

1  
2  
3

## **DISCUSSION DRAFT**

# NIST PRIVACY FRAMEWORK: AN ENTERPRISE RISK MANAGEMENT TOOL

April 30, 2019

## 4 Note to Reviewers

5 This document is provided for discussion purposes to promote the development of the NIST Privacy  
6 Framework: An Enterprise Risk Management Tool (Privacy Framework). NIST will use feedback on this  
7 discussion draft to develop a preliminary draft of the Privacy Framework.

8 **Structure:** Based on stakeholder feedback, this discussion draft is aligned with the structure of the  
9 Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) to support  
10 compatibility between the two frameworks. Feedback also supported use of additional organizing  
11 constructs referenced in NIST's Request for Information, such as privacy principles (e.g., the Fair  
12 Information Practice Principles), the information life cycle, and the NIST privacy engineering objectives  
13 (i.e., predictability, manageability, disassociability) or other constructs.<sup>1</sup> NIST welcomes feedback on  
14 how well these concepts have been integrated, as well as whether the Privacy Framework could be  
15 effectively implemented independently or in conjunction with the Cybersecurity Framework.

16 **Privacy Risk Management:** Based on feedback indicating a lack of a consistent or widespread  
17 understanding of privacy risks and privacy risk management, this discussion draft provides guidance on  
18 these topics in section 1.2 and Appendix D. NIST welcomes feedback on whether this guidance will be  
19 useful to organizations.

20 **Core:** This discussion draft provides a proposed Core, including functions, categories, and subcategories.  
21 NIST welcomes feedback on the Core, particularly regarding (i) gaps in, clarifications to, or usefulness of  
22 the categories and subcategories, (ii) organization of the functions, categories, and subcategories, and  
23 (iii) areas that need further development and may be more appropriate for the Roadmap section in  
24 Appendix F.

25 **Informative References:** This discussion draft defines informative references as specific sections of  
26 standards, guidelines, and practices that can be mapped to the Core subcategories and support  
27 achievement of the subcategory outcomes. In an effort to increase contributions of informative  
28 references and simplify updating, NIST is providing a mapping of the Core to relevant NIST guidance as a  
29 separate, companion document to this discussion draft. In addition, NIST will develop a process for  
30 accepting external informative references. NIST welcomes feedback regarding this approach to  
31 informative references.

32 **Overall Discussion Draft:** In general, NIST is interested in whether the Privacy Framework as proposed in  
33 this discussion draft could be readily usable as part of an enterprise's broader risk management  
34 processes and scalable to organizations of various sizes—and if not, how it could be improved to suit a  
35 greater range of organizations. Although these notes highlight key areas of interest, all feedback is  
36 welcome.

37 Please send feedback on this discussion draft to [privacyframework@nist.gov](mailto:privacyframework@nist.gov).

38

---

<sup>1</sup> See Federal Register Notice 83 FR 56824, *Developing a Privacy Framework* at <https://www.federalregister.gov/documents/2018/11/14/2018-24714/developing-a-privacy-framework>.

39 [Table of Contents](#)

40 **Note to Reviewers**.....1

41 **Executive Summary**.....3

42 **Acknowledgements**.....3

43 **1.0 Privacy Framework Introduction** .....3

44 1.1 Overview of the Privacy Framework ..... 4

45 1.2 Privacy Risk Management ..... 4

46 1.2.1 Cybersecurity and Privacy Risk Management ..... 5

47 1.2.2 Relationship Between Privacy Risk Management and Risk Assessment ..... 6

48 1.3 Document Overview ..... 7

49 **2.0 Privacy Framework Basics** .....8

50 2.1 Core ..... 8

51 2.2 Profile ..... 9

52 2.3 Implementation Tiers..... 10

53 **3.0 How to Use the Privacy Framework**.....10

54 3.1 Informative References..... 11

55 3.2 Strengthening Accountability..... 11

56 3.3 Basic Review of Privacy Practices..... 12

57 3.4 Establishing or Improving a Privacy Program ..... 13

58 3.5 Application in the System Development Life Cycle ..... 14

59 3.6 Communicating Privacy Requirements with Stakeholders ..... 15

60 3.7 Buying Decisions..... 16

61 **Appendix A: Privacy Framework Core** .....17

62 **Appendix B: Glossary** .....27

63 **Appendix C: Acronyms**.....29

64 **Appendix D: Privacy Risk Management Practices** .....30

65 **Appendix E: Implementation Tiers Definitions**.....35

66 **Appendix F: Roadmap** .....37

68 [List of Figures](#)

69 **Figure 1: Cybersecurity and Privacy Risk Relationship** ..... 5

70 **Figure 2: Cybersecurity Framework and Privacy Framework Functions Relationship** ..... 6

71 **Figure 3: Privacy Framework Core Structure** ..... 8

72 **Figure 4: Notional Information and Decision Flows within an Organization**..... 12

73 **Figure 5: Ecosystem Relationships** ..... 16

75 [List of Tables](#)

76 **Table 1: Privacy Framework Function and Category Unique Identifiers**..... 17

77 **Table 2: Privacy Framework Core**..... 19

78 **Table 3: Privacy Engineering and Security Objectives** ..... 32

## 80 Executive Summary

81 *The Executive Summary will be included in the preliminary draft.*

## 82 Acknowledgements

83 *Acknowledgements will be included in the preliminary draft.*

## 84 1.0 Privacy Framework Introduction

85 For more than two decades in the United States and across the world, the Internet and associated  
86 information technologies have driven unprecedented innovation, economic value, and access to social  
87 services. Many of these benefits are fueled by data about individuals that flow through a complex  
88 ecosystem—so complex that individuals may not be able to understand or attend to the potential  
89 consequences for privacy resulting from their interactions with systems, products, and services.  
90 Similarly, organizations may not fully realize the consequences either. Failure to manage privacy risks  
91 can have direct adverse consequences for people at both the individual and societal level, with  
92 secondary effects on organizations and economic growth. Finding ways to continue to derive benefits  
93 from data while simultaneously protecting individuals' privacy is challenging, and not well-suited to one-  
94 size-fits-all solutions.

95 Approaches to Privacy are challenging because it is an all-encompassing concept. It is a condition or  
96 state that safeguards important values such as human autonomy and dignity, yet the means for  
97 achieving it vary. For example, in some circumstances it can be achieved through obscurity, in other  
98 circumstances through individuals' control of various facets of their identities (e.g. body, data,  
99 reputation).<sup>2</sup> Moreover, human autonomy and dignity are not fixed, quantifiable constructs; they are  
100 mediated through cultural diversity and individual differences. This broad and shifting nature of privacy  
101 makes it difficult to communicate clearly about privacy risks within and between organizations and with  
102 individuals. What has been missing is a shared lexicon and practical structure that is flexible enough to  
103 address diverse privacy needs.

104 To enable innovation and increase trust in systems, products and services, NIST has developed the  
105 voluntary NIST Privacy Framework: An Enterprise Risk Management Tool (Privacy Framework) to help  
106 organizations consider:

- 107
- How their systems, products, and services affect individuals; and
  - How to integrate privacy practices into their organizational processes that result in effective  
108 solutions to mitigate these impacts and protect individuals' privacy.
- 109

110 The Privacy Framework has been developed to improve privacy risk management for organizations  
111 delivering or using *data processing* systems, products, or services in any sector of the economy or  
112 society, regardless of their focus or size. The common taxonomy that it provides is neither country- nor  
113 region-specific. Organizations outside the United States may also use the Privacy Framework to  
114 strengthen their own privacy efforts, and ideally, it can contribute to developing a common language for  
115 international cooperation on privacy.

---

<sup>2</sup> For more information, see Daniel Solove, *Understanding Privacy*, Harvard University Press, 2010; and Evan Selinger and Woodrow Hartzog, "Obscurity and Privacy," *Routledge Companion to Philosophy of Technology*, 2014, at <https://ssrn.com/abstract=2439866>.

## 116 1.1 Overview of the Privacy Framework

117 The Privacy Framework is composed of three parts: the Core, the Profiles, and the Implementation Tiers.  
118 Each component reinforces privacy risk management through the connection between business/mission  
119 drivers and privacy protection activities. These components are explained in more detail in section 2.0,  
120 but as an overview:

- 121 • The *Core* is a set of privacy protection activities and desired outcomes that allows for  
122 communicating prioritized privacy protection activities and outcomes across the organization  
123 from the executive level to the implementation/operations level. The Core consists of five  
124 concurrent and continuous functions—*Identify, Protect, Control, Inform, and Respond*. Together  
125 these functions provide a high-level, strategic view of the life cycle of an organization’s  
126 management of privacy risk. The Core then identifies underlying key categories and  
127 subcategories—which are discrete outcomes—for each function.
- 128 • A *Profile* represents the privacy outcomes the organization aims to achieve. To develop a Profile,  
129 an organization can review all of the functions, categories, and subcategories to determine  
130 which are most important to achieving the desired privacy outcomes, based on  
131 business/mission drivers, types of data processing, and individuals’ privacy needs. The  
132 organization can create or add functions, categories, and subcategories as needed. Profiles can  
133 be used to identify opportunities for improving privacy posture by comparing a “Current” Profile  
134 (the “as is” state) with a “Target” Profile (the “to be” state). Profiles can be used to conduct self-  
135 assessments and to communicate within an organization or between organizations about how  
136 privacy risks are being managed.
- 137 • *Implementation Tiers* (“Tiers”) provide context on how an organization views privacy risk and  
138 whether it has adequate processes and resources in place to manage that risk. Tiers reflect a  
139 progression from informal, reactive responses to approaches that are agile and risk-informed.  
140 When selecting Tiers, an organization should consider its current risk management practices; its  
141 data processing systems, products, or services; legal and regulatory requirements;  
142 business/mission objectives; organizational privacy values and individuals’ privacy needs; and  
143 organizational constraints.

## 144 1.2 Privacy Risk Management

145 *Risk management* is the ongoing set of processes for identifying, assessing, and responding to risk. To  
146 manage risk, organizations should seek to understand the likelihood that an event will occur and the  
147 potential impacts. While some organizations have a robust grasp of the underlying processes and  
148 resources needed to identify, assess, and respond to privacy risks, a common understanding of many  
149 aspects of privacy risk management is still not widespread.<sup>3</sup> To promote broader understanding, this  
150 section covers concepts and considerations that organizations may use to develop, improve, or  
151 communicate about their privacy risk management. Appendix D provides additional guidance on key  
152 privacy risk management practices.

---

<sup>3</sup> See *Summary Analysis of the Responses to the NIST Privacy Framework Request for Information* at p. 7  
[https://www.nist.gov/sites/default/files/documents/2019/02/27/rfi\\_response\\_analysis\\_privacyframework\\_2.27.19.pdf](https://www.nist.gov/sites/default/files/documents/2019/02/27/rfi_response_analysis_privacyframework_2.27.19.pdf)

153 1.2.1 Cybersecurity and Privacy Risk Management

154 Since its release in 2014, the Framework  
 155 for Improving Critical Infrastructure  
 156 Cybersecurity (Cybersecurity Framework)  
 157 has helped organizations to  
 158 communicate and manage cybersecurity  
 159 risk.<sup>4</sup> While managing cybersecurity risk  
 160 contributes to managing privacy risk, it is  
 161 not sufficient as privacy risks can also  
 162 arise outside the scope of cybersecurity  
 163 risks. **Figure 1** illustrates how NIST  
 164 considers the overlap and differences  
 165 between cybersecurity and privacy risks.  
 166 Cybersecurity risks arise from  
 167 unauthorized activity related to the loss  
 168 of confidentiality, integrity, or availability of a system or information asset. However, privacy risks arise  
 169 as a byproduct of intentional (i.e., authorized) data processing occurring in systems, products, and  
 170 services that help organizations to achieve their mission/business objectives. This data processing can  
 171 lead to unintended problems or adverse consequences for individuals.<sup>5</sup> An example is the concerns that

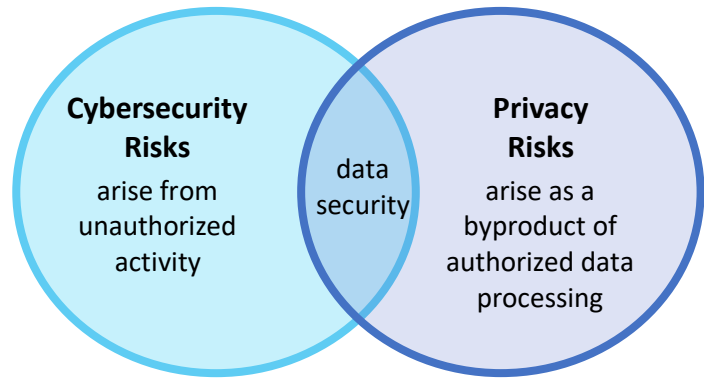


Figure 1: Cybersecurity and Privacy Risk Relationship

**Data Processing**

An operation or set of operations performed upon data across the full data life cycle, including but not limited to the collection, retention, logging, generation, transformation, use, disclosure, transfer, and disposal of data.

certain communities had about the installation of “smart meters” as part of the Smart Grid, a nationwide technological effort to increase energy efficiency.<sup>6</sup> 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.<sup>7</sup> The meters were operating as intended, but the data processing could lead to unintended consequences that people might feel surveilled.

Individuals can also experience problems or adverse consequences if the data being processed is subject to a loss of confidentiality, integrity, and availability. Figure 1 shows this data security issue as an overlap between managing cybersecurity and privacy risks.

Thus, *privacy risk* can be understood as the likelihood that individuals will experience problems resulting from data processing,

<sup>4</sup> See *Framework for Improving Critical Infrastructure Cybersecurity* at <https://doi.org/10.6028/NIST.CSWP.04162018>.

<sup>5</sup> NIST has created an illustrative problem set with problems that can range, for example, from embarrassment to discrimination, to economic loss and physical harm), see *NIST Privacy Risk Assessment Methodology* at <https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources>. Other organizations may have created additional problem sets, or may refer to them as adverse consequences or harms.

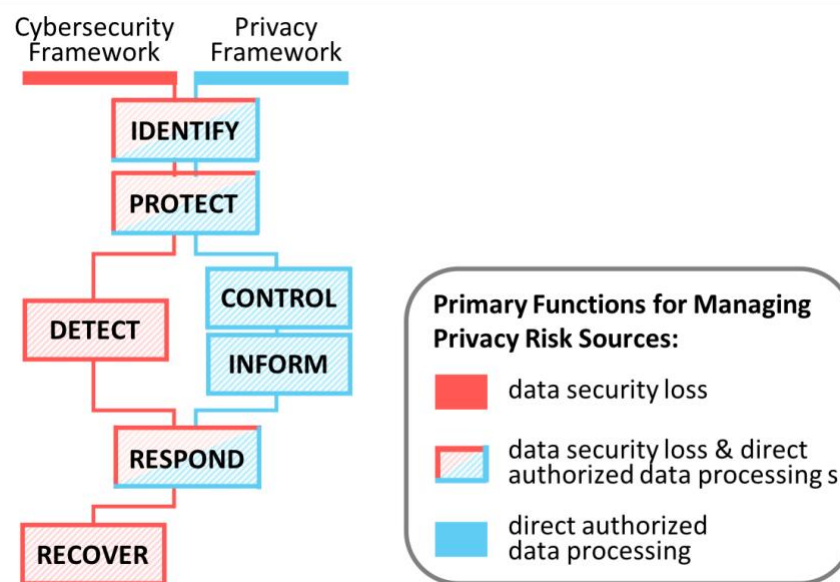
<sup>6</sup> See e.g., NISTIR 7628 Revision 1 Volume 1, *Guidelines for Smart Grid Cybersecurity: Volume 1 – Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements* at p. 26 <https://doi.org/10.6028/NIST.IR.7628r1>.

<sup>7</sup> See NIST Internal Report (NISTIR) 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems* at p. 2 <https://doi.org/10.6028/NIST.IR.8062>. For additional types of privacy risks arising from authorized data processing, see Appendix E of NISTIR 8062.

185 and the impact should they occur.<sup>8</sup> Organizations typically determine the acceptable level of risk for  
 186 achieving their organizational objectives and can express this as their risk tolerance. Privacy risk adds a  
 187 layer of complexity to the determination of risk tolerance because it manifests as an externality—  
 188 individuals, not organizations, experience the direct impact of the problems. Privacy risk management  
 189 should help organizations to internalize consideration of these impacts to individuals, and appropriately  
 190 account for them in their determination of risk tolerance. With an understanding of risk tolerance,  
 191 organizations can better prioritize privacy activities, enabling organizations to make informed decisions  
 192 about budgets and other resource allocations.

193 Given the relationship between privacy and cybersecurity, organizations may opt to use the  
 194 Cybersecurity Framework and the Privacy Framework together. **Figure 2** illustrates how the five  
 195 functions in those frameworks relate to each other.<sup>9</sup> While not exclusive:

- 196 • Identify, Protect, and Respond can be used to manage privacy risks whether they arise from loss  
 197 of data security or more directly from authorized data processing;
- 198 • Detect and Recover can be used to manage privacy risks arising from loss of data security; and
- 199 • Control and Inform can be used to manage privacy risks arising directly from authorized data  
 200 processing.



201

202

Figure 2: Cybersecurity Framework and Privacy Framework Functions Relationship

### 203 1.2.2 Relationship Between Privacy Risk Management and Risk Assessment

204 Privacy risk management is a cross-organizational set of processes that helps organizations to  
 205 understand how their systems, products, and services may create problems for individuals and how to  
 206 develop effective solutions to manage such risks. *Privacy risk assessment* is a sub-process for identifying,  
 207 evaluating, prioritizing, and responding to specific privacy risks engendered by systems, products, or

<sup>8</sup> Id at p. 21

<sup>9</sup> Although the Privacy Framework can be used independently, modeling the structural design of the Core, Profiles, and Tiers after the Cybersecurity Framework allows the two frameworks to be used together more readily.



208 services. In general, privacy risk assessments should produce the information that can help  
209 organizations to weigh the benefits of the data processing against the risks and to determine the  
210 appropriate response (see Appendix D for more guidance on the operational aspects of privacy risk  
211 assessment). Organizations may choose to respond to privacy risk in different ways, depending on the  
212 potential impact to individuals (and secondarily, organizations). Approaches include:

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

223 Privacy risk assessments are particularly important because as noted above privacy is a condition that  
224 safeguards multiple values. The methods for safeguarding these values may differ, and moreover, may  
225 be in tension with each other. For instance, if the organization is trying to achieve privacy through  
226 obscurity, this may lead to implementing measures such as data deletion schedules or privacy-  
227 enhancing cryptographic techniques that hide data even from the organization. If the organization is  
228 focused on control, obscurity measures could conflict with control measures. For example, if an  
229 individual requests access to data, the organization may not be able to produce the data if they have  
230 been deleted or encrypted in ways the organization cannot access. Privacy risk assessments can help an  
231 organization understand in a given context, the values to protect, the methods to employ, and how to  
232 balance implementation of different types of measures.

233 Lastly, privacy risk assessments help organizations distinguish between privacy risk and compliance risk.  
234 Identifying if data processing could create problems for individuals, even when the organization may be  
235 fully compliant with applicable laws or regulations, can help organizations make ethical decisions and  
236 avoid losses of trust that damage their reputations or slow adoption or cause abandonment of products  
237 and services.

### 238 1.3 Document Overview

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

- 240 • Section 2.0 describes the Privacy Framework components: the Core, the Profiles, and the  
241 Implementation Tiers.
- 242 • Section 3.0 presents examples of how the Privacy Framework can be used.
- 243 • Appendix A presents the Privacy Framework Core in a tabular format: the functions, categories,  
244 and subcategories.
- 245 • Appendix B contains a glossary of selected terms.
- 246 • Appendix C lists acronyms used in this document.
- 247 • Appendix D considers key practices that contribute to successful privacy risk management.
- 248 • Appendix E defines the Implementation Tiers.



- Appendix F provides a placeholder for a companion roadmap covering NIST’s next steps and identifying key areas where the relevant practices are not well enough understood to enable organizations to achieve a privacy outcome.

## 2.0 Privacy Framework Basics

The Privacy Framework provides a common language for understanding, managing, and communicating privacy risk with internal and external stakeholders. 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. Different types of entities—including sector-specific organizations—can use the Privacy Framework for different purposes, including the creation of common Profiles.

### 2.1 Core

The Core provides a set of activities to achieve specific privacy outcomes. The Core is not a checklist of actions to perform. It presents key privacy outcomes that are helpful in managing privacy risk. The Core comprises three elements: functions, categories, and subcategories, depicted in **Figure 3**.

The Core elements work together:

- Functions* organize basic privacy activities at their highest level. These functions are Identify, Protect, Control, Inform, and Respond. 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.
- Categories* are the subdivisions of a function into groups of privacy outcomes closely tied to programmatic needs and particular activities. Examples include “Protected Processing,” “Inventory and Mapping,” and “Risk Assessment.”
- 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. Examples include “Systems/products/services that process data, or with which individuals are interacting, are inventoried,” “Data are processed to limit the identification of individuals,” and “Individuals are informed when data are corrected or deleted.”

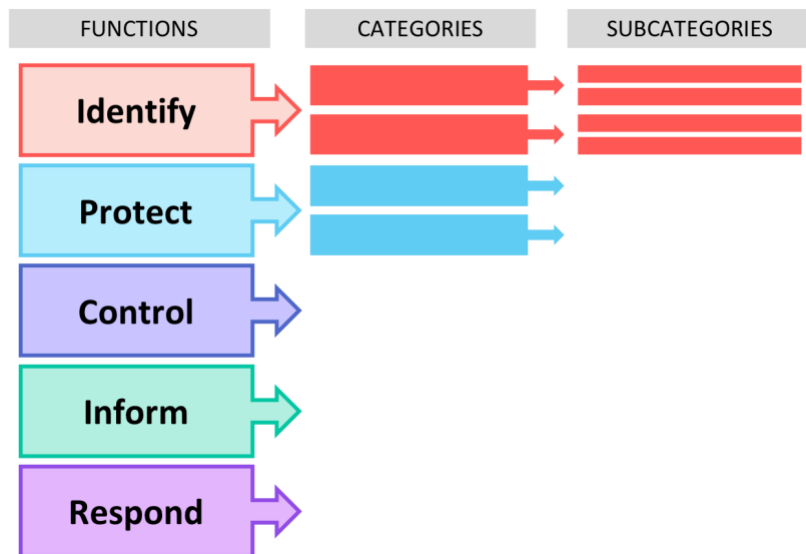


Figure 3: Privacy Framework Core Structure

The five Core functions, defined below, 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. See Appendix A for the complete Core.

- 291 • *Identify* – Develop the organizational understanding to manage privacy risk for individuals  
292 arising from data processing or their interactions with systems, products, or services.

293 The activities in the Identify function will be foundational for effective use of the Privacy  
294 Framework. Understanding the business context, including the circumstances under which data  
295 are processed, the privacy interests of individuals directly or indirectly served or affected by the  
296 organization, and legal/regulatory requirements will enable an organization to focus and  
297 prioritize its efforts, consistent with its risk management strategy and business needs. Examples  
298 of categories include: Inventory and Mapping, Business Environment, Governance, and Risk  
299 Assessment.

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

301 The Protect function not only encapsulates data security, the primary overlap between privacy  
302 and cybersecurity, but also includes practices that enable authorized data processing to be  
303 conducted in a protected state. Examples of categories include: Identity Management,  
304 Authentication, and Access Control; Awareness and Training; Data Security; and Protected  
305 Processing.

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

308 The Control function considers data management from both the standpoint of the organization  
309 and the individual. Examples of categories include: Policies, Processes, and Procedures; and Data  
310 Management.

- 311 • *Inform* – Develop and implement appropriate activities to enable organizations and individuals  
312 to have a reliable understanding about how data are processed.

313 The Inform function recognizes that both organizations and individuals need to know how data  
314 are processed in order to manage privacy risk effectively. Examples of categories include:  
315 Transparency Processes and Procedures, and Data Processing Awareness.

- 316 • *Respond* – Develop and implement appropriate activities to take action regarding a privacy  
317 breach or event.

318 The Respond function supports the ability to provide redress for individuals who have  
319 experienced a privacy breach or privacy event and to help organizations use lessons learned to  
320 improve their privacy practices. Examples of categories include: Mitigation and Redress.

## 321 2.2 Profile

322 The Profile is the alignment of the functions, categories, and subcategories with the business  
323 requirements, risk tolerance, privacy values, and resources of the organization. Under the Privacy  
324 Framework's risk-based approach, organizations may not need to achieve every outcome or activity  
325 reflected in the Core. When developing a Profile, an organization may select or tailor the Privacy  
326 Framework's functions, categories, and subcategories to its specific needs. An organization or industry  
327 sector also may develop its own additional functions, categories, and subcategories to account for  
328 unique organizational risks. An organization determines these needs by considering organizational or  
329 industry sector goals, legal/regulatory requirements and industry best practices, the organization's risk  
330 management priorities, and the privacy needs of individuals who are part of—or directly or indirectly  
331 served or affected by—an organization's systems, products, or services.

332 Profiles can be used to describe the current state or the desired target state of specific privacy activities.  
333 A Current Profile indicates privacy outcomes that an organization is currently achieving, while a Target  
334 Profile indicates the outcomes needed to achieve the desired privacy risk management goals. The  
335 differences between the two Profiles enable an organization to identify gaps, develop an action plan for  
336 improvement, and gauge the resources that would be needed (e.g., staffing, funding) to achieve privacy  
337 goals. This forms the basis of an organization's plan for reducing privacy risk in a cost-effective,  
338 prioritized manner. Profiles also can aid in communicating risk within and between organizations by  
339 helping organizations understand and compare the current or desired state of privacy outcomes.

340 This Privacy Framework does not prescribe Profile templates, to allow for flexibility in implementation.  
341 An organization may choose to have multiple Profiles for specific organizational components, systems,  
342 products, or services, or categories of individuals (e.g., employees, customers).

### 343 2.3 Implementation Tiers

344 Tiers are meant to support organizational decision-making about how to manage privacy risk by taking  
345 into account the nature of the privacy risks engendered by the organization's systems, products, or  
346 services and the adequacy of the processes and resources the organization has in place to manage such  
347 risks. When selecting Tiers, an organization should consider its current risk management practices; its  
348 data processing systems, products, or services; legal and regulatory requirements; business/mission  
349 objectives; organizational privacy values and individuals' privacy needs; and organizational constraints.

350 There are four distinct tiers: Partial (Tier 1), Risk Informed (Tier 2), Repeatable (Tier 3), and Adaptive  
351 (Tier 4). Tiers do not represent maturity levels, although organizations identified as Tier 1 are  
352 encouraged to consider moving toward Tier 2. Some organizations may never need to achieve Tier 3 or 4  
353 or may only focus on certain areas of these tiers. Progression to higher Tiers is appropriate when the  
354 nature of the privacy risks requires more multi-faceted risk management processes and resources.

355 Successful implementation of the Privacy Framework is based upon achieving the outcomes described in  
356 the organization's Target Profile(s) and not upon Tier determination. Still, Tier selection naturally affects  
357 Profiles, and helps to set the overall tone for how privacy risk will be managed within the organization.  
358 This should influence the prioritization of elements included in a Target Profile, and should influence  
359 assessments of progress in addressing gaps. The definitions of the Tiers are set forth in Appendix E.

### 360 3.0 How to Use the Privacy Framework

361 When used as a risk management tool, the Privacy Framework can assist an organization in its efforts to  
362 optimize beneficial uses of data and the development of innovative systems, products, and services  
363 while minimizing adverse consequences for individuals. The Privacy Framework can help organizations  
364 answer the fundamental question, "How are we considering the impacts to individuals as we develop  
365 our systems, products, and services?" As a result, the Privacy Framework can serve as the foundation for  
366 a new privacy program or a mechanism for improving an existing program. In either case, it is designed  
367 to complement existing business and system development operations, to provide a means of expressing  
368 privacy requirements to business partners and customers, and to support the identification of gaps in an  
369 organization's privacy practices.

370 To account for the unique needs of an organization, there are a wide variety of ways to use the Privacy  
371 Framework. The decision about how to apply it is left to the implementing organization. For example,  
372 one organization may choose to use the Implementation Tiers to articulate its envisioned privacy risk  
373 management processes. Another organization may already have robust privacy risk management  
374 processes, but may use the Core's five functions to analyze and articulate any gaps. Alternatively, an

375 organization seeking to establish a privacy program can use the Core categories and subcategories as a  
376 reference. The variety of ways in which the Privacy Framework can be used by organizations should  
377 discourage the notion of “compliance with the Privacy Framework” as a uniform or externally  
378 referenceable concept.

379 The following subsections present different ways in which organizations can use the Privacy Framework.

### 380 3.1 Informative References

381 The Privacy Framework is technology neutral, but it supports technological innovation because any  
382 organization or industry sector can map the outcome-based subcategories in the Core to standards,  
383 guidelines, and practices that evolve with technology and related business needs. By relying on  
384 consensus-based standards, guidelines, and practices, the tools and methods available to achieve  
385 positive privacy outcomes can scale across borders, accommodate the global nature of privacy risks, and  
386 evolve with technological advances and business requirements. The use of existing and emerging  
387 standards will enable economies of scale and drive the development of systems, products, and services  
388 that meet identified market needs while being mindful of the privacy needs of individuals.

389 Mapping subcategories to specific sections of standards, guidelines, and practices supports the  
390 achievement of the outcomes associated with each subcategory. The subcategories also can be used to  
391 identify where additional or revised standards, guidelines, and practices would help an organization to  
392 address emerging needs. An organization implementing a given subcategory, or developing a new  
393 subcategory, might discover that there are insufficient informative references for a related activity. To  
394 address that need, the organization might collaborate with technology leaders and/or standards bodies  
395 to draft, develop, and coordinate standards, guidelines, or practices.

396  
397  
398 NIST has developed a mapping of the Core subcategories to relevant NIST guidance, as well as a process  
399 for organizations or industry sectors to submit additional informative references and mappings for  
400 publication on NIST’s website at <https://www.nist.gov/privacy-framework>. These resources can support  
401 organizations’ application of the Privacy Framework and achievement of better privacy practices.

### 402 3.2 Strengthening Accountability

403 Accountability is generally considered a key privacy principle, although conceptually it is not unique to  
404 privacy.<sup>10</sup> Accountability occurs throughout an organization, and it can be expressed at varying degrees  
405 of abstraction, for example as a cultural value, as governance policies and procedures, or as traceability  
406 relationships between privacy requirements and controls. Privacy risk management can be a means of  
407 supporting accountability at all organizational levels as it connects senior executives, who can  
408 communicate the organization’s privacy values and risk tolerance, to those at the business/process

---

<sup>10</sup> See, e.g., Organisation for Economic Co-operation and Development (OECD), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* at <https://www.oecd.org/internet/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>; International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 29100, *Information technology – Security techniques – Privacy framework* at [https://standards.iso.org/ittf/PubliclyAvailableStandards/c045123\\_ISO\\_IEC\\_29100\\_2011.zip](https://standards.iso.org/ittf/PubliclyAvailableStandards/c045123_ISO_IEC_29100_2011.zip); Alliance of Automobile Manufacturers, Inc. and Association of Global Automakers, Inc., *Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technologies and Services* at [https://autoalliance.org/wp-content/uploads/2017/01/Consumer\\_Privacy\\_Principlesfor\\_VehicleTechnologies\\_Services-03-21-19.pdf](https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services-03-21-19.pdf).

409 manager level, who can collaborate on the development and implementation of governance policies and  
 410 procedures that support the organizational privacy values. These policies and procedures can then be  
 411 communicated to those at the implementation/operations level, who collaborate on defining the  
 412 privacy requirements that support the expression of the policies and procedures in the organization’s  
 413 systems, products, and services. Personnel at the implementation/operations level also select,  
 414 implement, and assess controls as the technical and policy measures that meet the privacy  
 415 requirements, and report upward on progress, gaps and deficiencies, and changing privacy risks so that  
 416 those at the business/process manager level and the senior executives can better understand and  
 417 respond appropriately. **Figure 4** provides a graphical representation of this iterative cycle and how  
 418 elements of the Privacy Framework can be incorporated to facilitate the process. In this way,  
 419 organizations can use the Privacy Framework as a tool to support accountability. They can also use the  
 420 Privacy Framework in conjunction with other frameworks and guidance that provide additional practices  
 421 to achieve accountability within and between organizations (see section 3.6 on Communicating Privacy  
 422 Requirements with Stakeholders).<sup>11</sup>



423  
424

Figure 4: Notional Information and Decision Flows within an Organization

### 425 3.3 Basic Review of Privacy Practices

426 The Privacy Framework can be used to compare an organization’s current privacy activities with those  
 427 outlined in the Core. Through the creation of a Current Profile, organizations can examine the extent to  
 428 which they are achieving the outcomes described in the Core categories and subcategories, aligned with  
 429 the five high-level functions: Identify, Protect, Control, Inform, and Respond. An organization may find  
 430 that it is already achieving the desired outcomes, thus managing privacy commensurate with the known

<sup>11</sup> See, e.g., NIST SP 800-37 Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* at <https://doi.org/10.6028/NIST.SP.800-37r2>; and Organization for the Advancement of Structured Information Standards (OASIS), *Privacy Management Reference Model and Methodology (PMRM) Version 1.0* at <https://docs.oasis-open.org/pmrm/PMRM/v1.0/PMRM-v1.0.pdf>.



431 risk. Alternatively, an organization may determine that it has areas for improvement. The organization  
 432 can use that information to develop an action plan to strengthen existing privacy practices and reduce  
 433 privacy risk. For example, an organization may be fulfilling its legal obligations with respect to processing  
 434 data, but it may lack a robust privacy risk assessment process that would help it achieve better privacy  
 435 outcomes for the individual. In building the Target Profile, the organization that is currently approaching  
 436 its privacy program from a predominantly regulatory and compliance standpoint will be able to  
 437 communicate the need for conducting privacy risk assessments to help it achieve more fine-tuned  
 438 privacy benefits for individuals. The organization can use this information to reprioritize resources or  
 439 adjust approaches to improve outcomes for both the organization and individuals.

440 While they do not replace a risk management process, the five high-level functions provide a concise  
 441 way for senior executives and others to distill the fundamental concepts of privacy risk so that they can  
 442 assess how identified risks are managed and how their organization stacks up at a high level against  
 443 existing privacy standards, guidelines, and practices.

### 444 3.4 Establishing or Improving a Privacy Program

445 Using a straightforward model of “ready, set, go” phases, the Privacy  
 446 Framework can support the creation of a new privacy program or  
 447 improvement of an existing program. These phases should be  
 448 repeated as necessary to continuously improve privacy.

#### 449 Ready

450 Effective privacy risk management requires an organization to  
 451 understand its business or mission environment; its legal  
 452 environment; its enterprise risk tolerance; the privacy risks  
 453 engendered by its systems, products, or services; and its role or  
 454 relationship to other organizations in the ecosystem. An organization  
 455 can use the Identify function to “get ready” by reviewing the  
 456 categories and subcategories, and beginning to develop its Current  
 457 Profile and Target Profile.<sup>12</sup>

458 An organization conducts privacy risk assessments pursuant to the  
 459 Risk Assessment category of the Identify function. These assessments  
 460 could be guided by the organization’s overall risk management process or previous risk assessment  
 461 activities. It is important that an organization identifies emerging privacy risks to gain a better  
 462 understanding of the impacts of its systems, products, or services on individuals. See Appendix D for  
 463 more information on privacy risk assessments.

#### 464 Set

465 The organization completes its Current Profile by indicating which category and subcategory outcomes  
 466 from the remaining functions are being achieved. If an outcome is partially achieved, noting this fact will  
 467 help support subsequent steps by providing baseline information. Informed by its privacy risk  
 468 assessment, the organization creates its Target Profile focused on the assessment of the Core categories  
 469 and subcategories describing the organization’s desired privacy outcomes. An organization also may

#### ***A Simplified Method for Establishing or Improving Privacy Programs***

**Ready:** use the Identify function to get “ready.”

**Set:** “set” an action plan based on the differences between Current and Target Profile(s).

**Go:** “go” forward with implementing the action plan.

<sup>12</sup> For additional guidance, see the “Prepare” step, Section 3.1, NIST Special Publication (SP) 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* at <https://doi.org/10.6028/NIST.SP.800-37r2>.

470 develop its own additional functions, categories and subcategories to account for unique organizational  
471 risks. It may also consider influences and requirements of external stakeholders such as business  
472 customers and partners when creating a Target Profile. An organization can develop multiple Profiles to  
473 support its different business lines or processes, which may have different business needs and  
474 associated risk tolerances.

475 The organization compares the Current Profile and the Target Profile to determine gaps. Next, it creates  
476 a prioritized action plan to address gaps—reflecting mission drivers, costs and benefits, and risks—to  
477 achieve the outcomes in the Target Profile. An organization using the Cybersecurity Framework and the  
478 Privacy Framework together may develop integrated action plans. The organization then determines  
479 resources, including funding and workforce, necessary to address the gaps, which can inform the  
480 selection of a target Tier. Using Profiles in this manner encourages the organization to make informed  
481 decisions about privacy activities, supports risk management, and enables the organization to perform  
482 cost-effective, targeted improvements.

### 483 Go

484 With the action plan “set,” the organization prioritizes which actions to take to address any gaps, and  
485 then adjusts its current privacy practices in order to achieve the Target Profile.<sup>13</sup> For further guidance,  
486 informative references that support outcome achievement for the categories and subcategories are  
487 available at <https://www.nist.gov/privacy-framework>. The organization should determine which  
488 standards, guidelines, and practices, including those that are sector specific, work best for its needs.

489 An organization can cycle through the phases non-sequentially as needed to continuously assess and  
490 improve its privacy posture. For instance, an organization may find that more frequent repetition of the  
491 Ready phase improves the quality of risk assessments. Furthermore, an organization may monitor  
492 progress through iterative updates to the Current Profile or the Target Profile to adjust to changing risks,  
493 subsequently comparing the Current Profile to the Target Profile. An organizations may also use this  
494 process to align its privacy program with its desired Tiers.

## 495 3.5 Application in the System Development Life Cycle

496 The Privacy Framework can be applied throughout the system development life cycle (SDLC) phases of  
497 plan, design, build/buy, deploy, operate, and decommission. The plan phase of the SDLC begins the cycle  
498 of any system and lays the groundwork for everything that follows. Overarching privacy considerations  
499 should be declared and described as clearly as possible. The plan should recognize that those  
500 considerations and requirements are likely to evolve during the remainder of the life cycle. A key  
501 milestone of the design phase is validating that the system privacy requirements match the needs and  
502 risk tolerance of the organization as they were expressed in a Profile. The desired privacy outcomes  
503 prioritized in a Target Profile should be incorporated when a) developing the system during the build  
504 phase and b) purchasing or outsourcing the system during the buy phase. That same Target Profile  
505 serves as a list of system privacy features that should be assessed when deploying the system to verify  
506 that all features are implemented. The privacy outcomes determined by using the Privacy Framework  
507 should then serve as a basis for ongoing operation of the system. This includes occasional reassessment,  
508 capturing results in a Current Profile, to verify that privacy requirements are still fulfilled.

---

<sup>13</sup> NIST SP 800-37 provides additional guidance on steps to execute on the action plan, including control selection, implementation, and assessment to close any gaps.



509 Privacy risk assessments typically focus on the information life cycle, the stages through which  
510 information passes, often characterized as creation or collection, processing, dissemination, use,  
511 storage, and disposition, to include destruction and deletion. Aligning the SDLC and the information  
512 lifecycle by identifying and understanding how data are processed during all stages of the SDLC helps  
513 organizations to better manage privacy risks and informs the selection and implementation of privacy  
514 controls throughout the SDLC.

### 515 3.6 Communicating Privacy Requirements with Stakeholders

516 The Privacy Framework provides a common language to communicate requirements among  
517 interdependent stakeholders. For example:

- 518 • An organization may use a Target Profile to express privacy risk management requirements to  
519 an external service provider (e.g., a cloud provider to which it is exporting data).
- 520 • An organization may express its privacy posture through a Current Profile to report results or to  
521 compare with acquisition requirements.
- 522 • An industry sector may establish a Target Profile that can be used among its constituents as an  
523 initial baseline Profile to build their tailored Target Profiles.
- 524 • An organization can better manage privacy risk affecting stakeholders by assessing their  
525 positions in the data processing ecosystem and the broader digital economy using Tiers.

526 Communication is especially important among stakeholders in supply chains. Supply chains are complex,  
527 globally distributed, and interconnected sets of resources and processes between multiple levels of  
528 organizations. Supply chains begin with the sourcing of products and services and extend from the  
529 design, development, manufacturing, processing, handling, and delivery of products and services to the  
530 end user. Given these complex and interconnected relationships, supply chain risk management (SCRM)  
531 is a critical organizational function.<sup>14</sup> SCRM practices should address the management of privacy risk  
532 associated with external parties, including both the effect an organization has on external parties and  
533 the effect external parties have on an organization. Such practices include identifying, assessing, and  
534 mitigating privacy risks arising from the processing of data, as well as from systems, products, and  
535 services that inherently lack the capabilities to mitigate privacy risks. Example activities may include:

- 536 • Determining privacy requirements for suppliers,
- 537 • Enacting privacy requirements through formal agreement (e.g., contracts),
- 538 • Communicating to suppliers how those privacy requirements will be verified and validated,
- 539 • Verifying that privacy requirements are met through a variety of assessment methodologies,  
540 and
- 541 • Governing and managing the above activities.

---

<sup>14</sup> Communicating Privacy Requirements with Stakeholders (section 3.6) and Buying Decisions (section 3.7) address only two uses of the Privacy Framework for SCRM and are not intended to address SCRM comprehensively.

542 As depicted in **Figure 5**, SCRM in the data  
 543 processing ecosystem encompasses a range  
 544 of entities and roles that may have multi-  
 545 directional relationships with each other  
 546 and individuals. Figure 5 displays entities as  
 547 having distinct roles, but organizations may  
 548 have multiple roles. For example, an  
 549 organization may be both a service provider  
 550 to other organizations and provide  
 551 commercial products or services to  
 552 individuals.

553 The parties described in Figure 5 comprise a  
 554 data processing ecosystem. These  
 555 relationships highlight the crucial role of  
 556 SCRM in addressing privacy risk in the  
 557 broader digital economy. These  
 558 relationships, the systems, products, and  
 559 services they provide, and the risks they  
 560 present should be identified and factored into  
 561 the data processing capabilities of  
 562 organizations, as well as their response protocols.

563 Whether considering individual subcategories of the Core or the comprehensive considerations of a  
 564 Profile, the Privacy Framework offers organizations and their partners a method to help ensure the  
 565 system, product, or service meets critical privacy outcomes. By first selecting outcomes that are relevant  
 566 to the context, the organization then can evaluate partners' systems, products, or services against this  
 567 outcome. For example, if a device is being purchased for environmental monitoring of a forest,  
 568 *manageability* may be important to support capabilities for minimizing the processing of data about  
 569 people using the forest and should drive a manufacturer evaluation against applicable subcategories  
 570 (see e.g., CT.DM-P1 in Appendix A: system or device configurations permit selective collection or  
 571 disclosure of data elements to allow for implementation of privacy principles such as data minimization).

### 572 3.7 Buying Decisions

573 Since either a Current or Target Profile can be used to generate a prioritized list of organizational privacy  
 574 requirements, these Profiles can also be used to inform decisions about buying products and services. In  
 575 circumstances where it may not be possible to impose a set of privacy requirements on the supplier, the  
 576 objective should be to make the best buying decision among multiple suppliers, given a carefully  
 577 determined list of privacy requirements. Often, this means some degree of trade-off, comparing  
 578 multiple products or services with known gaps to the Profile. If the system, product, or service  
 579 purchased did not meet all of the objectives described in the Profile, the organization can address the  
 580 residual risk through mitigation measures or other management actions.



Figure 5: Ecosystem Relationships

581 **Appendix A: Privacy Framework Core**

582 This appendix presents the Core: a table of functions, categories, and subcategories that describe  
 583 specific privacy activities that can support managing privacy risks when systems, products, and services  
 584 are processing data or interacting with individuals. This presentation format does not suggest a specific  
 585 implementation order—implementation may be non-sequential and iterative, depending on the SDLC  
 586 stage or status of the privacy program—or imply a degree of importance between the categories and  
 587 subcategories. The Core is not exhaustive; it is extensible, allowing organizations, sectors, and other  
 588 entities to adapt or add additional functions, categories and subcategories to their Profile(s).

589 For ease of use, each component of the Core is given a unique identifier. Functions and categories each  
 590 have a unique alphabetic identifier, as shown in **Table 1**. Subcategories within each category are  
 591 referenced numerically; the unique identifier for each subcategory is included in **Table 2**.

592 Additional supporting material, including informative references, relating to the Privacy Framework can  
 593 be found on the NIST website at <https://www.nist.gov/privacy-framework>.

594 **Table 1: Privacy Framework Function and Category Unique Identifiers**

	Function Unique Identifier	Function	Category Unique Identifier	Category
	<b>ID</b>	Identify-P	ID.IM-P	Inventory and Mapping
			ID.BE-P	Business Environment
			ID.GV-P	Governance
			ID.RA-P	Risk Assessment
			ID.RM-P	Risk Management Strategy
			ID.SC-P	Supply Chain Risk Management
	<b>PR</b>	Protect-P	PR.AC-P	Identity Management, Authentication, and Access Control
			PR.AT-P	Awareness and Training
			PR.DS-P	Data Security
			PR.DP-P	Data Protection Processes and Procedures
			PR.MA-P	Maintenance
			PR.PT-P	Protective Technology
			PR.PP-P	Protected Processing
	<b>CT</b>	Control-P	CT.PO-P	Data Management Processes and Procedures
			CT.DM-P	Data Management
	<b>IN</b>	Inform-P	IN.TP-P	Transparency Processes and Procedures
			IN.AW-P	Data Processing Awareness

<b>RS</b>	Respond-P	RS.RP-P	Response Planning
		RS.CO-P	Communications
		RS.AN-P	Analysis
		RS.MI-P	Mitigation
		RS.IM-P	Improvements
		RS.RE-P	Redress

595

596

Table 2: Privacy Framework Core

Function	Category	Subcategory
IDENTIFY-P (ID)	<b>Inventory and Mapping (ID.IM-P):</b> Data processing and individuals’ interactions with systems, products, or services are understood and inform the management of privacy risk.	<b>ID.IM-P1:</b> Systems/products/services that process data, or with which individuals are interacting, are inventoried.
		<b>ID.IM-P2:</b> The owners or operators of systems/products/services that process data, or with which individuals are interacting, are identified.
		<b>ID.IM-P3:</b> Data elements that systems/products/services are processing are inventoried.
		<b>ID.IM-P4:</b> Data actions are identified.
		<b>ID.IM-P5:</b> The data processing environment is identified (e.g., internal, cloud).
		<b>ID.IM-P6:</b> Data processing is mapped, illustrating the processing of data elements by system components and their owner/operators, and interactions of individuals and organizations with the systems/products/services.
	<b>Business Environment (ID.BE-P):</b> 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.	<b>ID.BE-P1:</b> The organization’s role in the supply chain is identified and communicated.
		<b>ID.BE-P2:</b> Priorities for organizational mission, objectives, and activities are established and communicated.
		<b>ID.BE-P3:</b> Systems/products/services that support organizational priorities are identified and key functional requirements communicated.
	<b>Governance (ID.GV-P):</b> The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk.	<b>ID.GV-P1:</b> Organizational privacy policies are established and communicated.
		<b>ID.GV-P2:</b> Processes to instill organizational privacy values within system/product/service development operations are in place.
		<b>ID.GV-P3:</b> Privacy roles and responsibilities for the entire workforce are established.

Function	Category	Subcategory
<b>Identify</b>		<b>ID.GV-P4:</b> Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., suppliers, customers, partners).
		<b>ID.GV-P5:</b> Legal, regulatory, and contractual requirements regarding privacy are understood and managed.
		<b>ID.GV-P6:</b> Governance and risk management processes address privacy risks.
	<b>Risk Assessment (ID.RA-P):</b> The organization understands the privacy risks to individuals and how such privacy risks may create secondary impacts on organizational operations (including mission, functions, reputation, or workforce culture).	<b>ID.RA-P1:</b> The purposes for the data actions are identified.
		<b>ID.RA-P2:</b> Contextual factors related to the systems/products/services and the data actions are identified (e.g., individuals’ privacy interests and perceptions, demographics, data sensitivity).
		<b>ID.RA-P3:</b> Potential problematic data actions and associated problems are identified.
		<b>ID.RA-P4:</b> Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.
		<b>ID.RA-P5:</b> Risk responses are identified and prioritized.
		<b>ID.RA-P6:</b> Risk is re-evaluated as data processing or individuals’ interactions with systems/products/services change.
	<b>Risk Management Strategy (ID.RM-P):</b> The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	<b>ID.RM-P1:</b> Risk management processes are established, managed, and agreed to by organizational stakeholders.
		<b>ID.RM-P2:</b> Organizational risk tolerance is determined and clearly expressed.
		<b>ID.RM-P3:</b> The organization’s determination of risk tolerance is informed by its role in the ecosystem.
	<b>Supply Chain Risk Management (ID.SC-P):</b> The organization’s priorities, constraints, risk tolerances, and assumptions are established	<b>ID.SC-P1:</b> Supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.

Function	Category	Subcategory
	and used to support risk decisions associated with managing privacy supply chain risk. The organization has established and implemented the processes to identify, assess, and manage privacy supply chain risks.	<b>ID.SC-P2:</b> Service providers/suppliers/third-party partners of data processing systems, products, and services are identified, prioritized, and assessed using a supply chain risk assessment process.
		<b>ID.SC-P3:</b> Contracts with service providers/suppliers/third-party partners are used to implement appropriate measures designed to meet the objectives of an organization’s privacy program and supply chain risk management plan.
		<b>ID.SC-P4:</b> Service providers/suppliers/third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
		<b>ID.SC-P5:</b> Response planning and testing are conducted with service providers/suppliers/third-party providers.
<b>PROTECT-P (PR)</b>	<b>Identity Management, Authentication, and Access Control (PR.AC-P):</b> Access to data and devices is limited to authorized individuals, processes, and devices, and is managed consistent with the assessed risk of unauthorized access.	<b>PR.AC-P1:</b> Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.
		<b>PR.AC-P2:</b> Physical access to data and devices is managed.
		<b>PR.AC-P3:</b> Remote access is managed.
		<b>PR.AC-P4:</b> Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
		<b>PR.AC-P5:</b> Network integrity is protected (e.g., network segregation, network segmentation).
		<b>PR.AC-P6:</b> Individuals and devices are proofed and bound to credentials, and authenticated commensurate with the risk of the transaction (e.g., individuals’ security and privacy risks and other organizational risks).
		<b>PR.AC-P7:</b> Attribute references are used instead of attribute values.
		<b>PR.AT-P1:</b> All users are informed and trained.



Function	Category	Subcategory
<b>Function</b>	<b>Awareness and Training (PR.AT-P):</b> The organization’s personnel and partners are provided privacy awareness education and are trained to perform their privacy-related duties and responsibilities consistent with related policies, procedures, and agreements.	<b>PR.AT-P2:</b> Privileged users understand their roles and responsibilities.
		<b>PR.AT-P3:</b> Third-party stakeholders (e.g., service providers, customers, partners) understand their roles and responsibilities.
		<b>PR.AT-P4:</b> Senior executives understand their roles and responsibilities.
		<b>PR.AT-P5:</b> Privacy personnel understand their roles and responsibilities.
	<b>Data Security (PR.DS-P):</b> Data are managed consistent with the organization’s risk strategy to protect individuals’ privacy and maintain data confidentiality, integrity, and availability.	<b>PR.DS-P1:</b> Data-at-rest is protected.
		<b>PR.DS-P2:</b> Data-in-transit is protected.
		<b>PR.DS-P3:</b> Systems/products/services and associated data are formally managed throughout removal, transfers, and disposition.
		<b>PR.DS-P4:</b> Adequate capacity to ensure availability is maintained.
		<b>PR.DS-P5:</b> Protections against data leaks are implemented.
		<b>PR.DS-P6:</b> Integrity checking mechanisms are used to verify software, firmware, and information integrity.
		<b>PR.DS-P7:</b> The development and testing environment(s) are separate from the production environment.
		<b>PR.DS-P8:</b> Integrity checking mechanisms are used to verify hardware integrity.
	<b>Data Protection Processes and Procedures (PR.DP-P):</b> Security and privacy policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage the protection of data.	<b>PR.DP-P1:</b> A baseline configuration of security and privacy controls is created and maintained.
		<b>PR.DP-P2:</b> A system development life cycle to manage systems and an information life cycle to manage data are aligned and implemented.
		<b>PR.DP-P3:</b> Configuration change control processes are in place.
<b>PR.DP-P4:</b> Backups of information are conducted, maintained, and tested.		
<b>PR.DP-P5:</b> Policy and regulations regarding the physical operating environment for organizational assets are met.		

Function	Category	Subcategory
<b>Function</b>		<b>PR.DP-P6:</b> Data are destroyed according to policy.
		<b>PR.DP-P7:</b> Protection processes are improved.
		<b>PR.DP-P8:</b> Effectiveness of protection technologies is shared.
		<b>PR.DP-P9:</b> Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
		<b>PR.DP-P10:</b> Response and recovery plans are tested.
		<b>PR.DP-P11:</b> Privacy procedures are included in human resources practices (e.g., deprovisioning, personnel screening).
		<b>PR.DP-P12:</b> A vulnerability management plan is developed and implemented.
	<b>Maintenance (PR.MA-P):</b> System maintenance and repairs are performed consistent with policies and procedures.	<b>PR.MA-P1:</b> Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.
		<b>PR.MA-P2:</b> Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.
	<b>Protective Technology (PR.PT-P):</b> Technical security solutions are managed to ensure the security and resilience of systems/products/services and associated data, consistent with related policies, procedures, and agreements.	<b>PR.PT-P1:</b> Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.
		<b>PR.PT-P2:</b> Removable media is protected and its use restricted according to policy.
		<b>PR.PT-P3:</b> The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
		<b>PR.PT-P4:</b> Communications and control networks are protected.
		<b>PR.PT-P5:</b> Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.
	<b>Protected Processing (PR.PP-P):</b> Technical data processing solutions increase disassociability consistent with related policies, procedures,	<b>PR.PP-P1:</b> Data are processed in an unobservable or unlinkable manner.
		<b>PR.PP-P2:</b> Data are processed to limit the identification of individuals.

Function	Category	Subcategory
	and agreements and the organization’s risk strategy to protect individuals’ privacy.	<b>PR.PP-P3:</b> Data are processed to restrict the formulation of inferences about individuals’ behavior or activities.
		<b>PR.PP-P4:</b> Data are processed through a distributed system architecture.
		<b>PR.PP-P5:</b> Data are processed on local devices.
<b>CONTROL-P (CT)</b>	<b>Data Management Processes and Procedures (CT.PO-P):</b> Policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage data consistent with the organization’s risk strategy to protect individuals’ privacy.	<b>CT.PO-P1:</b> Policies and procedures for authorizing data processing and maintaining authorizations are in place.
		<b>CT.PO-P2:</b> Processes for enabling data review, transmission/disclosure, alteration, or deletion are in place.
		<b>CT.PO-P3:</b> Processes and procedures for enabling individuals’ data processing preferences and requests (e.g., individual participation) are in place.
	<b>Data Management (CT.DM-P):</b> Data are managed consistent with the organization's risk strategy to protect individuals’ privacy and increase manageability.	<b>CT.DM-P1:</b> System or device configurations permit selective collection or disclosure of data elements to allow for implementation of privacy principles (e.g., data minimization).
		<b>CT.DM-P2:</b> Individuals’ authorization for the data action is obtained.
		<b>CT.DM-P3:</b> Data elements can be accessed for review.
		<b>CT.DM-P4:</b> Data elements can be accessed for transmission or disclosure.
		<b>CT.DM-P5:</b> Data elements can be accessed for alteration.
		<b>CT.DM-P6:</b> Data elements can be accessed for deletion.
		<b>CT.DM-P7:</b> Metadata containing processing permissions and related data values are transmitted with data elements.
<b>CT.DM-P8:</b> Processing permissions are transmitted using standardized formats.		
<b>INFORM-P (IN)</b>	<b>Transparency Processes and Procedures (IN.TP-P):</b> Policies (that address purpose, scope, roles, responsibilities, management	<b>IN.TP-P1:</b> Transparency procedures and mechanisms (e.g., internal or public reports) for data processing practices are in place.

Function	Category	Subcategory
	commitment, and coordination among organizational entities), processes, and procedures are maintained and used to increase transparency of the organization’s data processing practices.	<b>IN.TP-P2:</b> Processes for communicating data processing purposes are in place.
	<b>Data Processing Awareness (IN.AW-P):</b> Individuals and organizations have an awareness of data processing practices, and processes and procedures are used and maintained to increase predictability consistent with the organization’s risk strategy to protect individuals’ privacy.	<b>IN.AW-P1:</b> Records of data disclosures are maintained and can be shared.
		<b>IN.AW-P2:</b> Individuals are informed about data processing practices.
		<b>IN.AW-P3:</b> System/product/service design enhances data processing visibility.
		<b>IN.AW-P4:</b> Data sources are informed of data deletion and correction.
		<b>IN.AW-P5:</b> Individuals are informed when data are corrected or deleted.
		<b>IN.AW-P6:</b> Data provenance is maintained and can be shared. <b>IN.AW-P7:</b> Data analytic inputs and outputs are understood and evaluated for bias.
<b>RESPOND-P (RS)</b>	<b>Response Planning (RS.RP-P):</b> Response processes and procedures are executed and maintained to ensure response to privacy breaches and events.	<b>RS.RP-P1:</b> Response plan is executed during or after a privacy breach or event.
	<b>Communications (RS.CO-P):</b> Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies).	<b>RS.CO-P1:</b> Personnel know their roles and order of operations when a response is needed.
		<b>RS.CO-P2:</b> Privacy breaches and events are reported consistent with established criteria.
		<b>RS.CO-P3:</b> Information is shared consistent with response plans.
		<b>RS.CO-P4:</b> Coordination with stakeholders occurs consistent with response plans. <b>RS.CO-P5:</b> Data for voluntary information sharing is restricted to what is necessary for understanding the privacy breach or event.

Function	Category	Subcategory
		<b>RS.CO-P6:</b> Impacted individuals are notified about a privacy breach or event.
		<b>RS.AN-P1:</b> Notifications from detection systems or processes are investigated.
		<b>RS.AN-P2:</b> The impact of the privacy breach or event on individuals, the organization, and the ecosystem is understood.
		<b>RS.AN-P3:</b> Forensics are performed.
		<b>RS.AN-P4:</b> Privacy breaches and events are categorized consistent with response plan.
		<b>RS.AN-P5:</b> Processes are established to receive, analyze, and respond to problematic data actions disclosed to the organization from internal and external sources (e.g., internal testing, privacy researchers).
		<b>RS.MI-P1:</b> Privacy breaches and events are contained.
		<b>RS.MI-P2:</b> Privacy breaches and events are mitigated.
		<b>RS.MI-P3:</b> Newly identified problematic data actions are mitigated or documented as accepted risks.
		<b>RS.IM-P1:</b> Policies and processes incorporate lessons learned.
		<b>RS.RE-P1:</b> Processes for receiving and responding to complaints, concerns, and questions from individuals about organizational privacy practices are in place.
		<b>RS.RE-P2:</b> Individuals are provided with mitigation mechanisms.

597  
598  
599  
600  
601  
602  
603

604 **Appendix B: Glossary**

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

<b>Availability</b> [NIST SP 800-37]	Ensuring timely and reliable access to and use of information.
<b>Category</b>	The subdivision of a function into groups of privacy outcomes, closely tied to programmatic needs and particular activities. Examples of categories include “Protected Processing,” “Inventory and Mapping,” and “Risk Assessment.”
<b>Confidentiality</b> [NIST SP 800-37]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
<b>Control (function)</b>	Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.
<b>Core</b>	A set of privacy protection activities, desired outcomes, and applicable references. The Framework Core comprises three types of elements: functions, categories, and subcategories.
<b>Data</b>	A representation of information with the potential for adverse consequences for individuals when processed.
<b>Data Action</b> [NISTIR 8062, Adapted]	A system/product/service operation that processes data.
<b>Data Elements</b>	The smallest named item of data that conveys meaningful information.
<b>Data Processing</b> [NISTIR 8062, Adapted]	An operation or set of operations performed upon data across the full data life cycle, including but not limited to the collection, retention, logging, generation, transformation, use, disclosure, transfer, and disposal of data.
<b>Disassociability</b> [NISTIR 8062, Adapted]	Enabling the processing of data or events without association to individuals or devices beyond the operational requirements of the system.
<b>Function</b>	One of the main components of the Privacy Framework. Functions provide the highest level of structure for organizing basic privacy activities into categories and subcategories. The five functions are Identify, Protect, Control, Inform, and Respond.
<b>Identify (function)</b>	Develop the organizational understanding to manage privacy risk for individuals arising from data processing or their interactions with systems, products, or services.
<b>Implementation Tier</b>	The degree to which an organization’s current or target risk management practices demonstrate an understanding of privacy risk and how systematic the practices are.
<b>Inform (function)</b>	Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding about how data are processed.
<b>Integrity</b> [NIST SP 800-37]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

<b>Manageability</b> [NISTIR 8062, Adapted]	Providing the capability for granular administration of data, including alteration, deletion, and selective disclosure.
<b>Metadata</b> [NIST SP 800-53, Adapted]	Information describing the characteristics of data including, for example, structural metadata describing data structures (i.e., data format, syntax, semantics) and descriptive metadata describing data contents.
<b>Predictability</b> [NISTIR 8062, Adapted]	Enabling reliable assumptions by individuals, owners, and operators about data and its processing by a system.
<b>Privacy Breach</b>	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.
<b>Privacy Control</b> [NIST SP 800-37, Adapted]	The administrative, technical, and physical safeguards employed within an organization to satisfy privacy requirements.
<b>Privacy Event</b>	The occurrence of problematic data actions.
<b>Privacy Requirement</b>	A specification for system/product/service functionality to meet stakeholders' desired privacy outcomes.
<b>Privacy Risk</b>	The likelihood that individuals will experience problems resulting from data processing, and the impact should they occur.
<b>Privacy Risk Assessment</b>	A privacy risk management sub-process for identifying, evaluating, prioritizing, and responding to specific risks arising from data processing.
<b>Privacy Risk Management</b>	A cross-organizational set of processes for identifying, assessing, and responding to privacy risks.
<b>Problematic Data Action</b> [NISTIR 8062]	A data action that can cause an adverse effect, or problem, for individuals.
<b>Profile</b>	A representation of the outcomes based on business/mission objectives, types of data processing, and individuals' privacy needs that an organization has selected from the Privacy Framework categories and subcategories.
<b>Protect (function)</b>	Develop and implement appropriate data processing safeguards.
<b>Provenance</b> [NISTIR 8112, Adapted]	Metadata pertaining to the origination or source of specified data.
<b>Respond (function)</b>	Develop and implement appropriate activities to take action regarding a privacy breach or event.
<b>Risk</b> [NIST SP 800-30]	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.
<b>Subcategory</b>	The further divisions of a category into specific outcomes of technical and/or management activities. Examples of subcategories include "Systems/products/services that process data, or with which individuals are interacting, are inventoried," "Data are processed to limit the identification of individuals," and "Individuals are informed when data are corrected or deleted."



## 607 Appendix C: Acronyms

608 This appendix defines selected acronyms used in the publication.

609

610	IAB	Interactive Advertising Bureau
611	IEC	International Electrotechnical Commission
612	ISO	International Organization for Standardization
613	IT	Information Technology
614	NIST	National Institute of Standards and Technology
615	NISTIR	National Institute of Standards and Technology Internal Report
616	OASIS	Organization for the Advancement of Structured Information Standards
617	OECD	Organisation for Economic Co-operation and Development
618	OMB	Office of Management and Budget
619	PMRM	Privacy Management Reference Model and Methodology
620	PRAM	Privacy Risk Assessment Methodology
621	SCRM	Supply Chain Risk Management
622	SDLC	System Development Life Cycle
623	SP	Special Publication

## 624 Appendix D: Privacy Risk Management Practices

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

### 632 Organizing Preparatory Resources

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

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

- 642 • **Risk management role assignments** (ID.GV-P3, ID.GV-P4)

643 Enabling cross-organizational understanding of who has responsibility for different risk  
644 management tasks in the organization supports better coordination and accountability for  
645 decision-making. In addition, a broad range of perspectives can improve the process of  
646 identifying, assessing, and responding to privacy risks. A diverse and cross-functional team can  
647 help to identify a more comprehensive range of risks to individuals' privacy, and to select a  
648 wider set of mitigations. Determining which roles to include in the risk management discussions  
649 depends on organizational context and makeup, although collaboration between an  
650 organization's privacy and cybersecurity programs will be important. If one individual is being  
651 assigned to multiple roles, managing potential conflicts of interest should be considered.

- 652 • **Organizational risk management strategy** (ID.RM)

653 An organization's risk management strategy helps to align the organization's mission and values  
654 with organizational risk assumptions and constraints. Limitations on resources to achieve  
655 mission/business objectives and to manage risk will likely require trade-offs. Enabling personnel  
656 involved in the risk management process to better understand the organization's risk tolerance  
657 should help to guide decisions about how to allocate resources and improve decisions around  
658 risk response.

- 659 • **Key stakeholders** (ID.GV-P4, ID.SC)

660 Privacy stakeholders are those who have an interest or concern in the privacy outcomes of the  
661 system, product, or service. For example, legal concerns likely focus on whether the system,  
662 product, or service is operating in a way that would cause the organization to be out of  
663 compliance with privacy laws or regulations or its business agreements. Business owners that  
664 want to maximize usage may be concerned about loss of trust in the system, product, or service  
665 due to poor privacy. Individuals whose data are being processed or who are interacting with the

666 system, product, or service will be interested in not experiencing problems or adverse  
667 consequences. Understanding the stakeholders and the types of privacy outcomes they are  
668 interested in will facilitate system/product/service design that appropriately addresses  
669 stakeholders' needs.

670 • **Organizational-level privacy requirements (ID.GV)**

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

- 676 ○ Legal environment (e.g., laws, regulations, contracts)
- 677 ○ Organizational policies or cultural values
- 678 ○ Relevant global standards
- 679 ○ Privacy principles

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

681 Design artifacts may take many forms such as system design architectures or data flow  
682 diagrams. These artifacts help an organization build systems, products, and services that meet  
683 an organization's mission/business priorities and objectives. Therefore, they can help privacy  
684 programs understand how systems, products, and services need to function so that controls or  
685 measures that help to mitigate privacy risk can be selected and implemented in ways that  
686 maintain functionality while protecting privacy.

687 • **Data maps (ID.IM)**

688 Data maps illustrate data processing and individuals' interactions with systems, products, and  
689 services. A comprehensive data map shows the data processing environment and includes the  
690 components through which data are being processed or with which individuals are interacting,  
691 the owners or operators of the components, and discrete data actions and the specific data  
692 elements being processed. A data map can be overlaid on existing system/product/service  
693 design artifacts for convenience and ease of communication between organizational  
694 components. As discussed below, a data map is an important artifact in privacy risk assessment.

## 695 Determining Privacy Capabilities

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

705 In determining privacy capabilities, an organization may consider which of the privacy engineering and  
706 security objectives are most important with respect to its mission/business needs, risk tolerance, and  
707 organizational-level privacy requirements (see Organizing Preparatory Resources above). Not all of the

708 objectives may be equally important, or trade-offs may be necessary among them. Although the privacy  
 709 capabilities inform the privacy risk assessment by supporting risk prioritization decisions, the privacy  
 710 capabilities may also be informed by the risk assessment and adjusted to support the management of  
 711 specific privacy risks or address changes in the environment, including design changes to the system,  
 712 product, or service.

713 **Table 3: Privacy Engineering and Security Objectives<sup>15</sup>**

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

## 714 Defining Privacy Requirements

715 Privacy requirements specify the way the system, product, or service needs to function to meet  
 716 stakeholders' desired privacy outcomes (e.g., "the application is configured to allow users to select  
 717 specific data elements"). To define privacy requirements, consider organizational-level privacy  
 718 requirements (see Organizing Preparatory Resources above) and the outputs of a privacy risk  
 719 assessment. This process helps an organization to answer two questions: 1) what a system, product, or  
 720 service *can* do with data processing and interactions with individuals, and 2) what it *should* do. Then an  
 721 organization can allocate resources to design a system, product, or service in a way that achieves the  
 722 defined requirements. Ultimately, this can lead to the development of systems, products, and services  
 723 that are more mindful of individuals' privacy, and are based on informed risk decisions.

---

<sup>15</sup> The privacy engineering objectives are adapted from NISTIR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems* at <https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf>. The security objectives are from NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* at <https://doi.org/10.6028/NIST.SP.800-37r2>.

## 724 Conducting Privacy Risk Assessments

725 Conducting a privacy risk assessment helps an organization to identify privacy risks engendered by the  
726 system, product, or service and prioritize them to be able to make informed decisions about how to  
727 respond to the risks (ID.RA-P, ID.RM-P). Methodologies for conducting privacy risk assessments may  
728 vary, but organizations should consider the following characteristics:<sup>16</sup>

- 729 • **Risk model** (ID.RA-P6)

730 Risk models define the risk factors to be assessed and the relationships among those factors.<sup>17</sup> If  
731 an organization is not using a pre-defined risk model, the organization should clearly define  
732 which risk factors it will be assessing and the relationships among these factors. Although  
733 cybersecurity has a widely-used risk  
734 model based on the risk factors of  
735 threats, vulnerabilities, likelihood, and  
736 impact, there is not one commonly  
737 accepted privacy risk model. NIST has  
738 developed a privacy risk model based on the risk factors of problematic data actions, likelihood,  
739 and impact, each explained below.

- 740 ○ A problematic data action is any action a system takes to process data that could result in a  
741 problem for individuals. Organizations consider the type of problems that are relevant to  
742 the population of individuals. Problems can take any form and may consider the experience  
743 of individuals singly or as a group.<sup>18</sup>
- 744 ○ Likelihood is defined as a contextual analysis that a data action is likely to create a problem  
745 for a representative set of individuals. Context can include organizational factors (e.g., the  
746 public perception about participating organizations with respect to privacy), system factors  
747 (e.g., the nature and history of individuals' interactions with the system), or individual  
748 factors (e.g., demographics of the population set).<sup>19</sup>
- 749 ○ Impact is an analysis of the costs should the problem occur. As noted in section 1.2, the  
750 experience of individuals is a type of externality for organizations. Moreover, individuals'  
751 experiences may be subjective. Thus, impact may be difficult to assess accurately.  
752 Organizations should consider the best means of internalizing impact to individuals in order  
753 to appropriately prioritize and respond to privacy risks.<sup>20</sup>

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

---

<sup>16</sup> 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 <https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources>.

<sup>17</sup> See NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments* at p. 8 <https://doi.org/10.6028/NIST.SP.800-30r1>

<sup>18</sup> As part of its PRAM, NIST has created an illustrative catalog of problematic data actions and problems for consideration. See <https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources>. Other organizations may have created additional problem sets, or may refer to them as adverse consequences or harms.

<sup>19</sup> See NIST PRAM for more information about contextual factors. Id at Worksheet 2.

<sup>20</sup> The NIST PRAM uses indirect costs to an organization as a proxy for considering individual impact such as non-compliance costs, direct business costs, reputational costs, and internal culture costs. Id at Worksheet 3, Impact Tab.

- 754       • **Assessment approach**  
755       The assessment approach is the mechanism by which identified risks are prioritized. Assessment  
756       approaches can be categorized as quantitative, semi-quantitative, or qualitative.<sup>21 22</sup>  
757       • **Prioritizing risks (ID.RA-P7)**  
758       Given the applicable limits of an organization’s resources, organizations prioritize the risks to  
759       facilitate communication about how to respond.<sup>23</sup>  
760       • **Responding to risks**  
761       As described in section 1.2, responding to risk is usually categorized as mitigation,  
762       transfer/sharing, avoidance, or acceptance.<sup>24</sup>

### 763 Creating Privacy Requirements Traceability

764 Once the organization has determined which risks to mitigate, the organization can refine the privacy  
765 requirements and then select and implement controls (i.e., technical and/or policy safeguards) to meet  
766 the defined requirements.<sup>25</sup> An organization may use a variety of sources to select controls, such as NIST  
767 Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*.<sup>26</sup>  
768 After implementation, an organization iteratively assesses the controls for their effectiveness in meeting  
769 the privacy requirements and managing privacy risk. In this way, an organization creates traceability  
770 between the controls and the privacy requirements and demonstrate accountability between its  
771 systems, products, and services and its organizational privacy goals. (ID.RA-P7)

### 772 Monitoring Changing Privacy Risks

773 Privacy risk management is not a static process. An Organizations monitors how changes in its business  
774 environment and corresponding changes to its systems, products, and services may be affecting privacy  
775 risk, and iteratively use the practices in this appendix to adjust accordingly. (ID.RA-P8)

---

<sup>21</sup> See NIST SP 800-30, *Guide for Conducting Risk Assessments* at p. 14 <https://doi.org/10.6028/NIST.SP.800-30r1>

<sup>22</sup> The NIST PRAM uses a semi-quantitative approach based on a scale of 1-10.

<sup>23</sup> The NIST PRAM provides various prioritization representations, including a heat map. See <https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources>, Worksheet 3.

<sup>24</sup> The NIST PRAM provides a process for responding to prioritized privacy risks. Id at Worksheet 4.

<sup>25</sup> See NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* at <https://doi.org/10.6028/NIST.SP.800-37r2>

<sup>26</sup> See NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, as updated at <https://csrc.nist.gov/publications/sp800-53>

## 776 Appendix E: Implementation Tiers Definitions

777 The Tiers are defined through four areas summarized below:

### 778 Tier 1: Partial

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

### 796 Tier 2: Risk Informed

- 797 • **Privacy Risk Management Process** – Risk management practices are approved by management  
798 but may not be established as organizational-wide policy. Prioritization of privacy activities is  
799 directly informed by organizational risk objectives, privacy risk assessments, and  
800 business/mission requirements.
- 801 • **Integrated Privacy Risk Management Program** – There is an awareness of privacy risk at the  
802 organizational level, but an organization-wide approach to managing privacy risk has not been  
803 established. Information about data processing and resulting privacy risks is shared within the  
804 organization on an informal basis. Consideration of privacy in organizational objectives and  
805 programs may occur at some but not all levels of the organization. Privacy risk assessment  
806 occurs, but is not typically repeatable or reoccurring.
- 807 • **Ecosystem Relationships** – There is some understanding of an organization’s role in the larger  
808 ecosystem with respect to other entities (e.g., buyers, suppliers, service providers, business  
809 associates, partners). The organization is aware of the privacy ecosystem risks associated with  
810 the products and services it provides and uses, but does not act consistently or formally upon  
811 those risks.
- 812 • **Workforce** – There are personnel with specific privacy responsibilities, but they may have non-  
813 privacy responsibilities as well. Privacy training is conducted regularly for privacy personnel,  
814 although there is no consistent process for updates on best practices.

### 815 Tier 3: Repeatable

- 816 • **Privacy Risk Management Process** – The organization’s risk management practices are formally  
817 approved and expressed as policy. Organizational privacy practices are regularly updated based

- 818 on the application of risk management processes to changes in business/mission requirements  
819 and a changing risk, policy, and technology landscape.
- 820 • **Integrated Privacy Risk Management Program** – There is an organization-wide approach to  
821 manage privacy risk. Risk-informed policies, processes, and procedures are defined,  
822 implemented as intended, and reviewed. Consistent methods are in place to respond effectively  
823 to changes in risk. The organization consistently and accurately monitors privacy risk. Senior  
824 privacy and non-privacy executives communicate regularly regarding privacy risk. Senior  
825 executives ensure consideration of privacy through all lines of operation in the organization.
  - 826 • **Ecosystem Relationships** – The organization understands its role, dependencies, and  
827 dependents in the larger ecosystem and may contribute to the community’s broader  
828 understanding of risks. The organization is aware of the privacy ecosystem risks associated with  
829 the products and services it provides and it uses. Additionally, it usually acts formally upon those  
830 risks, including mechanisms such as written agreements to communicate baseline requirements,  
831 governance structures, and policy implementation and monitoring.
  - 832 • **Workforce** – Dedicated privacy personnel possess the knowledge and skills to perform their  
833 appointed roles and responsibilities. There is regular, up-to-date privacy training for all  
834 personnel.

#### 835 Tier 4: Adaptive

- 836 • **Privacy Risk Management Process** – The organization adapts its privacy practices based on  
837 lessons learned from privacy breaches and events, and identification of new privacy risks.  
838 Through a process of continuous improvement incorporating advanced privacy technologies and  
839 practices, the organization actively adapts to a changing policy and technology landscape and  
840 responds in a timely and effective manner to evolving privacy risks.
- 841 • **Integrated Privacy Risk Management Program** – There is an organization-wide approach to  
842 managing privacy risk that uses risk-informed policies, processes, and procedures to address  
843 potential privacy events. The relationship between privacy risk and organizational objectives is  
844 clearly understood and considered when making decisions. Senior executives monitor privacy  
845 risk in the same context as cybersecurity risk, financial risk, and other organizational risks. The  
846 organizational budget is based on an understanding of the current and predicted risk  
847 environment and risk tolerance. Business units implement executive vision and analyze system-  
848 level risks in the context of the organizational risk tolerances. Privacy risk management is part of  
849 the organizational culture and evolves from lessons learned and continuous awareness of data  
850 processing and resulting privacy risks. The organization can quickly and efficiently account for  
851 changes to business/mission objectives in how risk is approached and communicated.
- 852 • **Ecosystem Relationships** – The organization understands its role, dependencies, and  
853 dependents in the larger ecosystem and contributes to the community’s broader understanding  
854 of risks. The organization uses real-time or near-real-time information to understand and  
855 consistently act upon privacy ecosystem risks associated with the products and services it  
856 provides and it uses. Additionally, it communicates proactively, using formal (e.g., agreements)  
857 and informal mechanisms to develop and maintain strong ecosystem relationships.
- 858 • **Workforce** – The organization has specialized privacy skillsets throughout the organizational  
859 structure; personnel with diverse perspectives contribute to the management of privacy risks.  
860 There is regular, up-to-date, specialized privacy training for all personnel. Personnel at all levels  
861 understand the organizational privacy values and their role in maintaining them.

862



## 863 Appendix F: Roadmap

864 *This appendix will provide a companion roadmap to the Privacy Framework covering next steps and*  
865 *identifying key areas where the relevant practices are not well enough understood to enable*  
866 *organizations to achieve a privacy outcome. These areas will be based on input and feedback received*  
867 *from stakeholders through the Privacy Framework development process.*