NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT

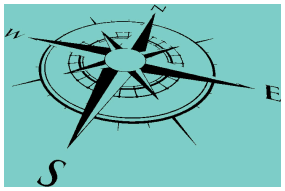
Following a transparent, consensus-based process including both private and public stakeholders to produce this voluntary tool, the National Institute of Standards and Technology (NIST) is publishing this Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management (Privacy Framework), to enable better privacy engineering practices that support privacy by design concepts and help organizations protect individuals' privacy. 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;1
- 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.

The Privacy Framework follows the structure of the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) [1] to facilitate the use of both frameworks together. Like the Cybersecurity Framework, the Privacy Framework is composed of three parts: Core, Profiles, and Implementation 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.
- Profiles enable the prioritization of the outcomes and activities that best meet organizational privacy values, mission or business needs, and risks.
- Implementation Tiers support decision-making and communication about the sufficiency of organizational processes and resources to manage privacy risk.

Contents



National Institute of Standards and Technology (NIST)

Vision

Better privacy engineering practices.

Mission

To help organizations build better privacy foundations by bringing privacy risk into parity with their broader enterprise risk portfolio.

Values

Predictability: Enabling reliable assumptions by individuals, owners, and operators about data and their processing by a system

Manageability: Providing the capability for granular administration of data, including collection, alteration, deletion, and selective disclosure

Disassociability: Enabling the processing of data or events without association to individuals or devices beyond the operational requirements of the system

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

Integrity: Guarding against improper information modification or destruction; includes ensuring information non-repudiation and authenticity

Availability: Ensuring timely and reliable access to and use of information

1. Core

Communicate prioritized privacy protection activities and outcomes across an organization.

Stakeholder(s)

Organizational Stakeholders :

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).

Workforce :

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.

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... 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. 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.12 Protect-P is specifically focused on managing risks associated with cybersecurity-related privacy events (e.g., privacy breaches). The Cybersecurity Framework, 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 Detect, Respond, and Recover Functions. Alternatively, organizations may use all five of the Cybersecurity Framework Functions in conjunction with Identify-P, Govern-P, Control-P, and Communicate-P to collectively address privacy and cybersecurity risks. Figure 5 uses the Venn diagram from section 1.2.1 to demonstrate how the Functions from both frameworks can be used in varying combinations to manage different aspects of privacy and cybersecurity risks. The five Privacy Framework Functions are defined as follows:

1.1. 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.

1.2. 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.

1.3. 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.

1.4. 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.

1.5. 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. Profiles

Determine which outcomes are most important.

A Profile represents an organization's current privacy activities or desired outcomes. To develop a Profile, an organization can review all of 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. — 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. The Privacy Framework does not prescribe Profile templates to allow for flexibility in implementation. Under the Privacy Framework's riskbased 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 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 in order 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 common Profiles.

3. Implementation

Provide a point of reference on how an organization views privacy risk.

Implementation Tiers ("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 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. — Tiers support organizational decision-making about how to manage privacy risk by taking into account 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. 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, and its workforce composition and training program. There are four distinct Tiers, Partial (Tier 1), Risk Informed (Tier 2), Repeatable (Tier 3), and Adaptive (Tier 4), descriptions of which are in Appendix E. The Tiers represent a progression, albeit not a compulsory one. 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.

4. Usage

Use the privacy framework.

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 the development of 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 impacts to individuals 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. The decision about how to apply it is left to the implementing organization. For example, an organization may already have robust privacy risk management processes, but may use the Core's five Functions as a streamlined way to analyze and articulate any gaps. 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. The following subsections present a few options for use of the Privacy Framework.

4.1. References

Map to informative references.

Informative references are mappings to Subcategories to provide implementation support, including mappings of tools, technical guidance, standards, laws, regulations, and best practices. Crosswalks that map the provisions of standards, laws, and regulations to Subcategories can help organizations determine which activities or outcomes to prioritize to facilitate compliance. The Privacy Framework is technology neutral, but it supports technological innovation because any organization or industry sector can develop these mappings as technology and related business needs evolve. By relying on consensus-based standards, guidelines, and practices, the tools and methods available to achieve positive privacy outcomes can scale across borders and accommodate the global nature of privacy risks. The use of existing and emerging standards will enable economies of scale and drive the development of systems, products, and services that meet identified market needs while being mindful of the privacy needs of individuals. Gaps in mappings can also be used to identify where additional or revised standards, guidelines, and practices would help an organization to address emerging needs. An organization implementing a given Subcategory, or developing a new Subcategory, might discover that there is insufficient guidance for a related activity or outcome. To address that need, an organization might collaborate with technology leaders and/or standards bodies to draft, develop, and coordinate standards, guidelines, or practices. A repository of informative references can be found at https://www.nist.gov/privacy-framework These resources can support organizations' use of the Privacy Framework and achievement of better privacy practices.

4.2. Accountability

Strengthen accountability.

Accountability is generally considered a key privacy principle, although conceptually it is not unique to privacy.13 Accountability occurs throughout an organization, and it can be expressed at varying degrees of abstraction, for example as a cultural value, as governance policies and procedures, or as traceability relationships between privacy requirements and controls. Privacy risk management can be a means of supporting accountability at all organizational levels as it connects senior executives, who can communicate an organization's privacy values and risk tolerance, to those at the business/process manager level, who can collaborate on the development and implementation of governance policies and procedures that support organizational privacy values. These policies and procedures can then be communicated to those at the implementation/operations level, who collaborate on defining the privacy requirements that support the expression of the policies and procedures in an organization's systems, products, and services. Personnel at the

implementation/operations level also select, implement, and assess controls as the technical and policy measures that meet the privacy requirements, and report on progress, gaps and deficiencies, incident management, and changing privacy risks so that those at the business/process manager level and the senior executives can better understand and respond appropriately. Figure 7 provides a graphical representation of this bi-directional collaboration and communication and how elements of the Privacy Framework can be incorporated to facilitate the process. In this way, organizations can use the Privacy Framework as a tool to support accountability. They can also use the Privacy Framework in conjunction with other frameworks and guidance that provide additional practices to achieve accountability within and between organizations. 14

4.3. Program

Establish or improve a privacy program.

Using a simple model of "ready, set, go" phases, the Privacy Framework can support the creation of a new privacy program or improvement of an existing program. As an organization goes through these phases, it may use informative references to provide guidance on prioritizing or achieving outcomes. See section 3.1 for more information about informative references. In addition, a repository can be found at https://www.nist.gov/privacy-framework

4.3.1. Understanding

Understand the organization's mission or business environment, legal environment, risk tolerance, privacy risks, and data processing role(s).

Ready — Effective privacy risk management requires an organization to understand its mission or business environment; its legal environment; its risk tolerance; the privacy risks engendered by its systems, products, or services; and its role(s) in the data processing ecosystem. An organization can use the Identify-P and Govern-P Functions to "get ready" by reviewing the Categories and Subcategories, and beginning to develop its Current Profile and Target Profile.15 Activities and outcomes such as establishing organizational privacy values and policies, determining and expressing an organizational risk tolerance, and conducting privacy risk assessments (see Appendix D for more information on privacy risk assessments) provide a foundation for completing the Profiles in "Set."

4.3.2. Outcomes

Indicate which Category and Subcategory outcomes from the remaining Functions are being achieved.

Set — An organization completes its Current Profile by indicating which Category and Subcategory outcomes from the remaining Functions are being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps by providing baseline information. Informed by the activities under Identify and Govern, such as organizational privacy values and policies, organizational risk tolerance, and privacy risk assessment results, an organization completes its Target Profile focused on the assessment of the Categories and Subcategories describing its desired privacy outcomes. An organization also may develop its own additional Functions, Categories, and Subcategories to account for unique organizational risks. It may also consider influences and requirements of external stakeholders such as business customers and partners when creating a Target Profile. An organization can develop multiple Profiles to support its different business lines or processes, which may have different business needs and associated risk tolerances. An organization compares the Current Profile and the Target Profile to determine gaps. Next, it creates a prioritized action plan to address gaps—reflecting mission drivers, costs and benefits, and risks—to achieve the outcomes in the Target Profile. An organization using the Cybersecurity Framework and the Privacy Framework together may develop integrated action plans. It then determines resources, including funding and workforce needs, necessary to address the gaps, which can inform the selection of an appropriate Tier. Using Profiles in this manner encourages an

organization to make informed decisions about privacy activities, supports risk management, and enables an organization to perform cost-effective, targeted improvements.

4.3.3. Prioritization

Prioritize actions to take to address gaps.

Go — With the action plan "set," an organization prioritizes which actions to take to address any gaps, and then adjusts its current privacy practices in order to achieve the Target Profile.16 An organization can go through the phases nonsequentially as needed to continuously assess and improve its privacy posture. For instance, an organization may find that more frequent repetition of the Ready phase improves the quality of privacy risk assessments. Furthermore, an organization may monitor progress through iterative updates to the Current Profile or the Target Profile to adjust to changing risks, subsequently comparing the Current Profile to the Target Profile.

4.4. SDLC

Align the Target Profile with the system development life cycle (SDLC).

Applying to the System Development Life Cycle — The Target Profile can be aligned with the system development life cycle (SDLC) phases of plan, design, build/buy, deploy, operate, and decommission to support the achievement of the prioritized privacy outcomes. 17 Beginning with the plan phase the prioritized privacy outcomes can be transformed into the privacy capabilities and requirements for the system, recognizing that requirements are likely to evolve during the remainder of the life cycle. A key milestone of the design phase is validating that the privacy capabilities and requirements match the needs and risk tolerance of an organization as expressed in the Target Profile. That same Target Profile can serve as an internal list to be assessed when deploying the system to verify that all privacy capabilities and requirements are implemented. The privacy outcomes determined by using the Privacy Framework should then serve as a basis for ongoing operation of the system. This includes occasional reassessment, capturing results in a Current Profile, to verify that privacy capabilities and requirements are still fulfilled. Privacy risk assessments typically focus on the data life cycle, the stages through which data passes, often characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion. Aligning the SDLC and the data lifecycle by identifying and understanding how data are processed during all stages of the SDLC helps organizations to better manage privacy risks and informs the selection and implementation of privacy controls to meet privacy requirements.

4.5. Data Processing

Develop Profiles relevant to role(s).

Using within the Data Processing Ecosystem — A key factor in the management of privacy risk is an entity's role(s) in the data processing ecosystem, which can affect not only its legal obligations, but also the measures it may take to manage privacy risk. As depicted in Figure 8, the data processing ecosystem encompasses a range of entities and roles that may have complex, multi-directional relationships with each other and individuals. Complexity can increase when entities are supported by a chain of sub-entities; for example, service providers may be supported by a series of service providers, or manufacturers may have multiple component suppliers. Figure 8 displays entities as having distinct roles, but some may have multiple roles, such as an organization providing services to other organizations and providing retail products to consumers. The roles in Figure 8 are intended to be notional classifications. In practice, an entity'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 sector designations. By developing one or more Profiles relevant to its role(s), an entity can use the Privacy Framework to consider how to manage privacy risk not only with regard to its own priorities, but also in relation to how the measures it may take affect other data processing ecosystem entities' management of privacy

risk. For example: • An organization that makes decisions about how to collect and use data about individuals may use a Profile to express privacy requirements to an external service provider (e.g., a cloud provider to which it is exporting data); the external service provider that processes the data may use its Profile to demonstrate the measures it has adopted to process data in line with contractual obligations. • An organization may express its privacy posture through a Current Profile to report results or to compare with acquisition requirements. • An industry sector may establish a common Profile that can be used by its members to customize their own Profiles. • A manufacturer may use a Target Profile to determine the capabilities to build into its products so that its business customers can meet the privacy needs of their end users. • A developer may use a Target Profile to consider how to design an application that enables privacy protections when used within other organizations' system environments. ^ The Privacy Framework provides a common language to communicate privacy requirements with entities within the data processing ecosystem. The need for this communication can be particularly notable when the data processing ecosystem crosses national boundaries, such as with international data transfers. Organizational practices that support communication may include: • Determining privacy requirements; • Enacting privacy requirements through formal agreement (e.g., contracts, multi-party frameworks); • Communicating how those privacy requirements will be verified and validated; • Verifying that privacy requirements are met through a variety of assessment methodologies; and • Governing and managing the above activities.

Stakeholder(s):

Public / Government Services	Developer
Individuals	Business Associates or Partners
Civil Society	Supplier or Service Provider
Research / Education	Manufacturer
Commercial Product / Services	

4.6. Purchasing Decisions

Use the Profiles to inform decisions about buying products and services.

Informing Buying Decisions — Since either a Current or Target Profile can be used to generate a prioritized list of privacy requirements, these Profiles can also be used to inform decisions about buying products and services. By first selecting outcomes that are relevant to its privacy goals, an organization then can evaluate partners' systems, products, or services against this outcome. For example, if a device is being purchased for environmental monitoring of a forest, manageability may be important to support capabilities for minimizing the processing of data about people using the forest and should drive a manufacturer evaluation against applicable Subcategories in the Core (e.g., CT.DP-P4: system or device configurations permit selective collection or disclosure of data elements). In circumstances where it may not be possible to impose a set of privacy requirements on the supplier, the objective should be to make the best buying decision among multiple suppliers, given a carefully determined list of privacy requirements. Often, this means some degree of trade-off, comparing multiple products or services with known gaps to the Profile. If the system, product, or service purchased did not meet all of the objectives described in the Profile, an organization could address the residual risk through mitigation measures or other management actions.

Administrative Information

Start Date: 2020-01-16
End Date:

Publication Date: 2020-01-17
Source: https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf

Submitter:

Given Name: **Surname:**
Email: **Phone:**