

From: Andrew Sanford <andrew.n.sanford@gmail.com>
Sent: Tuesday, September 10, 2019 6:51 PM
To: privacyframework <privacyframework@nist.gov>
Subject: NIST Privacy Framework: Preliminary Draft Comments

To whom it may concern,

Thank you for your work on this framework. Attached are my comments for improvement. Other than that, this framework looks great. Please let me know if you have any questions.

All the Best,
Andrew Sanford

1
2
3

PRELIMINARY DRAFT

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

September 6, 2019

4 Note to Reviewers

5 This preliminary draft is provided to promote the development of the NIST Privacy Framework: A Tool
6 for Improving Privacy through Enterprise Risk Management (Privacy Framework). The National Institute
7 of Standards and Technology (NIST) will use comments on this draft to develop version 1.0.

8 N.B. Throughout this document, references are made to a repository and a process for accepting
9 external informative references. NIST will make this process and repository available with version 1.0.

10 NIST welcomes feedback on this preliminary draft. In particular, NIST requests that reviewers consider
11 the following questions:

12 1. Does this preliminary draft:

- 13 a. adequately define outcomes that:
 - 14 i. cover existing practices;
 - 15 ii. strengthen individuals' privacy protection;
 - 16 iii. enable effective organizational use;
 - 17 iv. support enterprise mission/business objectives; and
 - 18 v. facilitate compliance with applicable laws or regulations;
- 19 b. appropriately integrate privacy risk into organizational risk;
- 20 c. provide guidance about privacy risk management practices at the right level of specificity;
- 21 d. adequately define the relationship between privacy and cybersecurity risk;
- 22 e. provide the capability for those in different organizational roles such as senior executives
23 and boards of directors, legal, compliance, security, and information technology or
24 operations to understand privacy risks and mitigations at the appropriate level of detail;
- 25 f. provide sufficient guidance and resources to aid organizations of all sizes to build and
26 maintain a privacy risk management program while maintaining flexibility; and
- 27 g. enable cost-effective implementation?

28 2. Will this preliminary draft, as presented:

- 29 a. be inclusive of, and not disruptive to, effective privacy practices in use today, including
30 widely used voluntary consensus standards that are not yet final;
- 31 b. enable organizations to use the Privacy Framework in conjunction with the Framework for
32 Improving Critical Infrastructure Cybersecurity to collaboratively address privacy and
33 cybersecurity risks; and
- 34 c. enable organizations to adapt to privacy risks arising from emerging technologies such as
35 the Internet of Things and artificial intelligence?

36 [Table of Contents](#)

37 **Note to Reviewers**.....1

38 **Executive Summary**.....3

39 **Acknowledgements**.....3

40 **1.0 Privacy Framework Introduction**4

41 1.1 Overview of the Privacy Framework 5

42 1.2 Privacy Risk Management 6

43 1.2.1 Cybersecurity and Privacy Risk Management 6

44 1.2.2 Relationship Between Privacy Risk Management and Risk Assessment 7

45 1.3 Document Overview 8

46 **2.0 Privacy Framework Basics**9

47 2.1 Core 9

48 2.2 Profiles..... 10

49 2.3 Implementation Tiers..... 11

50 **3.0 How to Use the Privacy Framework**.....12

51 3.1 Mapping to Informative References 12

52 3.2 Strengthening Accountability..... 13

53 3.3 Establishing or Improving a Privacy Program 14

54 3.4 Applying to the System Development Life Cycle 15

55 3.5 Using within the Data Processing Ecosystem 16

56 3.6 Informing Buying Decisions..... 17

57 **Appendix A: Privacy Framework Core**18

58 **Appendix B: Glossary**29

59 **Appendix C: Acronyms**.....32

60 **Appendix D: Privacy Risk Management Practices**33

61 **Appendix E: Implementation Tiers Definitions**.....38

62 **Appendix F: Roadmap**41

63 **Appendix G: References**.....42

64 [List of Figures](#)

65 **Figure 1: Core, Profiles, and Implementation Tiers**..... 5

66 **Figure 2: Cybersecurity and Privacy Risk Relationship** 6

67 **Figure 3: Relationship Between Privacy Risk and Organizational Risk** 7

68 **Figure 4: Privacy Framework Core Structure** 9

69 **Figure 5: Profile Development Process** 11

70 **Figure 6: Notional Collaboration and Communication Flows Within an Organization** 13

71 **Figure 7: Data Processing Ecosystem Relationships**..... 16

72 **Figure 8: Using Functions to Manage Privacy Risk**..... 19

73 [List of Tables](#)

74 **Table 1: Privacy Framework Function and Category Unique Identifiers**..... 20

75 **Table 2: Privacy Framework Core** 21

76 **Table 3: Privacy Engineering and Security Objectives** 35

77

78 Executive Summary

79 For more than two decades, the Internet and associated information technologies have driven
 80 unprecedented innovation, economic value, and improvement in social services. Many of these benefits
 81 are fueled by data about individuals that flow through a complex ecosystem—so complex that
 82 individuals may not be able to understand the potential consequences for their privacy as they interact
 83 with systems, products, and services. At the same time, organizations may not realize the full extent of
 84 these consequences for individuals, for society, or for their enterprises, which can affect their
 85 reputations, their bottom line, and their future prospects for growth.

Perhaps add a note that emphasizes security applies to both individuals & groups of people

86 The National Institute of Standards and Technology (NIST), working in collaboration with private and
 87 public stakeholders, has developed this voluntary NIST Privacy Framework: A Tool for Improving Privacy
 88 through Enterprise Risk Management (Privacy Framework). The Privacy Framework can drive better
 89 privacy engineering and help organizations protect individuals' privacy by:

Perhaps add a note that emphasizes security applies to both individuals and groups of people.

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

96 Deriving benefits from data while simultaneously managing risks to individuals' privacy is not well-suited
 97 to one-size-fits-all solutions. Like building a house, where homeowners get to choose room layouts but
 98 need to trust that the foundation is well-engineered, privacy protection should allow for individual
 99 choices, as long as effective privacy risk mitigations are already engineered into products and services.
 100 The Privacy Framework—through a risk- and outcome-based approach—is flexible enough to address
 101 diverse privacy needs, enable more innovative and effective solutions that can lead to better outcomes
 102 for individuals and enterprises, and stay current with technology trends, including artificial intelligence
 103 and the Internet of Things.

104 The Privacy Framework follows the structure of the Framework for Improving Critical Infrastructure
 105 Cybersecurity (Cybersecurity Framework) [1] to facilitate the use of both frameworks together. Like the
 106 Cybersecurity Framework, the Privacy Framework is composed of three parts: the Core, Profiles, and
 107 Implementation Tiers. Each component reinforces privacy risk management through the connection
 108 between business and mission drivers and privacy protection activities.

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

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

117 Acknowledgements

118 *Acknowledgements will be included in version 1.0.*

119 1.0 Privacy Framework Introduction

120 For more than two decades, the Internet and associated information technologies have driven
121 unprecedented innovation, economic value, and access to social services. Many of these benefits are
122 fueled by *data* about *individuals* that flow through a complex ecosystem—so complex that individuals
123 may not be able to understand the potential consequences for their privacy as they interact with
124 systems, products, and services. Organizations may not fully realize the consequences either. Failure to
125 manage *privacy risks* can have direct adverse consequences for people at both the individual and
126 societal level, with follow-on effects on organizations' reputation, bottom line, and future prospects for
127 growth. Finding ways to continue to derive benefits from data while simultaneously protecting
128 individuals' privacy is challenging, and not well-suited to one-size-fits-all solutions.

129 Privacy is challenging because not only is it an all-encompassing concept that helps to safeguard
130 important values such as human autonomy and dignity, but also the means for achieving it can vary. For
131 example, privacy can be achieved through seclusion, limiting observation, or individuals' control of
132 facets of their identities (e.g., body, data, reputation).¹ Moreover, human autonomy and dignity are not
133 fixed, quantifiable constructs; they are filtered through cultural diversity and individual differences. This
134 broad and shifting nature of privacy makes it difficult to communicate clearly about privacy risks within
135 and between organizations and with individuals. What has been missing is a common language and
136 practical tool that is flexible enough to address diverse privacy needs.

137 The National Institute of Standards and Technology (NIST) has developed this voluntary NIST Privacy
138 Framework: A Tool for Improving Privacy through Enterprise Risk Management (Privacy Framework) to
139 help organizations manage privacy risks by:

- 140 • Taking privacy into account as they design and deploy systems, products, and services that
141 affect individuals;
- 142 • Integrating privacy practices into their business processes that result in effective solutions to
143 mitigate any adverse impacts; and
- 144 • Communicating about these practices.

145 The Privacy Framework is intended to be widely usable by organizations of all sizes and agnostic to any
146 particular technology, sector, law, or jurisdiction.

- 147 • Different parts of an organization's workforce, including executives, legal, and information
148 technology (IT) may take responsibility for different outcomes and activities.
- 149 • It encourages cross-organization collaboration to develop Profiles and achieve outcomes.
- 150 • The Privacy Framework is usable by any organization or entity regardless of its role in the *data*
151 *processing ecosystem*—the complex and interconnected relationships among entities involved
152 in creating or deploying systems, products, or services.

¹ There are many publications that provide an in-depth treatment on the background of privacy or different aspects of the concept. For two examples, see 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>.

Change the figure to illustrate how Core feeds into profiles and profiles into Impl. Tiers, etc.

153 1.1 Overview of the Privacy Framework

154 As shown in **Figure 1**, the
 155 Privacy Framework is composed
 156 of three parts: the Core,
 157 Profiles, and Implementation
 158 Tiers. Each component
 159 reinforces *privacy risk*
 160 *management* through the
 161 connection between
 162 business/mission drivers and
 163 privacy protection activities. As
 164 further explained in section 2:

- 165 • The *Core* is a set of
 166 privacy protection
 167 activities and outcomes
 168 that allows for
 169 communicating
 170 prioritized privacy
 171 protection activities
 172 and outcomes across the

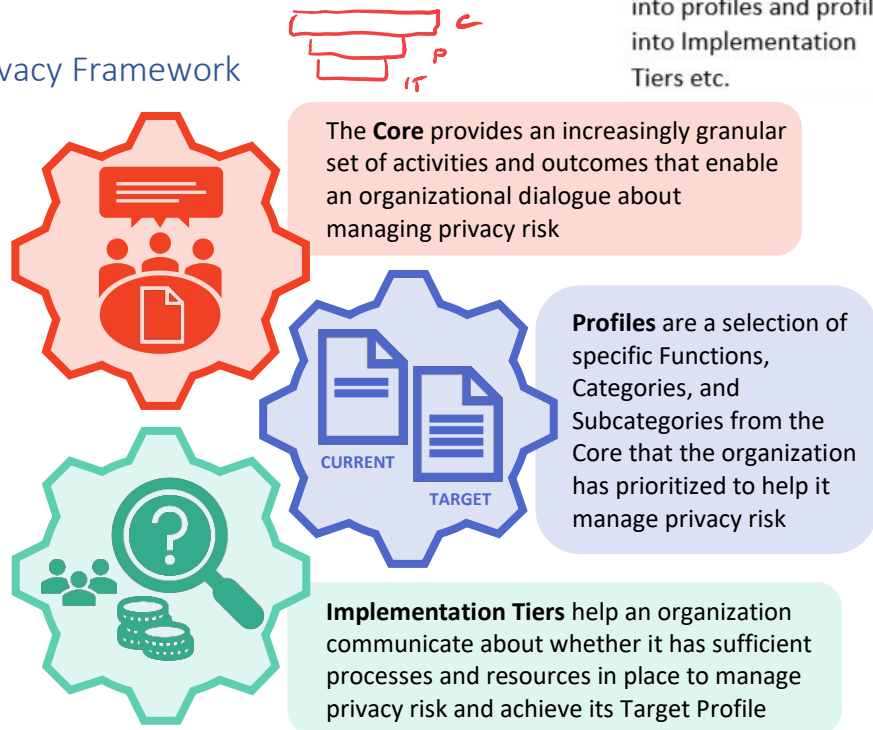


Figure 1: Core, Profiles, and Implementation Tiers

173 organization from the executive level to the implementation/operations level. There are five
 174 Functions: Identify-P, Govern-P, Control-P, Communicate-P, and Protect-P. The first four can be
 175 used to manage privacy risks arising from *data processing*, while Protect-P can help
 176 organizations manage privacy risks associated with *privacy breaches*.² Protect-P is not the only
 177 way to manage privacy risks associated with privacy breaches. For example, organizations may
 178 use the Cybersecurity Framework Functions in conjunction with the Privacy Framework to
 179 collectively address privacy and cybersecurity risks. The Core is further divided into key
 180 Categories and Subcategories—which are discrete outcomes—for each Function.

- 181 • A *Profile* represents the organization’s current privacy activities or desired outcomes. To
 182 develop a Profile, an organization can review all of the Functions, Categories, and Subcategories
 183 to determine which are most important to focus on based on business/mission drivers, types of
 184 data processing, and individuals’ privacy needs. The organization can create or add Functions,
 185 Categories, and Subcategories as needed. Profiles can be used to identify opportunities for
 186 improving privacy posture by comparing a “Current” Profile (the “as is” state) with a “Target”
 187 Profile (the “to be” state). Profiles can be used to conduct self-assessments and to communicate
 188 within an organization or between organizations about how privacy risks are being managed.
- 189 • *Implementation Tiers* (“Tiers”) provide a point of reference on how an organization views
 190 privacy risk and whether it has sufficient processes and resources in place to manage that risk.
 191 Tiers reflect a progression from informal, reactive responses to approaches that are agile and
 192 risk informed. When selecting Tiers, an organization should consider its Target Profile and how
 193 this relates to current risk management practices; its data processing systems, products, or

² The “-P” at the end of each Function name indicates that it is from the Privacy Framework in order to avoid confusion with Cybersecurity Framework Functions.

194 services; legal and regulatory requirements; business/mission objectives; organizational privacy
 195 values and individuals’ privacy needs; and organizational constraints.

196 **1.2 Privacy Risk Management**

197 While some organizations have a robust grasp of privacy risk management, a common understanding of
 198 many aspects of this topic is still not widespread.³ To promote broader understanding, this section
 199 covers concepts and considerations that organizations may use to develop, improve, or communicate
 200 about privacy risk management. Appendix D provides additional guidance on key privacy risk
 201 management practices.

202 **1.2.1 Cybersecurity and Privacy Risk Management**

203 Since its release in 2014, the
 204 Cybersecurity Framework has helped
 205 organizations to communicate and
 206 manage cybersecurity risk. [1] While
 207 managing cybersecurity risk
 208 contributes to managing privacy risk, it
 209 is not sufficient, as privacy risks can
 210 also arise outside the scope of
 211 cybersecurity risks. **Figure 2** illustrates
 212 how NIST considers the overlap and
 213 differences between cybersecurity
 214 and privacy risks.

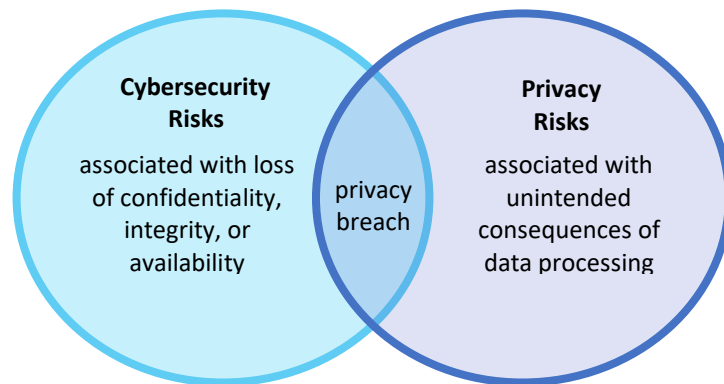


Figure 2: Cybersecurity and Privacy Risk Relationship

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

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

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

operations in the singular as a *data action* and collectively as data processing. The problems individuals can experience as a result of data processing can be expressed in various ways, but NIST describes them as ranging from dignity-type effects such as embarrassment or stigmas to more tangible harms such as discrimination, economic loss, or physical harm.⁴ Problems can arise as unintended consequences from data processing that organizations conduct to meet their mission or business objectives. An example is the concerns that certain communities had about the installation of “smart meters” as part of the Smart Grid, a nationwide technological effort to increase energy efficiency.⁵ 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

³ See *Summary Analysis of the Responses to the NIST Privacy Framework Request for Information* [2] at p. 7.

⁴ NIST has created an illustrative problem set for use in privacy risk assessment. See *NIST Privacy Risk Assessment Methodology* [3]. Other organizations may have created problem sets as well, or may refer to them as adverse consequences or harms.

⁵ See, for example, NIST Internal Report (IR) 7628 Revision 1 Volume 1, *Guidelines for Smart Grid Cybersecurity: Volume 1 – Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements* at [4] p. 26.

231 homes.⁶ The meters were operating as intended, but the data processing could lead to unintended
 232 consequences that people might feel surveilled.

233 However, these problems also can arise from privacy breaches where there is a loss of *confidentiality*,
 234 *integrity*, or *availability* at some point in the data processing, such as data theft by external attackers or
 235 the unauthorized access or use of data by employees who exceed their authorized privileges. **Figure 2**
 236 shows privacy breach as the overlap between a loss of confidentiality, integrity, or availability and
 237 unintended consequences of data processing for mission or business objectives.

238 Once an organization can identify the likelihood of any given problem arising from the data processing,
 239 which the Privacy Framework refers to as a *problematic data action*, it can assess the impact should the
 240 problematic data action occur. This impact assessment is where privacy risk and organizational risk
 241 intersect. Individuals, whether singly or in groups (including at a societal level) experience the direct
 242 impact of problems. As a result of the problems individuals experience, an organization may experience
 243 impacts such as noncompliance costs, customer abandonment of products and services, or harm to its
 244 external brand reputation or internal culture. These organizational impacts can be drivers for informed
 245 decision-making about resource allocation to strengthen privacy programs and to help organizations
 246 bring privacy risk into parity with other risks they are managing at the enterprise level. **Figure 3**
 247 illustrates this relationship between privacy risk and organizational risk.

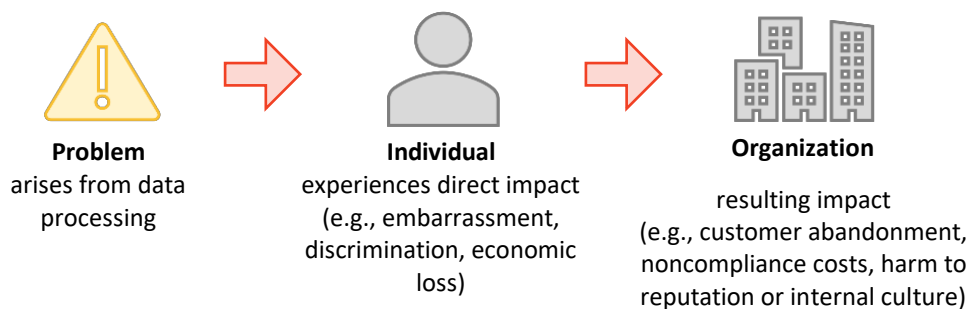


Figure 3: Relationship Between Privacy Risk and Organizational Risk

248 1.2.2 Relationship Between Privacy Risk Management and Risk Assessment

249 Privacy risk management is a cross-organizational set of processes that helps organizations to
 250 understand how their systems, products, and services may create problems for individuals and how to
 251 develop effective solutions to manage such risks. *Privacy risk assessment* is a sub-process for identifying,
 252 evaluating, prioritizing, and responding to specific privacy risks. In general, privacy risk assessments
 253 should produce the information that can help organizations to weigh the benefits of the data processing
 254 against the risks and to determine the appropriate response (see Appendix D for more guidance on the
 255 operational aspects of privacy risk assessment). Organizations may choose to respond to privacy risk in
 256 different ways, depending on the potential impact to individuals and resulting impacts to organizations.
 257 Approaches include:

- 258 • Mitigating the risk (e.g., organizations may be able to apply technical and/or policy measures to
 259 the systems, products, or services that minimize the risk to an acceptable degree);

⁶ See NIST IR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems* at [5] p. 2. For additional types of privacy risks associated with unintended consequences of data processing, see Appendix E of NIST IR 8062.

- 260 • Transferring or sharing the risk (e.g., contracts are a means of sharing or transferring risk to
261 other organizations, privacy notices and consent mechanisms are a means of sharing risk with
262 individuals);
- 263 • Avoiding the risk (e.g., organizations may determine that the risks outweigh the benefits, and
264 forego or terminate the data processing); or
- 265 • Accepting the risk (e.g., organizations may determine that problems for individuals are minimal
266 or unlikely to occur, therefore the benefits outweigh the risks, and it is not necessary to invest
267 resources in mitigation).

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

278 Lastly, privacy risk assessments help organizations distinguish between privacy risk and compliance risk.
279 Identifying if data processing could create problems for individuals, even when an organization may be
280 fully compliant with applicable laws or regulations, can help with ethical decision-making in system,
281 product, and service design or deployment. This facilitates optimizing beneficial uses of data while
282 minimizing adverse consequences for individuals' privacy and society as a whole, as well as avoiding
283 losses of trust that damage organizations' reputations, slow adoption, or cause abandonment of
284 products and services.

285 1.3 Document Overview

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

- 287 • Section 2 describes the Privacy Framework components: the Core, Profiles, and Implementation
288 Tiers.
- 289 • Section 3 presents examples of how the Privacy Framework can be used.
- 290 • Appendix A presents the Privacy Framework Core in a tabular format: Functions, Categories, and
291 Subcategories.
- 292 • Appendix B contains a glossary of selected terms.
- 293 • Appendix C lists acronyms used in this document.
- 294 • Appendix D considers key practices that contribute to successful privacy risk management.
- 295 • Appendix E defines the Implementation Tiers.
- 296 • Appendix F provides a placeholder for a companion roadmap covering NIST's next steps and
297 identifying key areas where the relevant practices are not well enough understood to enable
298 organizations to achieve a privacy outcome.
- 299 • Appendix G lists the references for this document.

300 2.0 Privacy Framework Basics

301 The Privacy Framework provides a common language for understanding, managing, and communicating
 302 privacy risk with internal and external stakeholders. It can be used to help identify and prioritize actions
 303 for reducing privacy risk, and it is a tool for aligning policy, business, and technological approaches to
 304 managing that risk. Different types of entities—including sector-specific organizations—can use the
 305 Privacy Framework for different purposes, including the creation of common Profiles.

306 2.1 Core

307 The Core provides a set of activities and outcomes that enable an organizational
 308 dialogue about managing privacy risk. The
 309 Core comprises three elements:
 310 Functions, Categories, and Subcategories,
 311 depicted in **Figure 4**.

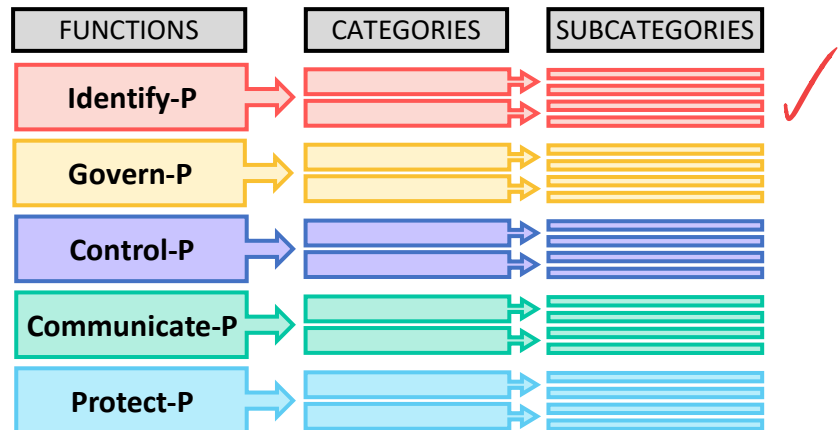


Figure 4: Privacy Framework Core Structure

313 The Core elements work together:

- 314 • *Functions* organize foundational
 315 privacy activities at their highest
 316 level. They aid an organization in
 317 expressing its management of
 318 privacy risk by understanding and managing data processing, enabling *risk management*
 319 decisions, determining how to interact with individuals, and improving by learning from
 320 previous activities. There are five Functions: Identify-P, Govern-P, Control-P, Communicate-P,
 321 and Protect-P. The first four can be used to manage privacy risks arising from data processing,
 322 while Protect-P can help organizations manage privacy risks associated with privacy breaches.⁷
 323 Protect-P is not the only way to manage privacy risks associated with privacy breaches. For
 324 example, organizations may use the Cybersecurity Framework Functions in conjunction with the
 325 Privacy Framework to collectively address privacy and cybersecurity risks.
- 326 • *Categories* are the subdivisions of a Function into groups of privacy outcomes closely tied to
 327 programmatic needs and particular activities. Examples include: “Disassociated Processing,”
 328 “Inventory and Mapping,” and “Risk Assessment.”
- 329 • *Subcategories* further divide a Category into specific outcomes of technical and/or management
 330 activities. They provide a set of results that, while not exhaustive, help support achievement of
 331 the outcomes in each Category. Examples include: “Systems/products/services that process data
 332 are inventoried,” “Data are processed to limit the identification of individuals (e.g., differential
 333 privacy techniques, tokenization),” and “Data corrections or deletions can be communicated to
 334 individuals or organizations (e.g., data sources) in the data processing ecosystem.”

335 The five Functions, defined below, are not intended to form a serial path or lead to a static desired end
 336 state. Rather, the Functions should be performed concurrently and continuously to form or enhance an
 337 operational culture that addresses the dynamic nature of privacy risk. See Appendix A for the complete
 338 Core.

⁷ The “-P” at the end of each Function name indicates that it is from the Privacy Framework in order to avoid confusion with Cybersecurity Framework Functions.

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

341 The activities in the Identify-P Function are foundational for effective use of the Privacy
342 Framework. Inventorying the circumstances under which data are processed, understanding the
343 privacy interests of individuals directly or indirectly served or affected by the organization, and
344 conducting risk assessments enable an organization to understand the business environment in
345 which it is operating and identify and prioritize privacy risks. Examples of Categories include:
346 “Inventory and Mapping,” “Business Environment,” and “Risk Assessment.”

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

350 The Govern-P Function is similarly foundational, but focuses on organizational-level activities
351 such as establishing organizational privacy values and policies, identifying legal/regulatory
352 requirements, and understanding organizational risk tolerance that enable an organization to
353 focus and prioritize its efforts, consistent with its risk management strategy and business needs.
354 Examples of Categories include: “Governance Policies, Processes, and Procedures,” “Risk
355 Management Strategy,” and “Monitoring and Review.”

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

358 The Control-P Function considers data management from both the standpoint of the
359 organization and the individual. Examples of Categories include: “Data Management Policies,
360 Processes, and Procedures” and “Data Management.”

- 361 • *Communicate-P* – Develop and implement appropriate activities to enable organizations and
362 individuals to have a reliable understanding about how data are processed and associated
363 privacy risks.

364 The Communicate-P Function recognizes that both organizations and individuals need to know
365 how data are processed in order to manage privacy risk effectively. Examples of Categories
366 include: “Communication Policies, Processes, and Procedures” and “Data Processing
367 Awareness.”

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

369 The Protect-P Function covers data protection to prevent privacy breaches, the overlap between
370 privacy and cybersecurity risk management. Examples of Categories include: “Identity
371 Management, Authentication, and Access Control,” “Data Security,” and “Protective
372 Technology.”

373 2.2 Profiles

374 Profiles are a selection of specific Functions, Categories, and Subcategories from the Core that the
375 organization has prioritized to help it manage privacy risk. Profiles align the Functions, Categories, and
376 Subcategories with the business requirements, risk tolerance, privacy values, and resources of the
377 organization. Under the Privacy Framework’s risk-based approach, organizations may not need to
378 achieve every outcome or activity reflected in the Core. When developing a Profile, an organization may
379 select or tailor the Privacy Framework’s Functions, Categories, and Subcategories to its specific needs.
380 An organization or industry sector also may develop its own additional Functions, Categories, and

381 Subcategories to account for unique organizational risks. An organization determines these needs by
 382 considering organizational or industry sector goals, legal/regulatory requirements and industry best
 383 practices, the organization’s risk management priorities, and the privacy needs of individuals who are
 384 part of—or directly or indirectly served or affected by—an organization’s systems, products, or services.

385 Profiles can be used to describe the current state or the desired target state of specific privacy activities.
 386 As **Figure 5** reflects, a Current Profile indicates privacy outcomes that an organization is currently
 387 achieving, while a Target Profile indicates the outcomes needed to achieve the desired privacy risk
 388 management goals. The differences between the two Profiles enable an organization to identify gaps,
 389 develop an action plan for improvement, and gauge the resources that would be needed (e.g., staffing,
 390 funding) to achieve privacy goals. This forms the basis of an organization’s plan for reducing privacy risk
 391 in a cost-effective, prioritized manner. Profiles also can aid in communicating risk within and between
 392 organizations by helping organizations understand and compare the current or desired state of privacy
 393 outcomes.

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

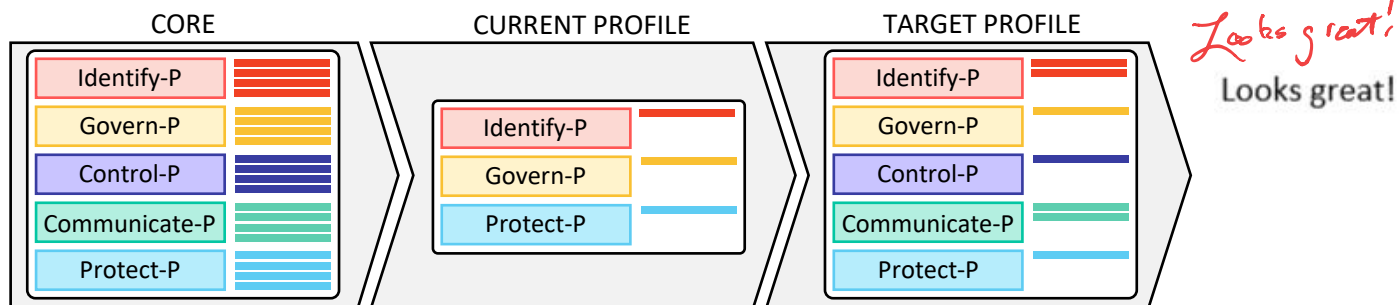


Figure 5: Profile Development Process

397 **2.3 Implementation Tiers**

398 Tiers support organizational decision-making about how to manage privacy risk by taking into account
 399 the nature of the privacy risks engendered by the organization’s systems, products, or services and the
 400 sufficiency of the processes and resources the organization has in place to manage such risks. When
 401 selecting Tiers, an organization should consider its current risk management practices; its data
 402 processing systems, products, or services; legal and regulatory requirements; business/mission
 403 objectives; organizational privacy values and individuals’ privacy needs; and organizational constraints.

404 There are four distinct tiers: Partial (Tier 1), Risk Informed (Tier 2), Repeatable (Tier 3), and Adaptive
 405 (Tier 4). Tiers do not represent maturity levels, although organizations identified as Tier 1 are
 406 encouraged to consider moving toward Tier 2. Some organizations may never need to achieve Tier 3 or 4
 407 or may only focus on certain areas of these tiers. Progression to higher Tiers is appropriate when an
 408 organization’s processes or resources at its current Tier are insufficient to help it manage its privacy
 409 risks.

410 An organization can use the Tiers to communicate with stakeholders whether it has sufficient resources
 411 and processes in place to achieve its Target Profile. This should influence the prioritization of elements
 412 included in a Target Profile, and should influence assessments of progress in addressing gaps. The
 413 definitions of the Tiers are set forth in Appendix E.

414 3.0 How to Use the Privacy Framework

415 When used as a risk management tool, the Privacy Framework can assist an organization in its efforts to
416 optimize beneficial uses of data and the development of innovative systems, products, and services
417 while minimizing adverse consequences for individuals. The Privacy Framework can help organizations
418 answer the fundamental question, “How are we considering the impacts to individuals as we develop
419 our systems, products, and services?” As a result, the Privacy Framework can serve as the foundation for
420 a new privacy program or a mechanism for improving an existing program. In either case, it is designed
421 to complement existing business and system development operations, to provide a means of expressing
422 *privacy requirements* to business partners and customers, and to support the identification of gaps in an
423 organization’s privacy practices.

424 To account for the unique needs of an organization, there are a wide variety of ways to use the Privacy
425 Framework. The decision about how to apply it is left to the implementing organization. For example,
426 one organization may choose to use the Implementation Tiers to articulate its envisioned privacy risk
427 management processes. Another organization may already have robust privacy risk management
428 processes, but may use the Core’s five Functions to analyze and articulate any gaps. Alternatively, an
429 organization seeking to establish a privacy program can use the Core’s Categories and Subcategories as a
430 reference. The variety of ways in which the Privacy Framework can be used by organizations should
431 discourage the notion of “compliance with the Privacy Framework” as a uniform or externally
432 referenceable concept.

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

434 3.1 Mapping to Informative References

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

443 Mapping Subcategories to specific sections of standards, guidelines, and practices supports the
444 achievement of the outcomes associated with each Subcategory. The Subcategories also can be used to
445 identify where additional or revised standards, guidelines, and practices would help an organization to
446 address emerging needs. An organization implementing a given Subcategory, or developing a new
447 Subcategory, might discover that there are insufficient informative references for a related activity. To
448 address that need, the organization might collaborate with technology leaders and/or standards bodies
449 to draft, develop, and coordinate standards, guidelines, or practices.

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

454 **3.2 Strengthening Accountability**

455 Accountability is generally considered a key privacy principle, although conceptually it is not unique to
 456 privacy.⁸ Accountability occurs throughout an organization, and it can be expressed at varying degrees
 457 of abstraction, for example as a cultural value, as governance policies and procedures, or as traceability
 458 relationships between privacy requirements and *controls*. Privacy risk management can be a means of
 459 supporting accountability at all organizational levels as it connects senior executives, who can
 460 communicate the organization’s privacy values and risk tolerance, to those at the business/process
 461 manager level, who can collaborate on the development and implementation of governance policies and
 462 procedures that support the organizational privacy values. These policies and procedures can then be
 463 communicated to those at the implementation/operations level, who collaborate on defining the
 464 privacy requirements that support the expression of the policies and procedures in the organization’s
 465 systems, products, and services. Personnel at the implementation/operations level also select,
 466 implement, and assess controls as the technical and policy measures that meet the privacy
 467 requirements, and report upward on progress, gaps and deficiencies, and changing privacy risks so that
 468 those at the business/process manager level and the senior executives can better understand and
 469 respond appropriately.

470 **Figure 6** provides a graphical representation of this iterative cycle and how elements of the Privacy
 471 Framework can be incorporated to facilitate the process. In this way, organizations can use the Privacy

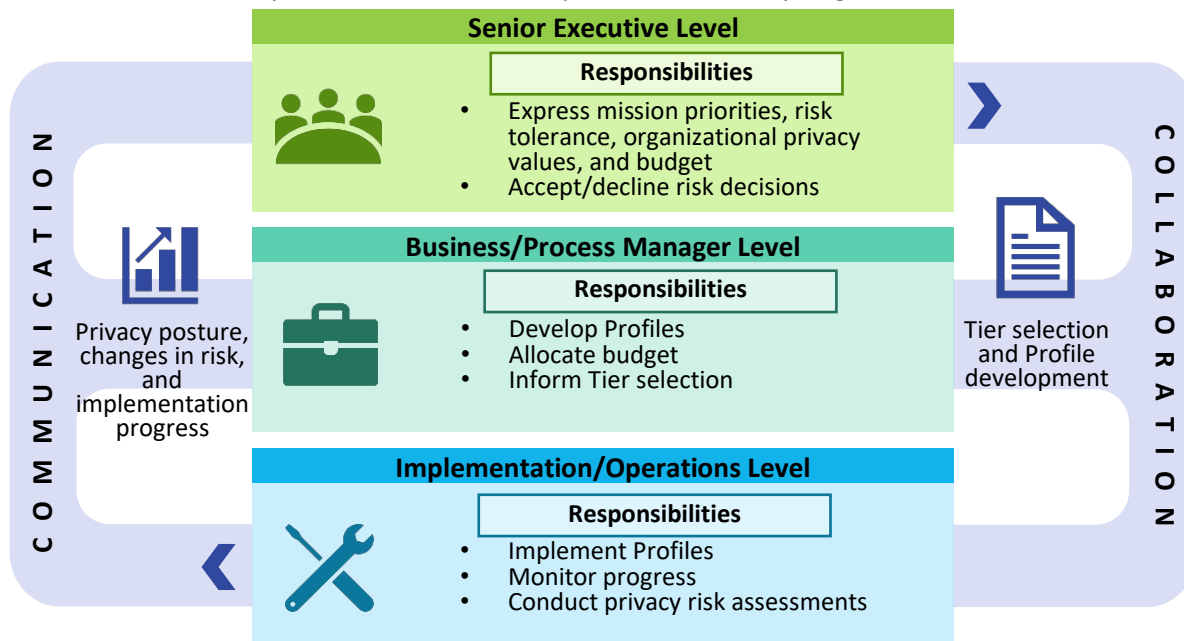


Figure 6: Notional Collaboration and Communication Flows Within an Organization

⁸ 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/oecdguidelinesonthe protectionofprivacyandtransborderflows ofpersonald ata.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>; 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>.

472 Framework as a tool to support accountability. They can also use the Privacy Framework in conjunction
 473 with other frameworks and guidance that provide additional practices to achieve accountability within
 474 and between organizations (see section 3.5 on Use within the Data Processing Ecosystem).⁹

475 3.3 Establishing or Improving a Privacy Program

476 Using a simple model of “ready, set, go” phases, the Privacy
 477 Framework can support the creation of a new privacy program or
 478 improvement of an existing program. These phases should be
 479 repeated as necessary to continuously improve privacy.

480 Ready

481 Effective privacy risk management requires an organization to
 482 understand its business or mission environment; its legal
 483 environment; its enterprise risk tolerance; the privacy risks
 484 engendered by its systems, products, or services; and its role or
 485 relationship to other organizations in the ecosystem. An
 486 organization can use the Identify-P and Govern-P Functions to “get
 487 ready” by reviewing the Categories and Subcategories, and
 488 beginning to develop its Current Profile and Target Profile.¹⁰

489 An organization conducts privacy risk assessments pursuant to the
 490 Risk Assessment category of the Identify Function. It is important
 491 that an organization identifies emerging privacy risks to gain a
 492 better understanding of the impacts of its systems, products, or services on individuals. See Appendix D
 493 for more information on privacy risk assessments.

494 Set

495 The organization completes its Current Profile by indicating which Category and Subcategory outcomes
 496 from the remaining Functions are being achieved. If an outcome is partially achieved, noting this fact will
 497 help support subsequent steps by providing baseline information. Informed by its privacy risk
 498 assessment, the organization creates its Target Profile focused on the assessment of the Categories and
 499 Subcategories describing the organization’s desired privacy outcomes. An organization also may develop
 500 its own additional Functions, Categories, and Subcategories to account for unique organizational risks. It
 501 may also consider influences and requirements of external stakeholders such as business customers and
 502 partners when creating a Target Profile. An organization can develop multiple Profiles to support its
 503 different business lines or processes, which may have different business needs and associated risk
 504 tolerances.

505 The organization compares the Current Profile and the Target Profile to determine gaps. Next, it creates
 506 a prioritized action plan to address gaps—reflecting mission drivers, costs and benefits, and risks—to
 507 achieve the outcomes in the Target Profile. An organization using the Cybersecurity Framework and the

A Simplified Method for Establishing or Improving a Privacy Program

Ready: use the Identify-P and Govern-P Functions 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.

⁹ See, e.g., NIST Special Publication (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>.

¹⁰ For additional guidance, see the “Prepare” step, Section 3.1, NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [6].

508 Privacy Framework together may develop integrated action plans. The organization then determines
509 resources, including funding and workforce, necessary to address the gaps, which can inform the
510 selection of an appropriate Tier. Using Profiles in this manner encourages the organization to make
511 informed decisions about privacy activities, supports risk management, and enables the organization to
512 perform cost-effective, targeted improvements.

513 Go

514 With the action plan “set,” the organization prioritizes which actions to take to address any gaps, and
515 then adjusts its current privacy practices in order to achieve the Target Profile.¹¹ For further guidance,
516 informative references that support outcome achievement for the Categories and Subcategories are
517 available at <https://www.nist.gov/privacy-framework>. The organization should determine which
518 standards, guidelines, and practices, including those that are sector specific, work best for its needs.

519 An organization can cycle through the phases nonsequentially as needed to continuously assess and
520 improve its privacy posture. For instance, an organization may find that more frequent repetition of the
521 Ready phase improves the quality of risk assessments. Furthermore, an organization may monitor
522 progress through iterative updates to the Current Profile or the Target Profile to adjust to changing risks,
523 subsequently comparing the Current Profile to the Target Profile. An organization may also use this
524 process to align its privacy program with its desired Tiers.

525 3.4 Applying to the System Development Life Cycle

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

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

¹¹ NIST SP 800-37 [6] provides additional guidance on steps to execute on the action plan, including control selection, implementation, and assessment to close any gaps.

545 3.5 Using within the Data Processing Ecosystem

546 The Privacy Framework provides
 547 a common language to
 548 communicate requirements with
 549 parties within the data
 550 processing ecosystem. As
 551 depicted in **Figure 7**, the data
 552 processing ecosystem
 553 encompasses a range of entities
 554 and roles that may have
 555 complex, multi-directional
 556 relationships with each other
 557 and individuals. Complexity can
 558 increase when entities are
 559 supported by a chain of sub-
 560 entities; for example, service
 561 providers may be supported by
 562 a series of service providers, or
 563 manufacturers may have
 564 multiple component suppliers.
 565 In addition, **Figure 7** displays
 566 entities as having distinct roles,
 567 but organizations may have
 568 multiple roles, such as an



569 **Figure 7: Data Processing Ecosystem Relationships**

569 organization providing services to other organizations and providing retail products to consumers. The
 570 roles in **Figure 7** are intended to be notional classifications. In practice, an organization’s role(s) may be
 571 legally codified—for example, some laws classify organizations as data controllers or data processors—
 572 or classifications may be derived from industry sector designations.

573 An organization should use the Privacy Framework from its standpoint in the data processing
 574 ecosystem and consider how to manage privacy risk not only with regard to its internal priorities, but
 575 also in relation to how they affect other parties’ management of privacy risk. An organization can use its
 576 Profiles to select Functions, Categories, and Subcategories that are relevant to its role(s). For example:

- 577 • An organization may use a Target Profile to express privacy risk management requirements to
 578 an external service provider (e.g., a cloud provider to which it is exporting data).
- 579 • An organization may express its privacy posture through a Current Profile to report results or to
 580 compare with acquisition requirements.
- 581 • An industry sector may establish a Target Profile that can be used among its constituents as an
 582 initial baseline Profile to build their own customized Target Profiles.
- 583 • An organization may use a Target Profile to determine the capabilities to build into its products
 584 so that its business customers can meet the privacy needs of their end users.

585 Communication is especially important among entities in the data processing ecosystem. Organizational
 586 practices should address this management of privacy risk, including identifying, assessing, and mitigating
 587 privacy risks arising from the processing of data, as well as from systems, products, and services that
 588 inherently lack the capabilities to mitigate privacy risks. Example activities may include:

- 589 • Determining privacy requirements for service providers,
- 590 • Enacting privacy requirements through formal agreement (e.g., contracts),
- 591 • Communicating to service providers how those privacy requirements will be verified and
- 592 validated,
- 593 • Verifying that privacy requirements are met through a variety of assessment methodologies,
- 594 and
- 595 • Governing and managing the above activities.

596 3.6 Informing Buying Decisions

597 Since either a Current or Target Profile can be used to generate a prioritized list of organizational privacy
598 requirements, these Profiles can also be used to inform decisions about buying products and services. By
599 first selecting outcomes that are relevant to its privacy goals, the organization then can evaluate
600 partners' systems, products, or services against this outcome. For example, if a device is being
601 purchased for environmental monitoring of a forest, *manageability* may be important to support
602 capabilities for minimizing the processing of data about people using the forest and should drive a
603 manufacturer evaluation against applicable Subcategories (e.g., CT.DP-P4 in Appendix A: system or
604 device configurations permit selective collection or disclosure of data elements).

605 In circumstances where it may not be possible to impose a set of privacy requirements on the supplier,
606 the objective should be to make the best buying decision among multiple suppliers, given a carefully
607 determined list of privacy requirements. Often, this means some degree of trade-off, comparing
608 multiple products or services with known gaps to the Profile. If the system, product, or service
609 purchased did not meet all of the objectives described in the Profile, the organization could address the
610 residual risk through mitigation measures or other management actions.

611 Appendix A: Privacy Framework Core

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

615 Note to Users

616 Under the Privacy Framework’s risk-based approach:

- 617 1. An organization may not need to achieve every outcome or activity reflected in the Core. It is
618 expected that an organization will use Profiles to select and prioritize the Functions, Categories,
619 and Subcategories that best meet its specific needs by considering its organizational or industry
620 sector goals, legal/regulatory requirements and industry best practices, the organization’s risk
621 management priorities, and the privacy needs of individuals who are directly or indirectly served
622 or affected by the organization’s systems, products, or services. **The Subcategories should not**
623 **be read as a checklist in isolation from their Categories, which often provide a risk-based**
624 **modifier on Subcategory selection.**
- 625 2. It is not obligatory to achieve an outcome in its entirety. An organization may use its Profiles to
626 express partial achievement of an outcome, as not all aspects of an outcome may be relevant
627 for the organization to manage privacy risk, or the organization may use a Target Profile to
628 express an aspect of an outcome that it does not currently have the capability to achieve.
- 629 3. It may be necessary to consider multiple outcomes in combination to appropriately manage
630 privacy risk. For example, an organization that responds to individuals’ requests for data access
631 may select for its Profile both the Subcategory CT.DM-P1: “Data elements can be accessed for
632 review” and the Category “Identity Management, Authentication, and Access Control” (PR.AC-P)
633 to ensure that only the individual to whom the data pertain gets access.

634 **Implementation:** The table format of the Core is not intended to suggest a specific implementation
635 order or imply a degree of importance between the Functions, Categories, and Subcategories.
636 Implementation may be nonsequential, simultaneous, or iterative, depending on the SDLC stage, status
637 of the privacy program, or scale of the workforce. In addition, the Core is not exhaustive; it is extensible,
638 allowing organizations, sectors, and other entities to adapt or add additional Functions, Categories, and
639 Subcategories to their Profiles.

640 Roles:

- 641 • **Workforce:** Different parts of an organization’s workforce may take responsibility for different
642 Categories or Subcategories. For example, the legal department may be responsible for carrying
643 out activities under “Governance Policies, Processes, and Procedures” while the IT department
644 is working on “Inventory and Mapping.” Ideally, the Core encourages cross-organization
645 collaboration to develop Profiles and achieve outcomes.
- 646 • **Ecosystem:** The Core is intended to be usable by any organization or entity regardless of its role
647 in the data processing ecosystem. Although the Privacy Framework does not classify ecosystem
648 roles, an organization should review the Core from its standpoint in the ecosystem. An
649 organization’s role(s) may be legally codified—for example, some laws classify organizations as
650 data controllers or data processors—or classifications may be derived from industry
651 designations. Since Core elements are not assigned by ecosystem role, an organization can use
652 its Profiles to select Functions, Categories, and Subcategories that are relevant to its role(s).

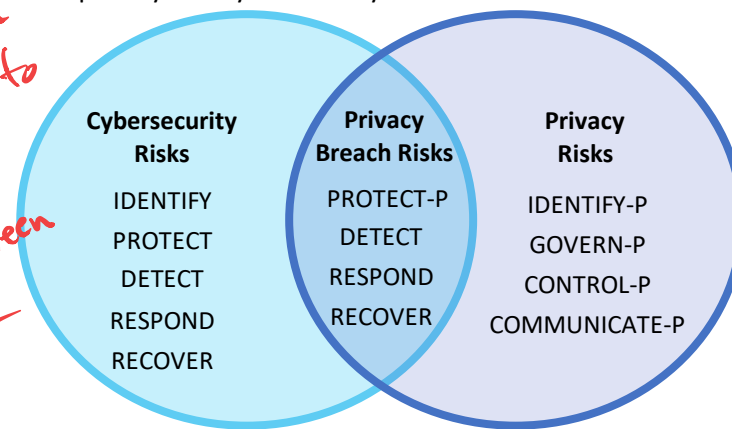
653 **Scalability:** Certain aspects of outcomes may be ambiguously worded. For example, outcomes may
 654 include terms like “communicated” or “disclosed” without stating to whom the communications or
 655 disclosures are being made. The ambiguity is intentional to allow for a wide range of organizations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

657 **Resource Repository:** Additional supporting resources, including informative references that can
 658 provide more guidance on how to achieve an outcome can be found on the NIST website at
 659 <https://www.nist.gov/privacy-framework>.

660 **Cybersecurity Framework Alignment:**

- 661 • **Figure 8** uses the Venn diagram from section 1.2.1 to demonstrate that the Privacy Framework
 662 Functions: Identify-P, Govern-P, Control-P, and Communicate-P can be used to manage privacy
 663 risks arising from data processing. Protect-P, Detect, Respond, and Recover can help
 664 organizations manage privacy risks associated with privacy breaches. Because Detect, Respond,
 665 and Recover are *cybersecurity incident*-related, these Functions are greyed out in **Table 1**
 666 because they are not part of the Privacy Framework, although organizations can find them in
 667 the Cybersecurity Framework and use them to further support the management of the privacy
 668 breach aspect of privacy risk. Alternatively, organizations may use the Cybersecurity Framework
 669 Functions in conjunction with Identify-P, Govern-P, Control-P, and Communicate-P to
 670 collectively address privacy and cybersecurity risks.



*Maybe change the
 cybersecurity Risks to
 end w/ "-C" to
 better differentiate between
 cybersecurity + privacy*



Maybe change the cybersecurity risks to end w/ “-C” to better differentiate between cybersecurity and privacy

Figure 8: Using Functions to Manage Privacy Risk

- 671 • Certain Categories or Subcategories may be identical to or have been adapted from the
 672 Cybersecurity Framework. The following legend can be used to identify this relationship in **Table**
 673 **2**.

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

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

682

Table 1: Privacy Framework Function and Category Unique Identifiers

683

Function Unique Identifier	Function	Category Unique Identifier	Category
ID-P	Identify-P	ID.IM-P	Inventory and Mapping
		ID.BE-P	Business Environment
		ID.RA-P	Risk Assessment
		ID.DE-P	Data Processing Ecosystem Risk Management
GV-P	Govern-P	GV.PP-P	Governance Policies, Processes, and Procedures
		GV.RM-P	Risk Management Strategy
		GV.AT-P	Awareness and Training
		GV.MT-P	Monitoring and Review
CT-P	Control-P	CT.PO-P	Data Management Policies, Processes, and Procedures
		CT.DM-P	Data Management
		CT.DP-P	Disassociated Processing
CM-P	Communicate-P	CM.PP-P	Communication Policies, Processes, and Procedures
		CM.AW-P	Data Processing Awareness
PR-P	Protect-P	PR.AC-P	Identity Management, Authentication, and Access Control
		PR.DS-P	Data Security
		PR.DP-P	Data Protection Policies, Processes, and Procedures
		PR.MA-P	Maintenance
		PR.PT-P	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Table 2: Privacy Framework Core

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

Function	Category	Subcategory	
	<p>Risk Assessment (ID.RA-P): The organization understands the privacy risks to individuals and how such privacy risks may create follow-on impacts on organizational operations, including mission, functions, other risk management priorities (e.g., compliance, financial), reputation, workforce, and culture.</p>	<p>ID.RA-P1: Contextual factors related to the systems/products/services and the data actions are identified (e.g., individuals’ demographics and privacy interests or perceptions, data sensitivity, visibility of data processing to individuals and third parties).</p> <p>ID.RA-P2: Data analytic inputs and outputs are identified and evaluated for bias.</p> <p>ID.RA-P3: Potential problematic data actions and associated problems are identified.</p> <p>ID.RA-P4: Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.</p> <p>ID.RA-P5: Risk responses are identified, prioritized, and implemented.</p>	
	<p>Data Processing Ecosystem Risk Management (ID.DE-P): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing privacy risk and third parties within the data processing ecosystem. The organization has established and implemented the processes to identify, assess, and manage privacy risks within the data processing ecosystem.</p>	<p>ID.DE-P1: Data processing ecosystem risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.</p> <p>ID.DE-P2: Data processing ecosystem parties (e.g., service providers, customers, partners, product manufacturers, application developers) are identified, prioritized, and assessed using a privacy risk assessment process.</p> <p>ID.DE-P3: Contracts with data processing ecosystem parties are used to implement appropriate measures designed to meet the objectives of an organization’s privacy program.</p> <p>ID.DE-P4: Interoperability frameworks or similar multi-party approaches are used to manage data processing ecosystem privacy risks.</p> <p>ID.DE-P5: Data processing ecosystem parties are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual or framework obligations.</p>	
	<p>GOVERN-P (GV-P): Develop and implement the</p>	<p>Governance Policies, Processes, and Procedures (GV.PP-P): The policies, processes, and procedures to manage and</p>	<p>GV.PP-P1: Organizational privacy values and policies (e.g., conditions on data processing, individuals’ prerogatives with respect to data processing) are established and communicated.</p>

Function	Category	Subcategory
organizational governance structure to enable an ongoing understanding of the organization’s risk management priorities that are informed by privacy risk.	monitor the organization’s regulatory, legal, risk , environmental, and operational requirements are understood and inform the management of privacy risk .	GV.PP-P2: Processes to instill organizational privacy values within system/product/service development and operations are established and in place.
		GV.PP-P3: Roles and responsibilities for the workforce are established with respect to privacy.
		GV.PP-P4: Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners).
		GV.PP-P5: Legal, regulatory, and contractual requirements regarding privacy are understood and managed.
		GV.PP-P6: Governance and risk management policies, processes, and procedures address privacy risks.
		Risk Management Strategy (GV.RM-P): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
		GV.RM-P2: Organizational risk tolerance is determined and clearly expressed.
		GV.RM-P3: The organization’s determination of risk tolerance is informed by its role in the data processing ecosystem .
		Awareness and Training (GV.AT-P): The organization’s workforce and third parties engaged in data processing are provided privacy awareness education and are trained to perform their privacy-related duties and responsibilities consistent with related policies, processes, procedures, and agreements and organizational privacy values.
		GV.AT-P2: Senior executives understand their roles and responsibilities.
		GV.AT-P3: Privacy personnel understand their roles and responsibilities.
		GV.AT-P4: Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities.
	Monitoring and Review (GV.MT-P): The policies, processes, and procedures for ongoing review of the organization’s privacy	GV.MT-P1: Privacy risk is re-evaluated on an ongoing basis and as key factors, including the organization’s business environment, governance (e.g., legal obligations, risk tolerance), data processing , and systems/products/services change.

Function	Category	Subcategory
	posture are understood and inform the management of privacy risk .	GV.MT-P2: Privacy values, policies, and training are reviewed and any updates are communicated.
		GV.MT-P3: Policies, processes, and procedures for assessing compliance with legal requirements and privacy policies are established and in place.
		GV.MT-P4: Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place.
		GV.MT-P5: Policies, processes, and procedures are established and in place to receive, analyze, and respond to problematic data actions disclosed to the organization from internal and external sources (e.g., internal discovery, privacy researchers).
		GV.MT-P6: Policies, processes, and procedures incorporate lessons learned from problematic data actions.
		GV.MT-P7: Policies, processes, and procedures for receiving, tracking, and responding to complaints, concerns, and questions from individuals about organizational privacy practices are established and in place.
		CONTROL-P (CT-P): Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.
CT.PO-P2: Policies, processes, and procedures for enabling data review, transfer, sharing or disclosure, alteration, and deletion are established and in place.		
CT.PO-P3: Policies, processes, and procedures for enabling individuals’ data processing preferences and requests are established and in place.		
CT.PO-P4: An information life cycle to manage data is aligned and implemented with the system development life cycle to manage systems.		
Data Management (CT.DM-P): Data are managed consistent with the organization’s risk strategy to protect individuals’ privacy,	CT.DM-P1: Data elements can be accessed for review.	
CT.DM-P2: Data elements can be accessed for transmission or disclosure.		

Function	Category	Subcategory	
	increase manageability , and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization).	<p>CT.DM-P3: Data elements can be accessed for alteration.</p> <p>CT.DM-P4: Data elements can be accessed for deletion.</p> <p>CT.DM-P5: Data are destroyed according to policy.</p> <p>CT.DM-P6: Data are transmitted using standardized formats.</p> <p>CT.DM-P7: Metadata containing processing permissions and related data values are transmitted with data elements.</p> <p>CT.DM-P8: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.</p>	
	<p>Disassociated Processing (CT.DP-P): Data processing solutions increase disassociability consistent with related policies, processes, procedures, and agreements and the organization’s risk strategy to protect individuals’ privacy.</p>	<p>CT.DP-P1: Data are processed in an unobservable or unlinkable manner (e.g., data actions take place on local devices, privacy-preserving cryptography).</p> <p>CT.DP-P2: Data are processed to limit the identification of individuals (e.g., differential privacy techniques, tokenization).</p> <p>CT.DP-P3: Data are processed to restrict the formulation of inferences about individuals’ behavior or activities (e.g., data processing is decentralized, distributed architectures).</p> <p>CT.DP-P4: System or device configurations permit selective collection or disclosure of data elements.</p> <p>CT.DP-P5: Attribute references are substituted for attribute values.</p> <p>CT.DP-P6: Data processing is limited to that which is relevant and necessary for a system/product/service to meet mission/business objectives.</p>	
	<p>COMMUNICATE-P (CM-P): Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding</p>	<p>Communication Policies, Processes, and Procedures (CM.PP-P): Policies, processes, and procedures are maintained and used to increase transparency of the organization’s data processing practices (e.g., purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities) and associated privacy risks.</p>	<p>CM.PP-P1: Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established and in place.</p> <p>CM.PP-P2: Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established.</p>

Function	Category	Subcategory
<p>about how data are processed and associated privacy risks.</p>	<p>Data Processing Awareness (CM.AW-P): Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the organization's risk strategy to protect individuals' privacy.</p>	<p>CM.AW-P1: Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place.</p>
		<p>CM.AW-P2: Mechanisms for obtaining feedback from individuals (e.g., surveys or focus groups) about data processing and associated privacy risks are established and in place.</p>
		<p>CM.AW-P3: System/product/service design enables data processing visibility.</p>
		<p>CM.AW-P4: Records of data disclosures and sharing are maintained and can be accessed for review or transmission/disclosure.</p>
		<p>CM.AW-P5: Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem.</p>
		<p>CM.AW-P6: Data provenance and lineage are maintained and can be accessed for review or transmission/disclosure.</p>
		<p>CM.AW-P7: Impacted individuals and organizations are notified about a privacy breach or event.</p>
		<p>CM.AW-P8: Individuals are provided with mitigation mechanisms to address impacts to individuals that arise from data processing.</p>
<p>PROTECT-P (PR-P): Develop and implement appropriate data processing safeguards.</p>	<p>Identity Management, Authentication, and Access Control (PR.AC-P): Access to data and devices is limited to authorized individuals, processes, and devices, and is managed consistent with the assessed risk of unauthorized access.</p>	<p>PR.AC-P1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.</p>
		<p>PR.AC-P2: Physical access to data and devices is managed.</p>
		<p>PR.AC-P3: Remote access is managed.</p>
		<p>PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.</p>
		<p>PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).</p>

Function	Category	Subcategory
		PR.AC-P6: 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).
	Data Security (PR.DS-P): Data are managed consistent with the organization’s risk strategy to protect individuals’ privacy and maintain data confidentiality , integrity , and availability .	PR.DS-P1: Data-at-rest are protected.
		PR.DS-P2: Data-in-transit are protected.
		PR.DS-P3: Systems/products/services and associated data are formally managed throughout removal, transfers, and disposition.
		PR.DS-P4: Adequate capacity to ensure availability is maintained.
		PR.DS-P5: Protections against data leaks are implemented.
		PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.
		PR.DS-P7: The development and testing environment(s) are separate from the production environment.
		PR.DS-P8: Integrity checking mechanisms are used to verify hardware integrity.
	Data Protection Policies, Processes, and Procedures (PR.DP-P): Security and privacy policies (which 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 .	PR.DP-P1: A baseline configuration of information technology is created and maintained incorporating security principles (e.g., concept of least functionality).
		PR.DP-P2: Configuration change control processes are established and in place.
		PR.DP-P3: Backups of information are conducted, maintained, and tested.
		PR.DP-P4: Policy and regulations regarding the physical operating environment for organizational assets are met.
		PR.DP-P5: Protection processes are improved.
		PR.DP-P6: Effectiveness of protection technologies is shared.
PR.DP-P7: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed.		
PR.DP-P8: Response and recovery plans are tested.		

Function	Category	Subcategory
		<p>PR.DP-P9: Privacy procedures are included in human resources practices (e.g., deprovisioning, personnel screening).</p>
		<p>PR.DP-P10: A vulnerability management plan is developed and implemented.</p>
	<p>Maintenance (PR.MA-P): System maintenance and repairs are performed consistent with policies, processes, and procedures.</p>	<p>PR.MA-P1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.</p>
	<p>PR.MA-P2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.</p>	
	<p>Protective Technology (PR.PT-P): Technical security solutions are managed to ensure the security and resilience of systems/products/services and associated data, consistent with related policies, processes, procedures, and agreements.</p>	<p>PR.PT-P1: Removable media is protected and its use restricted according to policy.</p>
		<p>PR.PT-P2: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.</p>
		<p>PR.PT-P3: Communications and control networks are protected.</p>
		<p>PR.PT-P4: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.</p>

685

686 **Appendix B: Glossary**

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

Attribute Reference (NIST SP 800-63-3 [7])	A statement asserting a property of a subscriber without necessarily containing identity information, independent of format. For example, for the attribute “birthday,” a reference could be “older than 18” or “born in December.”
Attribute Value (NIST SP 800-63-3 [7])	A complete statement asserting a property of a subscriber, independent of format. For example, for the attribute “birthday,” a value could be “12/1/1980” or “December 1, 1980.”
Availability [NIST SP 800-37 [6]]	Ensuring timely and reliable access to and use of information.
Category	The subdivision of a Function into groups of privacy outcomes closely tied to programmatic needs and particular activities.
Communicate-P (Function)	Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding about how data are processed and associated privacy risks.
Confidentiality [NIST SP 800-37 [6]]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Control-P (Function)	Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.
Core	A set of privacy protection activities and outcomes. The Framework Core comprises three elements: Functions, Categories, and Subcategories.
Cybersecurity Incident (OMB 17-12 [8])	An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
Data	A representation of information, including digital and non-digital formats.
Data Action (Adapted from NIST IR 8062 [5])	A system/product/service data life cycle operation, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal. <i>of PII</i>
Data Element	The smallest named item of data that conveys meaningful information.
Data Processing (Adapted from NIST IR 8062 [5])	The collective set of data actions (i.e., the complete data life cycle, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal).
Data Processing Ecosystem	The complex and interconnected relationships among entities involved in creating or deploying systems, products, or services or any components that process data.
Disassociability (Adapted from NIST IR 8062 [5])	Enabling the processing of data or events without association to individuals or devices beyond the operational requirements of the system.
Function	A component of the Core that provides the highest level of structure for organizing basic privacy activities into Categories and Subcategories.

of PII.

Govern-P (Function)	Develop and implement the organizational governance structure to enable an ongoing understanding of the organization’s risk management priorities that are informed by privacy risk.
Identify-P (Function)	Develop the organizational understanding to manage privacy risk for individuals arising from data processing.
Implementation Tier	Provides a point of reference on how an organization views privacy risk and whether it has sufficient processes and resources in place to manage that risk.
Individual	A single person or a group of persons, including at a societal level.
Integrity [NIST SP 800-37 [6]]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Lineage	The history of processing of a data element, which may include point-to-point data flows and the data actions performed upon the data element.
Manageability (Adapted from NIST IR 8062 [5])	Providing the capability for granular administration of data, including alteration, deletion, and selective disclosure.
Metadata (Adapted from NIST SP 800-53 [9])	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.
Predictability (Adapted from NIST IR 8062 [5])	Enabling reliable assumptions by individuals, owners, and operators about data and its processing by a system, product, or service.
Privacy Breach (Adapted from OMB M-17-12 [8])	The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses data or (2) an authorized user accesses data for an other than authorized purpose.
Privacy Control [Adapted from NIST SP 800-37 [6]]	The administrative, technical, and physical safeguards employed within an organization to satisfy privacy requirements.
Privacy Requirement	A specification for system/product/service functionality to meet stakeholders’ desired privacy outcomes.
Privacy Risk	The likelihood that individuals will experience problems resulting from data processing, and the impact should they occur.
Privacy Risk Assessment	A privacy risk management sub-process for identifying, evaluating, prioritizing, and responding to specific privacy risks.
Privacy Risk Management	A cross-organizational set of processes for identifying, assessing, and responding to privacy risks.
Problematic Data Action (Adapted from NIST IR 8062 [5])	A data action that could cause an adverse effect for individuals.
Processing	See <i>Data Processing</i> .
Profile	A selection of specific Functions, Categories, and Subcategories from the Core that the organization has prioritized to help it manage privacy risk.
Protect-P (Function)	Develop and implement appropriate data processing safeguards.
Provenance (Adapted from NIST IR 8112 [10])	Metadata pertaining to the origination or source of specified data.

State that this may also be PII

State that this may also be PII

Risk (NIST SP 800-30 [11])	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Risk Management	The process of identifying, assessing, and responding to risk.
Subcategory	The further divisions of a Category into specific outcomes of technical and/or management activities.

688

There's no definition here of personal information. I recommend going w/ GDPR's definition which, in my experience, adequately describes what PII is.

There's no definition of personal information. I recommend going w/ GDPR's definition which, in my experience, adequately describes what PII is.

689 Appendix C: Acronyms

690 This appendix defines selected acronyms used in the publication.

691

692	IEC	International Electrotechnical Commission
693	IR	Internal Report
694	ISO	International Organization for Standardization
695	IT	Information Technology
696	NIST	National Institute of Standards and Technology
697	OASIS	Organization for the Advancement of Structured Information Standards
698	OECD	Organisation for Economic Co-operation and Development
699	OMB	Office of Management and Budget
700	PMRM	Privacy Management Reference Model and Methodology
701	PRAM	Privacy Risk Assessment Methodology
702	SDLC	System Development Life Cycle
703	SP	Special Publication

704 Appendix D: Privacy Risk Management Practices

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

712 Organizing Preparatory Resources

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

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

- 722 • **Risk management role assignments** (GV.PP-P3, GV.PP-P4)

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

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

733 An organization's enterprise risk management strategy helps to align the organization's mission
734 and values with organizational risk assumptions and constraints. Limitations on resources to
735 achieve mission/business objectives and to manage a broad portfolio of risks will likely require
736 trade-offs. Enabling personnel involved in the privacy risk management process to better
737 understand the organization's risk tolerance should help to guide decisions about how to
738 allocate resources and improve decisions around risk response.

- 739 • **Key stakeholders** (GV.PP-P4, ID.DE-P)

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

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

750 • **Organizational-level privacy requirements (GV.PP-P)**

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

- 756 ○ Legal environment (e.g., laws, regulations, contracts),
- 757 ○ Organizational policies or cultural values,
- 758 ○ Relevant standards, and
- 759 ○ Privacy principles.

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

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

767 • **Data maps (ID.IM-P)**

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

775 Determining Privacy Capabilities

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

785 In determining privacy capabilities, an organization may consider which of the privacy engineering and
786 security objectives are most important with respect to its mission/business needs, risk tolerance, and

787 organizational-level privacy requirements (see Organizing Preparatory Resources above). Not all of the
 788 objectives may be equally important, or trade-offs may be necessary among them. Although the privacy
 789 capabilities inform the privacy risk assessment by supporting risk prioritization decisions, the privacy
 790 capabilities may also be informed by the risk assessment and adjusted to support the management of
 791 specific privacy risks or address changes in the environment, including design changes to the system,
 792 product, or service.

793 **Table 3: Privacy Engineering and Security Objectives¹²**

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

794 **Defining Privacy Requirements**

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

¹² The privacy engineering objectives are adapted from NIST IR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems* [5]. 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* [6].

804 Conducting Privacy Risk Assessments

805 Conducting a privacy risk assessment helps an organization to identify privacy risks engendered by the
806 system, product, or service and prioritize them to be able to make informed decisions about how to
807 respond to the risks (ID.RA-P, GV.RM-P). Methodologies for conducting privacy risk assessments may
808 vary, but organizations should consider the following characteristics:¹³

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

810 Risk models define the risk factors to be assessed and the relationships among those factors.¹⁴ If
811 an organization is not using a pre-defined risk model, the organization should clearly define
812 which risk factors it will be assessing and the relationships among these factors. Although
813 cybersecurity has a widely used risk model
814 based on the risk factors of threats,
815 vulnerabilities, likelihood, and impact,
816 there is not one commonly accepted
817 privacy risk model. NIST has developed a
818 privacy risk model based on the risk factors of problematic data actions, likelihood, and impact,
819 each explained below.

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

- 820 ○ A problematic data action is any action a system takes to process data that could result in a
821 problem for individuals. Organizations consider the type of problems that are relevant to
822 the population of individuals. Problems can take any form and may consider the experience
823 of individuals singly or as a group.¹⁵
- 824 ○ Likelihood is defined as a contextual analysis that a data action is likely to create a problem
825 for a representative set of individuals. Context can include organizational factors (e.g., the
826 public perception about participating organizations with respect to privacy), system factors
827 (e.g., the nature and history of individuals' interactions with the system, visibility of data
828 processing to individuals and third parties), or individual factors (e.g., individuals'
829 demographics, privacy interests or perceptions, data sensitivity).¹⁶ A data map can help with
830 this contextual analysis (see Organizing Preparatory Resources).
- 831 ○ Impact is an analysis of the costs should the problem occur. As noted in section 1.2, the
832 experience of individuals is a type of externality for organizations. Moreover, individuals'
833 experiences may be subjective. Thus, impact may be difficult to assess accurately.
834 Organizations should consider the best means of internalizing impact to individuals in order
835 to appropriately prioritize and respond to privacy risks.¹⁷

¹³ 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 [3].

¹⁴ See NIST SP 800-30 Rev. 1, *Guide for Conducting Risk Assessments* at [11] p. 8.

¹⁵ As part of its PRAM, NIST has created an illustrative catalog of problematic data actions and problems for consideration [3]. Other organizations may have created additional problem sets, or may refer to them as adverse consequences or harms.

¹⁶ See NIST PRAM for more information about contextual factors. Id at Worksheet 2.

¹⁷ The NIST PRAM uses organizational costs such as non-compliance costs, direct business costs, reputational costs, and internal culture costs as drivers for considering how to assess individual impact. Id at Worksheet 3, Impact Tab.

- 836 • **Assessment approach**
- 837 The assessment approach is the mechanism by which identified risks are prioritized. Assessment
- 838 approaches can be categorized as quantitative, semi-quantitative, or qualitative.^{18 19}
- 839 • **Prioritizing risks** (ID.RA-P4)
- 840 Given the applicable limits of an organization’s resources, organizations prioritize the risks to
- 841 facilitate communication about how to respond.²⁰
- 842 • **Responding to risks** (ID.RA-P5)
- 843 As described in section 1.2.2, responding to risk is usually categorized as mitigation,
- 844 transfer/sharing, avoidance, or acceptance.²¹

845 Creating Privacy Requirements Traceability

846 Once the organization has determined which risks to mitigate, the organization can refine the privacy

847 requirements and then select and implement controls (i.e., technical and/or policy safeguards) to meet

848 the defined requirements.²² An organization may use a variety of sources to select controls, such as NIST

849 SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*.²³ After

850 implementation, an organization iteratively assesses the controls for their effectiveness in meeting the

851 privacy requirements and managing privacy risk. In this way, an organization creates traceability

852 between the controls and the privacy requirements, and demonstrates accountability between its

853 systems, products, and services and its organizational privacy goals.

854 Monitoring Changing Privacy Risks

855 Privacy risk management is not a static process. An organization monitors how changes in its business

856 environment and corresponding changes to its systems, products, and services may be affecting privacy

857 risk, and iteratively use the practices in this appendix to adjust accordingly. (GV.MT-P1)

¹⁸ See NIST SP 800-30 Rev. 1, *Guide for Conducting Risk Assessments* at [11] p. 14.

¹⁹ The NIST PRAM uses a semi-quantitative approach based on a scale of 1-10.

²⁰ The NIST PRAM provides various prioritization representations, including a heat map. See [3] Worksheet 3.

²¹ The NIST PRAM provides a process for responding to prioritized privacy risks. Id at Worksheet 4.

²² See NIST SP 800-37 Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* at [6].

²³ See NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, as updated at [9].

858 Appendix E: Implementation Tiers Definitions

859 The Tiers are defined through four areas summarized below:

860 Tier 1: Partial

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

878 Tier 2: Risk Informed

- 879 • **Privacy Risk Management Process** – Risk management practices are approved by management
880 but may not be established as organization-wide policy. Prioritization of privacy activities is
881 directly informed by organizational risk objectives, privacy risk assessments, and
882 business/mission requirements.
- 883 • **Integrated Privacy Risk Management Program** – There is an awareness of privacy risk at the
884 organizational level, but an organization-wide approach to managing privacy risk has not been
885 established. Information about data processing and resulting privacy risks is shared within the
886 organization on an informal basis. Consideration of privacy in organizational objectives and
887 programs may occur at some but not all levels of the organization. Privacy risk assessment
888 occurs, but is not typically repeatable or reoccurring.
- 889 • **Data Processing Ecosystem Relationships** – There is some understanding of an organization’s
890 role in the larger ecosystem with respect to other entities (e.g., buyers, suppliers, service
891 providers, business associates, partners). The organization is aware of the privacy ecosystem
892 risks associated with the products and services it provides and uses, but does not act
893 consistently or formally upon those risks.
- 894 • **Workforce** – There are personnel with specific privacy responsibilities, but they may have non-
895 privacy responsibilities as well. Privacy training is conducted regularly for privacy personnel,
896 although there is no consistent process for updates on best practices.

897 Tier 3: Repeatable

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

917 Tier 4: Adaptive

- 918 • **Privacy Risk Management Process** – The organization adapts its privacy practices based on
919 lessons learned from privacy breaches and events, and identification of new privacy risks.
920 Through a process of continuous improvement incorporating advanced privacy technologies and
921 practices, the organization actively adapts to a changing policy and technology landscape and
922 responds in a timely and effective manner to evolving privacy risks.
- 923 • **Integrated Privacy Risk Management Program** – There is an organization-wide approach to
924 managing privacy risk that uses risk-informed policies, processes, and procedures to address
925 problematic data actions. The relationship between privacy risk and organizational objectives is
926 clearly understood and considered when making decisions. Senior executives monitor privacy
927 risk in the same context as cybersecurity risk, financial risk, and other organizational risks. The
928 organizational budget is based on an understanding of the current and predicted risk
929 environment and risk tolerance. Business units implement executive vision and analyze system-
930 level risks in the context of the organizational risk tolerances. Privacy risk management is part of
931 the organizational culture and evolves from lessons learned and continuous awareness of data
932 processing and resulting privacy risks. The organization can quickly and efficiently account for
933 changes to business/mission objectives in how risk is approached and communicated.
- 934 • **Data Processing Ecosystem Relationships** – The organization understands its role,
935 dependencies, and dependents in the larger ecosystem and contributes to the community’s
936 broader understanding of risks. The organization uses real-time or near-real-time information to
937 understand and consistently act upon privacy ecosystem risks associated with the products and
938 services it provides and it uses. Additionally, it communicates proactively, using formal (e.g.,
939 agreements) and informal mechanisms to develop and maintain strong ecosystem relationships.

- 940 • **Workforce** – The organization has specialized privacy skillsets throughout the organizational
941 structure; personnel with diverse perspectives contribute to the management of privacy risks.
942 There is regular, up-to-date, specialized privacy training for all personnel. Personnel at all levels
943 understand the organizational privacy values and their role in maintaining them.

944

945 **Appendix F: Roadmap**

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

950 Appendix G: References

- [1] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). <https://doi.org/10.6028/NIST.CSWP.04162018>
- [2] National Institute of Standards and Technology (2019) Summary Analysis of the Responses to the NIST Privacy Framework Request for Information. (National Institute of Standards and Technology, Gaithersburg, MD). https://www.nist.gov/sites/default/files/documents/2019/02/27/rfi_response_analysis_privacyframework_2.27.19.pdf
- [3] National Institute of Standards and Technology (2019) NIST Privacy Risk Assessment Methodology (PRAM). (National Institute of Standards and Technology, Gaithersburg, MD). <https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources>
- [4] The Smart Grid Interoperability Panel—Smart Grid Cybersecurity Committee (2014) Guidelines for Smart Grid Cybersecurity: Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements. (National Institute of Standards and Technology, Gaithersburg, MD). NIST Internal Report (IR) 7628, Rev. 1, Vol. 1. <https://doi.org/10.6028/NIST.IR.7628r1>
- [5] Brooks S., Garcia M., Lefkovitz N., Lightman S., Nadeau E. (2017) An Introduction to Privacy Engineering and Risk Management in Federal Systems. (National Institute of Standards and Technology, Gaithersburg, MD). NIST Internal Report (IR) 8062. <https://doi.org/10.6028/NIST.IR.8062>
- [6] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD). NIST Special Publication (SP) 800-37 Rev. 2. <https://doi.org/10.6028/NIST.SP.800-37r2>
- [7] Grassi P., Garcia M., Fenton J. (2017) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD). NIST Special Publication (SP) 800-63-3. <https://csrc.nist.gov/publications/detail/sp/800-63/3/final>
- [8] Office of Management and Budget (OMB), *Preparing for and Responding to a Breach of Personally Identifiable Information*, OMB Memorandum 17-12, January 3, 2017. Available at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf
- [9] Joint Task Force (2017) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD). NIST Special Publication (SP) 800-53, multiple revisions. <https://csrc.nist.gov/publications/sp800-53>
- [10] Grassi P., Lefkovitz N., Nadeau E., Galluzzo R., Dinh A. (2018) Attribute Metadata: A Proposed Schema for Evaluating Federated Attributes. (National Institute of Standards and Technology, Gaithersburg, MD). NIST Internal Report (IR) 8112. <https://doi.org/10.6028/NIST.IR.8112>
- [11] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD). NIST Special Publication (SP) 800-30 Rev. 1. <https://doi.org/10.6028/NIST.SP.800-30r1>

951