resulting impacts to organizations. Response approaches include:[16] [17]

- Mitigating the risk (e.g., organizations may be able to apply technical and/or policy measures to the systems, products, or services that minimize the risk to an acceptable degree);
- Transferring or sharing the risk (e.g., contracts are a means of sharing or transferring risk to other organizations, privacy notices and consent mechanisms are a means of sharing risk with individuals);
- Avoiding the risk (e.g., organizations may determine that the risks outweigh the benefits, and forego or terminate the data processing); or
- Accepting the risk (e.g., organizations may determine that problems for individuals are minimal or unlikely to occur, therefore the benefits outweigh the risks, and it is not necessary to invest resources in mitigation).

Privacy risk assessments are particularly important because, as noted above, privacy is a condition that safeguards multiple values. The methods for safeguarding these values may differ, and moreover, may be in tension with each other. Depending on its objectives, if an organization is trying to achieve privacy by limiting observation, this may lead to implementing measures such as distributed data architectures or privacy-enhancing cryptographic techniques that hide data even from the organization. If an organization is also trying to enable individual control, the measures could conflict. For example, if an individual requests access to data, the organization may not be able to produce the data if the data have been distributed or encrypted in ways the organization cannot access. Privacy risk assessments can help an organization understand in a given context the values to protect, the methods to employ, and how to balance implementation of different types of measures.

Lastly, privacy risk assessments help organizations distinguish between privacy risk and compliance risk. Identifying if data processing could create problems for individuals, even when an organization may be fully compliant with applicable laws or regulations, can help with ethical decision-making in system, product, and service design or deployment. Although there is no objective standard for ethical decision-making, it is grounded in the norms, values, and legal expectations in a given society. This facilitates optimizing beneficial uses of data while minimizing adverse consequences for individuals' privacy and society as a whole, as well as avoiding losses of trust that damage organizations' reputations, slow adoption, or cause abandonment of products and services.

---

[15] See European Data Protection Supervisor (2019) Necessity & Proportionality. Available at https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en.

[16] See NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* [7].

[17] Where positive risks (i.e., opportunities) are to be considered, such as for setting enterprise risk appetite and tolerance, there are four generally used response types: realize, share, enhance, and accept. For more information on considerations of positive risks as an input to ERM, see NIST Special Publication 800-221, *Enterprise Impact of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio* at [5] p. 35–37.

See Appendix D for more information on the operational aspects of privacy risk assessment.

## 1.3. Document Overview

The remainder of this document contains the following sections and appendices:

- **Section 2** describes the Privacy Framework components: Core, Profiles, and Implementation Tiers.
- **Section 3** presents examples of how the Privacy Framework can be used.
- The **References section** lists the references for the document.
- **Appendix A** presents the Privacy Framework Core in a tabular format: Functions, Categories, and Subcategories.
- **Appendix B** contains a glossary of selected terms.
- **Appendix C** lists acronyms used in this document.
- **Appendix D** considers key practices that contribute to successful privacy risk management.

## 2. Privacy Framework Basics

The Privacy Framework provides a common language for understanding, managing, and communicating privacy risk with internal and external stakeholders. It is adaptable to any organization's role(s) in the data processing ecosystem. It can be used to help identify and prioritize actions for reducing privacy risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk.

### 2.1. Core

Set forth in Appendix A, the Core provides an increasingly granular set of activities and outcomes that enable a dialogue about managing privacy risk. As depicted in **Figure 4**, the Core comprises Functions, Categories, and Subcategories.

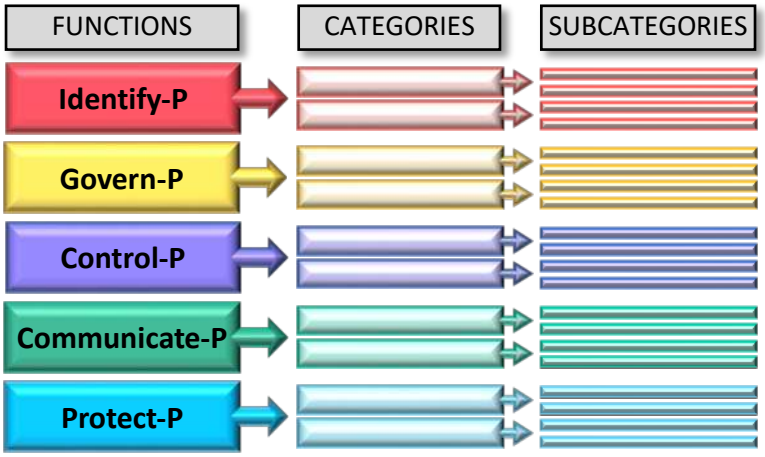



**Figure 4: Privacy Framework Core Structure**

The Core elements work together:

- *Functions* organize foundational privacy activities at their highest level. They aid an organization in expressing its management of privacy risk by understanding and managing data processing, enabling risk management decisions, determining how to interact with individuals, and improving by learning from previous activities. They are not intended to form a serial path or lead to a static desired end state. Rather, the Functions should be performed concurrently and continuously to form or enhance an operational culture that addresses the dynamic nature of privacy risk.
- *Categories* are the subdivisions of a Function into groups of privacy outcomes closely tied to programmatic needs and particular activities.
- *Subcategories* further divide a Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category.

The five Functions, Identify-P, Govern-P, Control-P, Communicate-P, and Protect-P, defined below, can be used to manage privacy risks arising from data processing.[18] Protect-P is specifically focused on managing risks associated with cybersecurity-related privacy events (e.g., *privacy breaches*). CSF 2.0, although intended to cover all types of cybersecurity incidents, can be leveraged to further support the management of risks associated with cybersecurity-related privacy events by using the Govern, Detect, Respond, and Recover Functions.

[18] The "-P" at the end of each Function name indicates that it is from the Privacy Framework in order to avoid confusion with Cybersecurity Framework Functions.

Alternatively, organizations may use all six CSF 2.0 Functions in conjunction with Identify-P, Govern-P, Control-P, and Communicate-P to collectively address privacy and cybersecurity risks. The five Privacy Framework Functions are defined as follows:

- *Identify-P* – Develop the organizational understanding to manage privacy risk for individuals arising from data processing.

  The activities in the Identify-P Function are foundational for effective use of the Privacy Framework. Inventorying the circumstances under which data are processed, understanding the privacy interests of individuals directly or indirectly served or affected by an organization, and conducting risk assessments enable an organization to understand the business environment in which it is operating and identify and prioritize privacy risks.

- *Govern-P* – Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.

  The Govern-P Function is similarly foundational, but focuses on organizational-level activities such as establishing organizational privacy values and policies, identifying legal/regulatory requirements, and understanding organizational *risk tolerance* that enable an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

- *Control-P* – Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.

  The Control-P Function considers data processing management from the standpoint of both organizations and individuals.

- *Communicate-P* – Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks.

  The Communicate-P Function recognizes that both organizations and individuals may need to know how data are processed in order to manage privacy risk effectively.

- *Protect-P* – Develop and implement appropriate data processing safeguards.

  The Protect-P Function covers data protection to prevent cybersecurity-related privacy events, the overlap between privacy and cybersecurity risk management.

## 2.2. Profiles

Profiles are a selection of specific Functions, Categories, and Subcategories from the Core that an organization has prioritized to help it manage privacy risk. Profiles can be used to describe the current state and the desired target state of specific privacy activities. A Current Profile indicates privacy outcomes that an organization is currently achieving, while a Target Profile indicates the outcomes needed to achieve the desired privacy risk management goals. The differences between the two Profiles enable an organization to identify gaps, develop an action plan for improvement, and gauge the resources that would be needed (e.g., staffing, funding) to achieve privacy outcomes. This forms the basis of an organization's plan for reducing privacy risk in a cost-effective, prioritized manner. Profiles also can aid in communicating risk within and between organizations by helping organizations understand and compare the current and desired state of privacy outcomes.

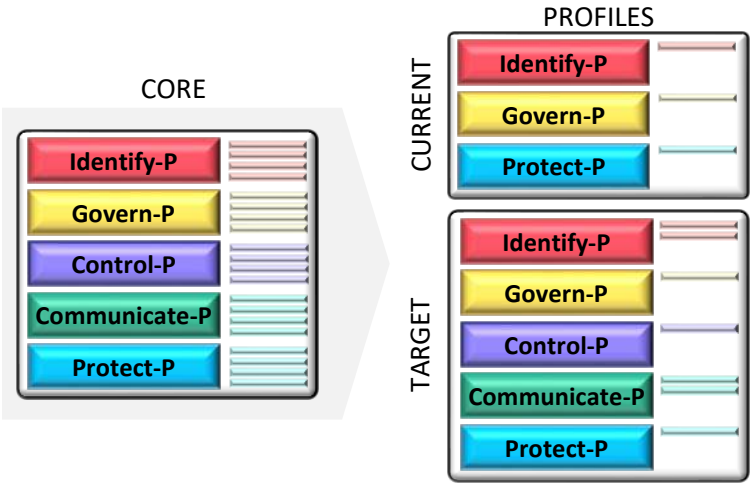



**Figure 5: Relationship Between Core and Profiles**

The Privacy Framework does not prescribe Profile templates to allow for flexibility in implementation. When creating Profiles, organizations may include additional categories of information to support achievement of their prioritized outcomes and activities. Examples of these categories of information include:

- Priority level
- Status
- Associated policies, processes, and procedures
- Roles and responsibilities
- Informative references (e.g., NIST Privacy Workforce Taxonomy)[19]

Under the Privacy Framework's risk-based approach, organizations may not need to achieve every outcome or activity reflected in the Core. When developing a Profile, an organization may select or tailor the Functions, Categories, and Subcategories to its specific needs, including developing its own additional Functions, Categories, and Subcategories to account for unique

[19] The NIST Privacy Workforce Taxonomy is a set of Task, Knowledge, and Skill Statements aligned with the NIST Privacy Framework and the NICE Workforce Framework. The Privacy Workforce Taxonomy can help organizations better achieve their desired privacy outcomes, support recruitment with more consistent position descriptions, and inform the education and training of professionals to produce a workforce capable of managing privacy risk. More information is available at https://www.nist.gov/privacy-framework/workforce-advancement/privacy-workforce-taxonomy.

organizational risks. An organization determines these needs by considering its mission or business objectives, privacy values, and risk tolerance; role(s) in the data processing ecosystem or industry sector; legal/regulatory requirements and industry best practices; risk management priorities and resources; and the privacy needs of individuals who are directly or indirectly served or affected by an organization's systems, products, or services.

As illustrated in **Figure 6**, there is no specified order of development of Profiles. An organization may first develop a Target Profile to focus on its desired outcomes for privacy and then develop a Current Profile to identify gaps. Alternatively, an organization may begin by identifying its current activities and then consider how to adjust these activities for its Target Profile. An organization may choose to develop multiple Profiles for different roles, systems, products, or services, or categories of individuals (e.g., employees, customers) to enable better prioritization of activities and outcomes where there may be differing degrees of privacy risk.

Organizations in a certain industry sector or with similar roles in the data processing ecosystem may coordinate to develop Community Profiles to address shared interests and goals.[20] An organization can use a Community Profile as a basis for its own organizational Profile. The National Cybersecurity Center of Excellence (NCCoE) offers numerous resources to support organizations seeking to utilize existing Community Profiles or to develop their own Community Profile(s). These resources can be found at https://www.nccoe.nist.gov/.

## 2.3. Tiers

Tiers support organizational decision-making about how to manage privacy risk by considering the nature of the privacy risks engendered by an organization's systems, products, or services and the sufficiency of the processes and resources an organization has in place to manage such risks. As illustrated in Figure 6 below, there are four distinct Tiers, Partial (Tier 1), Risk Informed (Tier 2), Repeatable (Tier 3), and Adaptive (Tier 4). Tiers are described in more detail in Appendix E.

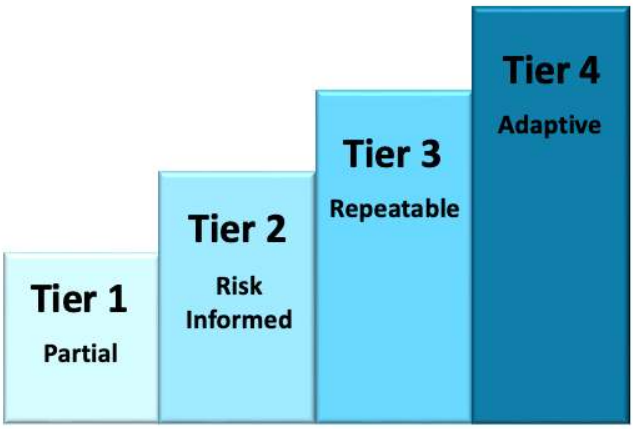



**Figure 6: Privacy Framework Tiers**

[20] More information on CSF Community Profiles can be found at https://www.nist.gov/cyberframework/profiles.

When selecting Tiers, an organization should consider:

- Its Target Profile(s) and how achievement may be supported or hampered by its current risk management practices
- The degree of integration of privacy risk into its enterprise risk management portfolio
- Its data processing ecosystem relationships
- Its workforce composition and training program.

The Tiers represent a progression, but progression is not required. Although organizations at Tier 1 will likely benefit from moving to Tier 2, not all organizations need to achieve Tiers 3 or 4 (or may only focus on certain areas of these Tiers). Progression to higher Tiers is appropriate when an organization's processes or resources at its current Tier may be insufficient to help it manage its privacy risks.

An organization can use the Tiers to communicate internally about resource allocations necessary to progress to a higher Tier or as general benchmarks to gauge progress in its capability to manage privacy risks. An organization can also use Tiers to understand the scale of resources and processes of other organizations in the data processing ecosystem and how they align with the organization's privacy risk management priorities. Nonetheless, successful implementation of the Privacy Framework is based upon achieving the outcomes described in an organization's Target Profile(s) and not upon Tier determination.

## 3. How to Use the Privacy Framework

When used as a risk management tool, the Privacy Framework can assist an organization in its efforts to optimize beneficial uses of data and develop innovative systems, products, and services while minimizing adverse consequences for individuals. The Privacy Framework can help organizations answer the fundamental question, "How are we considering the privacy impacts to individuals and groups as we develop our systems, products, and services?" To account for the unique needs of an organization, use of the Privacy Framework is flexible, although it is designed to complement existing business and system development operations. Privacy Framework 1.1 may be used in many ways. For example, an organization may already have robust privacy risk management processes, but it may use the Core's five Functions as a streamlined way to analyze gaps and articulate privacy program needs with leadership and decision-makers. Alternatively, an organization seeking to establish a privacy program can use the Core's Categories and Subcategories as a reference. Other organizations may compare Profiles or Tiers to align privacy risk management priorities across different roles in the data processing ecosystem.

The variety of ways in which the Privacy Framework can be used by organizations should discourage the notion of "compliance with the Privacy Framework" as a uniform or externally referenceable concept. A few example options for use of the Privacy Framework are as follows:

- **Using with Informative References.** Informative References, such as those found in the Privacy Framework online Resource Repository and National Online Informative Reference Program, support Privacy Framework 1.1 use by mapping to the Privacy Framework Core. Informative References include crosswalks, Profiles, guidelines, and tools.
- **Strengthening Accountability.** Privacy Framework 1.1 supports collaboration and communication across an organization, from senior executives to business/process managers to the implementation/operations level.
- **Establishing or improving a privacy program.** Privacy Framework 1.1 can support the creation of a new privacy program or improvement of an existing program.
- **Applying to the system development life cycle.** A Privacy Framework 1.1 Target Profile can be aligned with the system development life cycle phases (e.g., plan, design, deploy, decommission) to support achievement of prioritized privacy outcomes.
- **Using within the data processing ecosystem.** By developing one or more Privacy Framework 1.1 Profiles relevant to its role(s) in the data processing ecosystem, an organization can consider how its privacy risk management practices affect other data processing ecosystem entities' management of privacy risk.
- **Informing Buying Decisions.** A Privacy Framework 1.1 Profile can be used to generate a prioritized list of privacy requirements

For more details on how to use Privacy Framework 1.1, please visit the "Using Privacy Framework 1.1" webpage. Informative References, informational videos, and the Privacy Framework Quick Start Guide, can also be found at the Privacy Framework Learning Center.

## References

[1] National Institute of Standards and Technology (2024) Cybersecurity Framework 2.0. (National Institute of Standards and Technology, Gaithersburg, MD). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[2] National Institute of Standards and Technology (2019) NIST Privacy Risk Assessment Methodology (PRAM). (National Institute of Standards and Technology, Gaithersburg, MD). https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources

[3] The Smart Grid Interoperability Panel—Smart Grid Cybersecurity Committee (2014) Guidelines for Smart Grid Cybersecurity: Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7628, Rev. 1, Vol. 1. https://doi.org/10.6028/NIST.IR.7628r1

[4] Brooks SW, Garcia ME, Lefkovitz NB, Lightman S, Nadeau EM (2017) An Introduction to Privacy Engineering and Risk Management in Federal Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8062. https://doi.org/10.6028/NIST.IR.8062

[5] Quinn S, Ivy N, Chua J, Barrett M, Feldman L, Topper D, Witte G, Gardner RK, Scarfone K (2023) Enterprise Impact of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-221. https://doi.org/10.6028/NIST.SP.800-221

[6] National Institute of Standards and Technology (2023) Artificial Intelligence Risk Management Framework (AI RMF 1.0). (National Institute of Standards and Technology, Gaithersburg, MD), NIST AI 100-1. https://doi.org/10.6028/NIST.AI.100-1

[7] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

[8] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37 Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[9] Temoshok D, Proud-Madruga D, Choong Y, Galluzzo R, Gupta S, LaSalle C, Lefkovitz N, Regenscheid A (2024) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-4 2nd Public Draft, Includes updates as of August 21, 2024. https://doi.org/10.6028/NIST.SP.800-63-4.2pd

[10] Office of Management and Budget (2017) Preparing for and Responding to a Breach of Personally Identifiable Information. (The White House, Washington, DC), OMB Memorandum M-17-12, January 3, 2017. Available at https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf

[11] Joint Task Force (2020) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5, includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[12] Grassi PA, Lefkovitz NB, Nadeau EM, Galluzzo RJ, Dinh AT (2018) Attribute Metadata: A Proposed Schema for Evaluating Federated Attributes. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8112. https://doi.org/10.6028/NIST.IR.8112

[13] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

[14] "Definitions," Title 44 *U.S. Code*, Sec. 3542. 2013 ed. https://www.govinfo.gov/app/details/USCODE-2013-title44/USCODE-2013-title44-chap35-subchapIII-sec3542/summary

# Appendix A. Privacy Framework Core

This appendix presents the Core: a table of Functions, Categories, and Subcategories that describe specific activities and outcomes that can support managing privacy risks when systems, products, and services are processing data.

## Note to Users

**Risk-based Approach:**

- **The Core is not a checklist of actions to perform. An organization selects Functions, Categories, and Subcategories consistent with its risk strategy to protect individuals' privacy.** An organization may not need to achieve every outcome or activity reflected in the Core. It is expected that an organization will use Profiles to select and prioritize the Functions, Categories, and Subcategories that best meet its specific needs by considering its goals, role(s) in the data processing ecosystem or industry sector, legal/regulatory requirements and industry best practices, risk management priorities, and the privacy needs of individuals who are directly or indirectly served or affected by an organization's systems, products, or services.
- **It is not obligatory to achieve a Core outcome in its entirety.** An organization may use its Profiles to express partial achievement of an outcome, as not all aspects of an outcome may be relevant for it to manage privacy risk. An organization may also use a Target Profile to express an aspect of an outcome that it does not currently have the capability to achieve.
- **It may be necessary to consider multiple Core outcomes in combination to appropriately manage privacy risk.** For example, an organization that responds to individuals' requests for data access may select for its Profile both the Subcategory CT.DM-P1: "Data elements can be accessed for review" and the Category "Identity Management, Authentication, and Access Control" (PR.AC-P) to ensure that only the individual to whom the data pertain gets access.

**Implementation:**

- **The tabular format of the Core is not intended to suggest a specific implementation order or imply a degree of importance between the Functions, Categories, and Subcategories.** Implementation may be nonsequential, simultaneous, or iterative, depending on the SDLC stage, status of the privacy program, scale of the workforce, or role(s) of an organization in the data processing ecosystem.
- **The Core is not exhaustive.** The Core is extensible, allowing organizations, sectors, and other entities to adapt or add additional Functions, Categories, and Subcategories to their Profiles.

**Roles:**

- **Ecosystem Roles:** The Core is intended to be usable by any organization or entity regardless of its role(s) in the data processing ecosystem. Although the Privacy

Framework does not classify ecosystem roles, an organization should review the Core from its standpoint in the ecosystem. An organization's role(s) may be legally codified—for example, some laws classify organizations as data controllers or data processors—or classifications may be derived from industry designations. Since Core elements are not assigned by ecosystem role, an organization can use its Profiles to select Functions, Categories, and Subcategories that are relevant to its role(s).

- **Organizational Roles:** Different parts of an organization's workforce may take responsibility for different Categories or Subcategories. For example, the legal department may be responsible for carrying out activities under "Governance Policies, Processes, and Procedures" while the IT department is working on "Inventory and Mapping." Ideally, the Core encourages cross- organization collaboration to develop Profiles and achieve outcomes.

**Scalability:** Certain aspects of outcomes may be ambiguously worded. For example, outcomes may include terms like "communicated" or "disclosed" without stating to whom the communications or disclosures are being made. The ambiguity is intentional to allow for a wide range of organizations with different use cases to determine what is appropriate or required in a given context.

**Online Resource Repository:** Standalone resources that can provide more information on how to prioritize or achieve outcomes can be found at https://www.nist.gov/privacy-framework.

**Cybersecurity Framework Alignment:**

- The Privacy Framework 1.1 update maintains alignment with CSF 2.0 wherever possible, while also addressing organizations' unique privacy needs. In order to achieve this, some Privacy Framework 1.0 Categories and Subcategories have been withdrawn or relocated. These changes are noted in **Table 2** where applicable.
- Certain Functions, Categories, or Subcategories may be identical to or have been adapted from the Cybersecurity Framework. The following legend can be used to identify this relationship in **Table 2**.

The Function, Category, or Subcategory aligns with the Cybersecurity Framework, but the text has been adapted for the Privacy Framework.

The Category or Subcategory is identical to the Cybersecurity Framework.

- A complete crosswalk between Privacy Framework 1.1 and CSF 2.0 can be found in the resource repository at https://www.nist.gov/privacy-framework/resource-repository.

**Core Identifiers:** For ease of use, each component of the Core is given a unique identifier. Functions and Categories each have a unique alphabetic identifier, as shown in **Table 1**. Subcategories within each Category have a number added to the alphabetic identifier; the unique identifier for each Subcategory is included in **Table 2**.

733 **Table 1: Privacy Framework 1.1 Function and Category Unique Identifiers**

734

| Function Unique Identifier | Function | Category Unique Identifier | Category |
|---|---|---|---|
| **ID-P** | Identify-P | ID.IM-P | Inventory and Mapping |
| | | ID.BE-P | Business Environment |
| | | ID.RA-P | Risk Assessment |
| **GV-P** | Govern-P | GV.PO-P | Governance Policies, Processes, and Procedures |
| | | GV.RM-P | Risk Management Strategy |
| | | GV.OV-P | Oversight |
| | | GV.RR-P | Roles, Responsibilities, and Authorities |
| | | GV.DE-P | Data Processing Ecosystem Risk Management |
| | | GV.AT-P | Awareness and Training |
| | | GV.MT-P | Monitoring and Review |
| **CT-P** | Control-P | CT.PO-P | Data Processing Policies, Processes, and Procedures |
| | | CT.DM-P | Data Processing Management |
| | | CT.DP-P | Disassociated Processing |
| **CM-P** | Communicate-P | CM.PO-P | Communication Policies, Processes, and Procedures |
| | | CM.AW-P | Data Processing Awareness |
| **PR-P** | Protect-P | PR.PO-P | Data Protection Policies, Processes, and Procedures |
| | | PR.AA-P | Identity Management, Authentication, and Access Control |
| | | PR.DS-P | Data Security |
| | | PR.PS-P | Platform Security |
| | | PR.IR-P | Technology Infrastructure Resilience |

735 **Table 2: Privacy Framework Core**

| Function | Category | Subcategory |
|---|---|---|
| **IDENTIFY-P (ID-P):** Develop the organizational understanding to manage privacy risk for individuals arising from data processing. | **Inventory and Mapping (ID.IM-P):** Data processing by systems, products, or services is understood and informs the management of privacy risk. | **ID.IM-P1:** Systems/products/services that process data are inventoried. |
| | | **ID.IM-P2:** Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried. |
| | | **ID.IM-P3:** Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried. |
| | | **ID.IM-P4:** Data actions of the systems/products/services are inventoried. |
| | | **ID.IM-P5:** The purposes for the data actions are inventoried. |
| | | **ID.IM-P6:** Data elements within the data actions are inventoried. |
| | | **ID.IM-P7:** The data processing environment is identified (e.g., geographic location, internal, cloud, third parties). |
| | | **ID.IM-P8:** Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services. |
| | **Business Environment (ID.BE-P):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform privacy roles, responsibilities, and risk management decisions. | **ID.BE-P1:** The organization's role(s) in the data processing ecosystem are identified, communicated, and understood. |
| | | **ID.BE-P2:** The organizational mission is identified, communicated, and understood and informs privacy risk management. |
| | | **ID.BE-P3:** Systems/products/services that support organizational priorities are identified and key requirements communicated and understood. |

| | Function | Category | Subcategory |
|---|---|---|---|
| | | | **ID.BE-P4:** Data processing ecosystem parties (e.g., service providers, customers, partners, product manufacturers, application developers) are identified and prioritized. |
| | | | **ID.BE-P5:** Objectives, capabilities, and services that stakeholders depend on or expect from the organization are identified, communicated, and understood. |
| | | | **ID.BE-P6:** Outcomes, capabilities, and services that the organization depends on are identified, communicated, and understood. |
| | | **Risk Assessment (ID.RA-P):** The organization understands the privacy risks to individuals and how such privacy risks may create follow-on impacts on organizational operations, including mission, functions, other risk management priorities (e.g., compliance, financial), reputation, workforce, and culture. | **ID.RA-P1:** Contextual factors related to the systems/products/services and the data actions are identified (e.g., individuals' demographics and privacy interests or perceptions, data sensitivity and/or types, visibility of data processing to individuals and third parties). |
| | | | **ID.RA-P2:** *This Subcategory related to artificial intelligence systems is WITHDRAWN to keep PF 1.1 Core outcomes technology-neutral.* |
| | | | **ID.RA-P3:** Potential problematic data actions and associated problems are identified. |
| | | | **ID.RA-P4:** Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk. |
| | | | **ID.RA-P5:** Risk responses are identified, prioritized, and implemented. |
| | | | **ID.RA-P6:** Data processing ecosystem parties (e.g., service providers, customers, partners, product manufacturers, application developers) are assessed using a privacy risk assessment process. |
| | | **Data Processing Ecosystem Risk Management (ID.DE-P):** *Category is moved to Govern-P and renamed GV.DE-P.* | **ID.DE-P1:** *Moved to GV.DE-P1* |
| | | | **ID.DE-P2:** *Moved to ID.BE-P4 and ID.RA-P6* |
| | | | **ID.DE-P3:** *Moved to GV.DE-P2* |
| | | | **ID.DE-P4:** *Moved to GV.DE-P3* |
| | | | **ID.DE-P5:** *Moved to GV.DE-P4* |
| | **GOVERN-P (GV-P):** Develop and implement the organizational | **Governance Policies, Processes, and Procedures (GV.PO-P):** The policies, processes, and procedures to manage and monitor the organization's regulatory, | **GV.PO-P1:** Organizational privacy values and policies (e.g., conditions on data processing such as data uses or retention periods, individuals' prerogatives with respect to data processing) are established, communicated, and enforced. |

| Function | Category | Subcategory |
|---|---|---|
| governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk. | legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk. | **GV.PO-P2:** Processes to instill organizational privacy values within system/product/service development and operations are established and in place. |
| | | **GV.PO-P3:** *Moved to GV.RR-P2* |
| | | **GV.PO-P4:** *Moved to GV.RR-P3* |
| | | **GV.PO-P5:** Legal, regulatory, and contractual requirements regarding privacy are understood and managed. |
| | | **GV.PO-P6:** Governance and enterprise risk management policies, processes, and procedures address privacy risks. |
| | | **GV.PO-P7:** Privacy procedures are included in human resources practices (e.g., deprovisioning, personnel screening). |
| | **Risk Management Strategy (GV.RM-P):** The organization's priorities, constraints, risk tolerance and appetite, and assumptions are established and used to support operational risk decisions. | **GV.RM-P1:** Risk management objectives and processes are established, managed, and agreed to by organizational stakeholders. |
| | | **GV.RM-P2:** The organization's risk appetite and risk tolerance are determined and communicated and are informed by the organization's role(s) in the data processing ecosystem. |
| | | **GV.RM-P3:** *Moved to GV.RM-P2* |
| | | **GV.RM-P4:** Strategic direction that describes appropriate risk response options is established and communicated. |
| | | **GV.RM-P5:** Lines of communication across the organization are established for privacy risks, including risks from data processing ecosystem parties. |
| | | **GV.RM-P6:** A standardized method for calculating, documenting, categorizing, and prioritizing privacy risks is established and communicated. |
| | | **GV.RM-P7:** Strategic opportunities (i.e., positive risks) are characterized and included in organizational privacy risk discussions. |

| | Function | Category | Subcategory |
|---|---|---|---|
| | | **Oversight (GV.OV-P):** Results of organization-wide privacy risk management activities and performance are used to inform, improve, and adjust the risk management strategy. | **GV.OV-P1:** Privacy risk management strategy outcomes are reviewed to inform and adjust strategy and direction. |
| | | | **GV.OV-P2:** The privacy risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks. |
| | | | **GV.OV-P3:** Organizational privacy risk management performance is measured and reviewed to confirm and adjust strategic direction. |
| | | **Roles, Responsibilities, and Authorities (GV.RR-P):** Privacy roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated. | **GV.RR-P1:** Organizational leadership is responsible and accountable for privacy risk and fosters a culture that is risk-aware, ethical, and continually improving. |
| | | | **GV.RR-P2:** Roles and responsibilities for the workforce are established with respect to privacy. |
| | | | **GV.RR-P3:** Privacy roles and responsibilities are coordinated and aligned with external stakeholders (e.g., service providers, customers, partners). |
| | | | **GV.RR-P4:** Adequate resources are allocated commensurate with privacy risk strategy, roles and responsibilities, and policies. |
| | | **Data Processing Ecosystem Risk Management (GV.DE-P):** The organization's priorities, constraints, risk tolerance, and assumptions are established and used to support processes and risk decisions associated with data processing ecosystem risk management. | **GV.DE-P1:** Data processing ecosystem risk management strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders. |
| | | | **GV.DE-P2:** Contracts with data processing ecosystem parties are used to implement appropriate measures designed to meet the objectives of an organization's privacy program. |
| | | | **GV.DE-P3:** Interoperability frameworks or similar multi-party approaches are used to manage data processing ecosystem privacy risks. |
| | | | **GV.DE-P4:** Data processing ecosystem parties are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual, interoperability framework, or other obligations. |

| | Function | Category | Subcategory |
|---|---|---|---|
| | | | **GV.DE-P5:** Data processing ecosystem risk management is integrated into privacy and enterprise risk management, risk assessment, and improvement processes. |
| | | **Awareness and Training (GV.AT-P):** The organization's personnel are provided with privacy awareness and training so that they can perform their privacy-related tasks | **GV.AT-P1:** Personnel are provided with awareness and training so that they possess the knowledge and skills to perform privacy-related tasks. |
| | | | **GV.AT-P2:** Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform privacy-related tasks. |
| | | | **GV.AT-P3:** *Moved to GV.AT-P2* |
| | | | **GV.AT-P4:** *Moved to GV.AT-P2* |
| | | **Monitoring and Review (GV.MT-P):** The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk. | **GV.MT-P1:** Privacy risk is re-evaluated on an ongoing basis and as key factors, including the organization's business environment (e.g., introduction of new technologies), governance (e.g., legal obligations, risk tolerance), data processing, and systems/products/services change. |
| | | | **GV.MT-P2**: Privacy values, policies, and training are reviewed and any updates are communicated. |
| | | | **GV.MT-P3**: Policies, processes, and procedures for assessing compliance with legal requirements and privacy policies are established and in place. |
| | | | **GV.MT-P4:** Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place. |
| | | | **GV.MT-P5:** Policies, processes, and procedures are established and in place to receive, analyze, and respond to problematic data actions disclosed to the organization from internal and external sources (e.g., internal discovery, privacy researchers, professional events). |
| | | | **GV.MT-P6:** Policies, processes, and procedures incorporate lessons learned from problematic data actions. |

| | Function | Category | Subcategory |
|---|---|---|---|
| | | | **GV.MT-P7:** Policies, processes, and procedures for receiving, tracking, and responding to complaints, concerns, and questions from individuals about organizational privacy practices are established and in place. |
| | **CONTROL-P (CT-P):** Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks. | **Data Processing Policies, Processes, and Procedures (CT.PO-P):** Policies, processes, and procedures are maintained and used to manage data processing (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) consistent with the organization's risk strategy to protect individuals' privacy. | **CT.PO-P1:** Policies, processes, and procedures for authorizing data processing (e.g., organizational decisions, individual consent), revoking authorizations, and maintaining authorizations are established and in place. |
| | | | **CT.PO-P2:** Policies, processes, and procedures for enabling data review, transfer, sharing or disclosure, alteration, and deletion are established and in place (e.g., to maintain data quality, manage data retention). |
| | | | **CT.PO-P3:** Policies, processes, and procedures for enabling individuals' data processing preferences and requests are established and in place. |
| | | | **CT.PO-P4:** A data life cycle to manage data is aligned and implemented with the system development life cycle to manage systems. |
| | | **Data Processing Management (CT.DM-P):** Data are managed consistent with the organization's risk strategy to protect individuals' privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization). | **CT.DM-P1:** Data elements can be accessed for review. |
| | | | **CT.DM-P2:** Data elements can be accessed for transmission or disclosure. |
| | | | **CT.DM-P3:** Data elements can be accessed for alteration. |
| | | | **CT.DM-P4:** Data elements can be accessed for deletion. |
| | | | **CT.DM-P5:** Data are destroyed according to policy. |
| | | | **CT.DM-P6:** Data are transmitted using standardized formats. |
| | | | **CT.DM-P7:** Mechanisms for transmitting processing permissions are established and in place. |
| | | | **CT.DM-P8:** Mechanisms for transmitting data elements in accordance with processing permissions are established and in place. |
| | | | **CT.DM-P9:** Log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization. |

| | Function | Category | Subcategory |
|---|---|---|---|
| | | | **CT.DM-P10:** Technical measures implemented to manage data processing are tested and assessed. |
| | | | **CT.DM-P11:** Stakeholder privacy preferences are included in algorithmic design objectives and outputs are evaluated against these preferences. |
| | | **Disassociated Processing (CT.DP-P):** Data processing solutions increase disassociability consistent with the organization's risk strategy to protect individuals' privacy and enable implementation of privacy principles (e.g., data minimization). | **CT.DP-P1:** Data are processed to limit observability, linkability, and singling out (e.g., data actions take place on local devices, privacy-preserving cryptography). |
| | | | **CT.DP-P2:** Data are processed to limit the identification of individuals (e.g., de-identification privacy techniques, tokenization). |
| | | | **CT.DP-P3:** Data are processed to limit the formulation of inferences about individuals' behavior or activities (e.g., data processing is decentralized, distributed architectures). |
| | | | **CT.DP-P4:** System or device configurations permit selective collection or disclosure of data elements. |
| | | | **CT.DP-P5:** Attribute values are substituted with derived attribute values (e.g., providing an "age older than" statement rather than the actual age). |
| | **COMMUNICATE-P (CM-P):** Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks. | **Communication Policies, Processes, and Procedures (CM.PO-P):** Policies, processes, and procedures are maintained and used to increase transparency of the organization's data processing practices (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) and associated privacy risks. | **CM.PO-P1:** Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established and in place. |
| | | | **CM.PO-P2:** Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established. |
| | | **Data Processing Awareness (CM.AW-P):** Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the | **CM.AW-P1:** Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place. |
| | | | **CM.AW-P2:** Mechanisms for obtaining feedback from individuals (e.g., surveys or focus groups) about data processing and associated privacy risks are established and in place. |

| | Function | Category | Subcategory |
|---|---|---|---|
| | | organization's risk strategy to protect individuals' privacy. | **CM.AW-P3:** System/product/service design enables data processing visibility. |
| | | | **CM.AW-P4:** Records of data disclosures and sharing are maintained and can be accessed for review or transmission/disclosure. |
| | | | **CM.AW-P5:** Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem. |
| | | | **CM.AW-P6:** Data provenance and lineage are maintained and can be accessed for review or transmission/disclosure. |
| | | | **CM.AW-P7:** Impacted individuals and organizations are notified about a privacy breach or event. |
| | | | **CM.AW-P8:** Individuals are provided with mitigation mechanisms (e.g., credit monitoring, consent withdrawal, data alteration or deletion) to address impacts of problematic data actions. |
| | **PROTECT-P (PR-P):** Develop and implement appropriate data processing safeguards. | **Data Protection Policies, Processes, and Procedures (PR.PO-P):** Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data. | **PR.PO-P1:** *Moved to PR.PS-P1* |
| | | | **PR.PO-P2:** *Moved to PR.PS-P1* |
| | | | **PR.PO-P3:** *Moved to PR.DS-P10* |
| | | | **PR.PO-P4:** *Moved to PR.IR-P2* |
| | | | **PR.PO-P5:** Improvements to data protection policies, processes, and procedures are identified (e.g., from evaluations, security tests and exercises, execution of policies, processes, and procedures), communicated, and implemented. |
| | | | **PR.PO-P6:** *Moved to PR.PO-P5* |
| | | | **PR.PO-P7:** Incident response and recovery plans are established, communicated, maintained, and improved. |
| | | | **PR.PO-P8:** *Moved to PR.PO-P7* |
| | | | **PR.PO-P9:** *Moved to GV.PO-P7* |
| | | | **PR.PO-P10:** *Moved to PR.PS-P2* |
| | | **Identity Management, Authentication, and Access Control (PR.AA-P):** Access to data, devices, and systems is limited to authorized individuals, services, and | **PR.AA-P1:** Identities and credentials for authorized individuals, services, and hardware are managed by the organization. |
| | | | **PR.AA-P2**: Identities are proofed and bound to credentials based on the context of interactions. |

| Function | Category | Subcategory |
|---|---|---|
| | hardware, and is managed commensurate with the assessed risk of unauthorized access. | **PR.AA-P3:** Individuals, services, and hardware are authenticated commensurate with risk.› |
| | | **PR.AA-P4:** Identity assertions are protected, conveyed, and verified. |
| | | **PR.AA-P5:** 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. |
| | | **PR.AA-P6:** Physical access to data and devices is managed, monitored, and enforced commensurate with risk. |
| | **Identity Management, Authentication, and Access Control (PR.AC-P):** *Category is withdrawn; Subcategories moved to PR.AA-P and PR.IR-P* | **PR.AC-P1:** *Moved to PR.AA-P1* |
| | | **PR.AC-P2:** *Moved to PR.AA-P6* |
| | | **PR.AC-P3:** *Moved to PR.AA-P3, PR.AA-P5, and PR.IR-P1* |
| | | **PR.AC-P4:** *Moved to PR.AA-P5* |
| | | **PR.AC-P5:** *Moved to PR.IR-P1* |
| | | **PR.AC-P6:** *Moved to PR.AA-P2* |
| | **Data Security (PR.DS-P):** Data are managed consistent with the organization's risk strategy to protect individuals' privacy and maintain data confidentiality, integrity, and availability. | **PR.DS-P1:** The confidentiality, integrity, and availability of data-at-rest are protected. |
| | | **PR.DS-P2:** The confidentiality, integrity, and availability of data-in-transit are protected. |
| | | **PR.DS-P3:** Systems/products/services and associated data are managed throughout their life cycle. |
| | | **PR.DS-P4:** *Moved to PR.IR-P4* |
| | | **PR.DS-P5:** *Moved to PR.DS-P1, P2, and P9* |
| | | **PR.DS-P6:** *Moved to PR.DS-P8* |
| | | **PR.DS-P7:** *Moved to PR.IR-P1* |
| | | **PR.DS-P8:** The authenticity and integrity of hardware and software are assessed prior to acquisition and use. |
| | | **PR.DS-P9:** The confidentiality, integrity, and availability of data-in-use are protected. |

| Function | Category | Subcategory |
|---|---|---|
| | | **PR.DS-P10:** Backups of data are created, protected, maintained, and tested. |
| | **Platform Security (PR.PS-P):** The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms and associated data are managed consistent with the organization's risk strategy to protect individuals' privacy and maintain data confidentiality, integrity, and availability. | **PR.PS-P1:** Configuration management practices are established and applied. |
| | | **PR.PS-P2:** Software is maintained, replaced, and removed commensurate with risk. |
| | | **PR.PS-P3:** Hardware is maintained, replaced, and removed commensurate with risk. |
| | | **PR.PS-P4:** Installation and execution of unauthorized software are prevented. |
| | **Technology Infrastructure Resilience (PR.IR-P):** Security architectures are managed with the organization's risk strategy to protect individuals' privacy and maintain data confidentiality, integrity, and availability. | **PR.IR-P1:** Networks and environments are protected from unauthorized logical access and usage. |
| | | **PR.IR-P2:** The organization's technology assets, including associated data, are protected from environmental threats. |
| | | **PR.IR-P3:** Mechanisms are implemented to achieve resilience requirements in normal and adverse situations. |
| | | **PR.IR-P4:** Adequate resource capacity to ensure availability is maintained. |
| | **Maintenance (PR.MA-P):** *Category is withdrawn; Subcategories moved to PR.PS-P* | **PR.MA-P1:** *Moved to PR.PS-P2 and P3* |
| | | **PR.MA-P2:** *Moved to PR.PS-P2 and P3* |
| | **Protective Technology (PR.PT-P):** *Category is withdrawn; Subcategories moved to PR.AA-P, PR.PS-P, and PR.IR-P* | **PR.PT-P1:** *Moved to PR.PS-P1* |
| | | **PR.PT-P2:** *Moved to PR.PS-P1* |
| | | **PR.PT-P3:** *Moved to PR.AA-P6 and PR.IR-P1* |
| | | **PR.PT-P4:** *Moved to PR.IR-P3* |

736

## Appendix B. Glossary

This appendix defines selected terms used for the purposes of this publication.

**Attribute Value (NIST SP 800-63-4 2pd [9])**
A complete statement that asserts an identity attribute of a subscriber, independent of format. For example, for the attribute "birthday," a value could be "12/1/1980" or "December 1, 1980."

**Availability (44 U.S.C. [14])**
Ensuring timely and reliable access to and use of information.

**Category**
The subdivision of a Function into groups of privacy outcomes closely tied to programmatic needs and particular activities.

**Communicate-P (Function)**
Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks.

**Confidentiality (44 U.S.C. [14])**
Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

**Control-P (Function)**
Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.

**Core**
A set of privacy protection activities and outcomes. The Framework Core comprises three elements: Functions, Categories, and Subcategories.

**Cybersecurity Incident (OMB 17-12 [10])**
An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

**Data**
A representation of information, including digital and non-digital formats.

**Data Action (Adapted from NIST IR 8062 [4])**
A system/product/service data life cycle operation, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal.

**Data Element**
The smallest named item of data that conveys meaningful information.

**Data Processing (Adapted from NIST IR 8062 [4])**
The collective set of data actions (i.e., the complete data life cycle, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal).

**Data Processing Ecosystem**
The complex and interconnected relationships among entities involved in creating or deploying systems, products, or services or any components that process data.

**Derived Attribute Value (NIST SP 800-63-4 2pd [9])**
A statement that asserts a limited identity *attribute* of a subscriber without containing the attribute value from which it is derived, independent of format. For example, instead of requesting the attribute "birthday," a derived value could be "older than 18". Instead of requesting the attribute for "physical address," a derived value could be "currently residing in this district." Previously referred to as "attribute reference."

**Disassociability (Adapted from NIST IR 8062 [4])**
Enabling the processing of data or events without association to individuals or devices beyond the operational requirements of the system.

**Function**
A component of the Core that provides the highest level of structure for organizing basic privacy activities into Categories and Subcategories.

**Govern-P (Function)**
Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.

**Identify-P (Function)**
Develop the organizational understanding to manage privacy risk for individuals arising from data processing.

**Implementation Tier**
Provides a point of reference on how an organization views privacy risk and whether it has sufficient processes and resources in place to manage that risk.

**Individual**
A single person or a group of persons, including at a societal level.

**Integrity (44 U.S.C. [14])**
Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity.

**Lineage**
The history of processing of a data element, which may include point-to-point data flows and the data actions performed upon the data element.

**Manageability (Adapted from NIST IR 8062 [4])**
Providing the capability for granular administration of data, including alteration, deletion, and selective disclosure.

**Metadata (Adapted from NIST SP 800-53 [11])**
Information describing the characteristics of data.

This may include, for example, structural metadata describing data structures (i.e., data format, syntax, semantics) and descriptive metadata describing data contents.

**Predictability (Adapted from NIST IR 8062 [4])**
Enabling reliable assumptions by individuals, owners, and operators about data and their processing by a system, product, or service.

**Privacy Breach (Adapted from OMB M-17-12 [10])**
The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses data or (2) an authorized user accesses data for an other than authorized purpose.

**Privacy Control (Adapted from NIST SP 800-37 [8])**
The administrative, technical, and physical safeguards employed within an organization to satisfy privacy requirements.

**Privacy Event**
The occurrence or potential occurrence of problematic data actions.

**Privacy Requirement**
A specification for system/product/service functionality to meet stakeholders' desired privacy outcomes.

**Privacy Risk**
The likelihood that individuals will experience problems resulting from data processing, and the impact should they occur.

**Privacy Risk Assessment**
A privacy risk management sub-process for identifying and evaluating specific privacy risks.

**Privacy Risk Management**
A cross-organizational set of processes for identifying, assessing, and responding to privacy risks.

**Problematic Data Action (Adapted from NIST IR 8062 [4])**
A data action that could cause an adverse effect for individuals.

**Processing**
See *Data Processing*.

**Profile**
A selection of specific Functions, Categories, and Subcategories from the Core that an organization has prioritized to help it manage privacy risk.

**Protect-P (Function)**
Develop and implement appropriate data processing safeguards.

**Provenance (Adapted from NIST IR 8112 [12])**
Metadata pertaining to the origination or source of specified data.

**Risk (NIST SP 800-30 [13])**
A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

**Risk Management**
The process of identifying, assessing, and responding to risk.

**Risk Tolerance (NIST SP 800-39 [7])**
The level of risk or degree of uncertainty that is acceptable to organizations.

**Subcategory**
The further divisions of a Category into specific outcomes of technical and/or management activities.

## Appendix C. Acronyms

This appendix defines selected acronyms used in the publication.

**IEC**
International Electrotechnical Commission

**IR**
Interagency or Internal Report

**ISO**
International Organization for Standardization

**IT**
Information Technology

**NIST**
National Institute of Standards and Technology

**OASIS**
Organization for the Advancement of Structured Information Standards

**OECD**
Organisation for Economic Co-operation and Development

**OMB**
Office of Management and Budget

**PMRM**
Privacy Management Reference Model and Methodology

**PRAM**
Privacy Risk Assessment Methodology

**RFC**
Request for Comment

**RFI**
Request for Information

**SDLC**
System Development Life Cycle

**SP**
Special Publication

# Appendix D. Privacy Risk Management Practices

Section 1.2 introduces a number of considerations around privacy risk management, including the relationship between cybersecurity and privacy risk, the relationship between AI and privacy risk, and the role of privacy risk assessment. This appendix considers some of the key practices that contribute to successful privacy risk management, including organizing preparatory resources, determining privacy capabilities, defining privacy requirements, conducting privacy risk assessments, creating privacy requirements traceability, and monitoring for changing privacy risks. Category and Subcategory references are included to facilitate use of the Core to support these practices; these references appear in parentheticals.

## Organizing Preparatory Resources

The appropriate resources facilitate informed decision-making about privacy risks at all levels of an organization. As a practical matter, the responsibility for the development of various resources may belong to different components of an organization. Therefore, a component of an organization depending on certain resources may find that they either do not exist, or may not sufficiently address privacy. In these circumstances, the dependent component can consider the purpose of the resource and either seek the information through other sources or make the best decision it can with the available information. In short, good resources are helpful, but any deficiencies should not prevent organizational components from making the best risk decisions they can within their capabilities.

The following resources, while not exhaustive, build a foundation for better decision-making.

- **Risk management role assignments** (GV.RR-P)

  Establishing and enabling cross-organizational understanding of who is accountable and who has responsibility for privacy risk management as well as other risk management tasks in an organization supports better coordination and accountability for decision-making. In addition, a broad range of perspectives can improve the process of identifying, assessing, and responding to privacy risks. A diverse and cross-functional team can help to identify a more comprehensive range of risks to individuals' privacy, and to select a wider set of mitigations. Determining which roles to include in the risk management discussions depends on organizational context and makeup, although collaboration among an organization's programs that implicate privacy risk (e.g., privacy, cybersecurity, AI) will be important. If one individual is being assigned to multiple roles, managing potential conflicts of interest should be considered.

- **Enterprise risk management strategy** (GV.RM-P)

  An organization's enterprise risk management strategy helps to align an organization's mission and values with organizational risk tolerance, assumptions, constraints, and priorities. Limitations on resources to achieve mission or business objectives and to manage a broad portfolio of risks will likely require trade-offs. Enabling personnel involved in the privacy risk management process to better understand an organization's

strategic direction, risk tolerance, and lines of communication should help to guide decisions about how to allocate resources and improve decisions around risk response.

- **Key stakeholders** (GV.RR-P3, GV.DE-P)

  Privacy stakeholders are those who have an interest or concern in the privacy outcomes of the system, product, or service. For example, legal concerns likely focus on whether the system, product, or service is operating in a way that would cause an organization to be out of compliance with privacy laws or regulations or its business agreements. Business owners that want to maximize usage may be concerned about loss of trust in the system, product, or service due to poor privacy. Individuals whose data are being processed or who are interacting with the system, product, or service will be interested in not experiencing problems or adverse consequences. Understanding the stakeholders and the types of privacy outcomes they are interested in will facilitate system/product/service design that appropriately addresses stakeholders' needs.

- **Organizational-level privacy requirements** (GV.PO-P)

  Organizational-level privacy requirements are a means of expressing the legal obligations, privacy values, and policies to which an organization intends to adhere. Understanding these requirements is key to ensuring that the system/product/service design complies with its obligations. Organizational-level privacy requirements may be derived from a variety of sources, including:

  - Legal environment (e.g., laws, regulations, contracts);
  - Organizational policies or cultural values;
  - Relevant standards; and
  - Privacy principles.

- **System/product/service design artifacts** (ID.BE-P3)

  Design artifacts may take many forms such as system design architectures or data flow diagrams. These artifacts help an organization determine how its systems, products, and services will operate. Therefore, they can help privacy programs understand how systems, products, and services need to function so that controls or measures that help to mitigate privacy risk can be selected and implemented in ways that maintain functionality while protecting privacy.

- **Data maps** (ID.IM-P)

  Data maps illustrate data processing and individuals' interactions with systems, products, and services. A data map shows the data processing environment and includes the components through which data are being processed or with which individuals are interacting, the owners or operators of the components, and discrete data actions and the specific data elements being processed. Data maps can be illustrated in different ways, and the level of detail may vary based on an organization's needs. A data map can be overlaid on existing system/product/service design artifacts for convenience and

ease of communication between organizational components. As discussed below, a data map is an important artifact in privacy risk assessment.

## Determining Privacy Capabilities

Privacy capabilities can be used to describe the system, product, or service property or feature that achieves the desired privacy outcome (e.g., "the service enables data minimization"). The security objectives confidentiality, integrity, and availability along with security requirements are used to inform the security capabilities for a system, product, or service. As set forth in **Table 3**, an additional set of privacy engineering objectives can support the determination of privacy capabilities. An organization may also use the privacy engineering objectives as a high-level prioritization tool. Systems, products, or services that are low in predictability, manageability, or disassociability may be a signal of increased privacy risk, and therefore merit a more comprehensive privacy risk assessment.

In determining privacy capabilities, an organization may consider which of the privacy engineering and security objectives are most important with respect to its mission or business needs, risk tolerance, and organizational-level privacy requirements (see Organizing Preparatory Resources above). Not all of the objectives may be equally important, or trade-offs may be necessary among them. Although the privacy capabilities inform the privacy risk assessment by supporting risk prioritization decisions, the privacy capabilities may also be informed by the risk assessment and adjusted to support the management of specific privacy risks or address changes in the environment, including design changes to the system, product, or service.

978 **Table 3: Privacy Engineering and Security Objectives[21]**

| | Objective | Definition | Principal Related Functions from the Privacy Framework Core |
|---|---|---|---|
| **Privacy Engineering Objectives** | Predictability | Enabling reliable assumptions by individuals, owners, and operators about data and their processing by a system | Identify-P, Govern-P, Control-P, Communicate-P, Protect-P |
| | Manageability | Providing the capability for granular administration of data, including collection, alteration, deletion, and selective disclosure | Identify-P, Govern-P, Control-P |
| | Disassociability | Enabling the processing of data or events without association to individuals or devices beyond the operational requirements of the system | Identify-P, Govern-P, Control-P |
| **Security Objectives** | Confidentiality | Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information | Identify-P, Govern-P, Protect-P |
| | Integrity | Guarding against improper information modification or destruction; includes ensuring information non-repudiation and authenticity | Identify-P, Govern-P, Protect-P |
| | Availability | Ensuring timely and reliable access to and use of information | Identify-P, Govern-P, Protect-P |

979 ## Defining Privacy Requirements

980 Privacy requirements specify the way a system, product, or service needs to function to meet
981 stakeholders' desired privacy outcomes (e.g., "the application is configured to allow users to
982 select specific data elements"). To define privacy requirements, consider organizational-level
983 privacy requirements (see Organizing Preparatory Resources above) and the outputs of a
984 privacy risk assessment. This process helps an organization to answer two questions: 1) What
985 can a system, product, or service do with data processing and interactions with individuals? 2)
986 What should it do? Then an organization can allocate resources to design a system, product, or
987 service in a way that achieves the defined requirements. Ultimately, defining privacy
988 requirements can lead to the development of systems, products, and services that are more
989 mindful of individuals' privacy, and are based on informed risk decisions.

990 ## Conducting Privacy Risk Assessments

991 Conducting a privacy risk assessment helps an organization to identify privacy risks engendered
992 by the system, product, or service and prioritize them to be able to make informed decisions
993 about how to respond to the risks consistent with the organization's overall risk management

[21] The privacy engineering objectives are adapted from NIST IR 8062 [4]. The security objectives are from NIST SP 800-37, Rev. 2 [8].

strategy (ID.RA-P, GV.RM-P). Methodologies for conducting privacy risk assessments may vary, but organizations should consider the following characteristics:[22]

- **Risk model** (ID.RA-P, GV.MT-P1)

  Risk models define the risk factors to be assessed and the relationships among those factors.[23] If an organization is not using a pre-defined risk model, an organization should clearly define which risk factors it will be assessing and the relationships among these factors. Although cybersecurity has a widely used risk model based on the risk factors of threats, vulnerabilities, likelihood, and impact, there is not one commonly accepted privacy risk model. NIST has developed a privacy risk model to calculate risk based on the likelihood of a problematic data action multiplied by the impact of a problematic data action; each of the three risk factors are explained below.

  **Privacy Risk Factors:**
  Problematic Data Action | Likelihood | Impact

  - A problematic data action is any action a system takes to process data that could result in a problem for individuals. Organizations consider the type of problems that are relevant to the population of individuals. Problems can take any form and may consider the experience of individuals.[24]
  - Likelihood is defined as a contextual analysis that a data action is likely to create a problem for a representative set of individuals. Context can include organizational factors (e.g., geographic location, the public perception about participating organizations with respect to privacy), system factors (e.g., the nature and history of individuals' interactions with the system, visibility of data processing to individuals and third parties), or individual factors (e.g., individuals' demographics, privacy interests or perceptions, data sensitivity).[25] A data map can help with this contextual analysis (see Organizing Preparatory Resources).
  - Impact is an analysis of the costs should the problem occur. As noted in section 1.2, organizations do not experience these problems directly. Moreover, individuals' experiences may be subjective. Thus, impact may be difficult to assess accurately. Organizations should consider the best means of internalizing impact to individuals in order to appropriately prioritize and respond to privacy risks.[26]

[22] NIST has developed a Privacy Risk Assessment Methodology (PRAM) that can help organizations identify, assess, and respond to privacy risks. It is comprised of a set of worksheets available at [2].
[23] See NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments* [13] at p. 8.
[24] As part of its PRAM, NIST has created an illustrative catalog of problematic data actions and problems for consideration [2]. Other organizations may have created additional problem sets, or may refer to them as adverse consequences or harms.
[25] See NIST PRAM for more information about contextual factors. Id. at Worksheet 2.
[26] The NIST PRAM uses organizational costs such as non-compliance costs, direct business costs, reputational costs, and internal culture costs as drivers for considering how to assess individual impact. Id. at Worksheet 3, Impact Tab.

- **Assessment approach**

  The assessment approach is the mechanism by which identified risks are prioritized. Assessment approaches can be categorized as quantitative, semi-quantitative, or qualitative.[27] [28]

- **Prioritizing risks** (ID.RA-P4)

  Given the applicable limits of an organization's resources, organizations prioritize the risks to facilitate communication about how to respond.[29]

- **Responding to risks** (ID.RA-P5)

  As described in section 1.2.2, response approaches include mitigation, transfer/sharing, avoidance, or acceptance.[30]

## Creating Privacy Requirements Traceability

Once an organization has determined which risks to mitigate, it can refine the privacy requirements and then select and implement controls (i.e., technical, physical, and/or policy safeguards) to meet the requirements [8]. An organization may use a variety of sources to select controls, such as NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations [11].* After implementation, an organization iteratively assesses the controls for their effectiveness in meeting the privacy requirements and managing privacy risk. In this way, an organization creates traceability between the controls and the privacy requirements, and demonstrates accountability between its systems, products, and services and its organizational privacy goals.

## Monitoring Change

Privacy risk management is not a static process. An organization monitors how changes in its business environment—including new laws and regulations and emerging technologies—and corresponding changes to its systems, products, and services may be affecting privacy risk, and iteratively uses the practices in this appendix to adjust accordingly (GV.MT-P1).

## Supporting Effective Oversight

Organization-wide privacy risk management outcomes, activities, and performance are used to inform, improve, and adjust the organization's overall risk management strategy. An organization reviews its privacy risk management strategy outcomes and measures its privacy risk management performance to adjust its strategic direction and ensure privacy risk management sufficiently addresses organizational requirements and risks (GV.OV-P).

[27] See NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments* at [13] p. 14.
[28] The NIST PRAM uses a semi-quantitative approach based on a scale of 1-10.
[29] The NIST PRAM provides various prioritization representations, including a heat map. See [2] Worksheet 3.
[30] The NIST PRAM provides a process for responding to prioritized privacy risks. See [2] at Worksheet 4.

## Appendix E. Tiers Definitions

The four Tiers summarized below are each defined with four elements:

### Tier 1: Partial

- **Privacy Risk Management Process** – Organizational privacy risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner. Prioritization of privacy activities may not be directly informed by organizational risk management priorities, privacy risk assessments, or mission or business objectives.
- **Integrated Privacy Risk Management Program** – There is limited awareness of privacy risk at the organizational level. The organization implements privacy risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable the sharing of information about data processing and resulting privacy risks within the organization.
- **Data Processing Ecosystem Relationships** – There is limited understanding of an organization's role(s) in the larger ecosystem with respect to other entities (e.g., buyers, suppliers, service providers, business associates, partners). The organization does not have processes for identifying how privacy risks may proliferate throughout the ecosystem or for communicating privacy risks or requirements to other entities in the ecosystem.
- **Workforce** – Some personnel may have a limited understanding of privacy risks or privacy risk management processes, but have no specific privacy responsibilities. If available, privacy training is ad hoc and the content is not kept current with best practices.

### Tier 2: Risk Informed

- **Privacy Risk Management Process** – Risk management practices are approved by management but may not be established as organization-wide policy. Prioritization of privacy activities is directly informed by organizational risk management priorities, privacy risk assessments, or mission or business objectives.
- **Integrated Privacy Risk Management Program** – There is an awareness of privacy risk at the organizational level, but an organization-wide approach to managing privacy risk has not been established. Information about data processing and resulting privacy risks is shared within the organization on an informal basis. Consideration of privacy in organizational objectives and programs may occur at some but not all levels of the organization. Privacy risk assessment occurs, but is not typically repeatable or reoccurring.
- **Data Processing Ecosystem Relationships** – There is some understanding of an organization's role(s) in the larger ecosystem with respect to other entities (e.g., buyers, suppliers, service providers, business associates, partners). The organization is aware of the privacy ecosystem risks associated with the products and services it provides and uses, but does not act consistently or formally upon those risks.

- **Workforce** – There are personnel with specific privacy responsibilities, but they may have non-privacy responsibilities as well. Privacy training is conducted regularly for privacy personnel, although there is no consistent process for updates on best practices.

### Tier 3: Repeatable

- **Privacy Risk Management Process** – The organization's risk management practices are formally approved and expressed as policy. Organizational privacy practices are regularly updated based on the application of risk management processes to changes in mission or business objectives and a changing risk, policy, and technology landscape.
- **Integrated Privacy Risk Management Program** – There is an organization-wide approach to manage privacy risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. The organization consistently and accurately monitors privacy risk. Senior privacy and non-privacy executives communicate regularly regarding privacy risk. Senior executives ensure consideration of privacy through all lines of operation in the organization.
- **Data Processing Ecosystem Relationships** – The organization understands its role(s), dependencies, and dependents in the larger ecosystem and may contribute to the community's broader understanding of risks. The organization is aware of the privacy ecosystem risks associated with the products and services it provides and it uses. Additionally, it usually acts formally upon those risks, including mechanisms such as written agreements to communicate privacy requirements, governance structures, and policy implementation and monitoring.
- **Workforce** – Dedicated privacy personnel possess the knowledge and skills to perform their appointed roles and responsibilities. There is regular, up-to-date privacy training for all personnel.

### Tier 4: Adaptive

- **Privacy Risk Management Process** – The organization adapts its privacy practices based on lessons learned from privacy events, and identification of new privacy risks. Through a process of continuous improvement incorporating advanced privacy technologies and practices, the organization actively adapts to a changing policy and technology landscape and responds in a timely and effective manner to evolving privacy risks.
- **Integrated Privacy Risk Management Program** – There is an organization-wide approach to managing privacy risk that uses risk-informed policies, processes, and procedures to address problematic data actions. The relationship between privacy risk and organizational objectives is clearly understood and considered when making decisions. Senior executives monitor privacy risk in the same context as cybersecurity risk, financial risk, 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. Privacy risk management is part of the

organizational culture and evolves from lessons learned and continuous awareness of data processing and resulting privacy risks. The organization can quickly and efficiently account for changes to business/mission objectives in how risk is approached and communicated.

- **Data Processing Ecosystem Relationships** – The organization understands its role(s), dependencies, and dependents in the larger ecosystem and contributes to the community's broader understanding of risks. The organization uses real-time or near-real-time information to understand and consistently act upon privacy ecosystem risks associated with the products and services it provides and it uses. Additionally, it communicates proactively, using formal (e.g., agreements) and informal mechanisms to develop and maintain strong ecosystem relationships.
- **Workforce** – The organization has specialized privacy skillsets throughout the organizational structure; personnel with diverse perspectives contribute to the management of privacy risks. There is regular, up-to-date, specialized privacy training for all personnel. Personnel at all levels understand the organizational privacy values and their role in maintaining them.