Version 1.0

NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT, VERSION 1.0

January 16, 2020

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.01162020

The contents of this document do not have the force and effect of law and are not meant to bind the public in any way.

National Institute of Standards and Technology
U.S. Department of Commerce

版本 1.0

NIST 隐私框架：通过企业改进隐私的工具

风险管理，版本 1.0

January 16, 2020

本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.CSWP.01162020

本文档的内容不具有以下效力：
法律，且无意以任何方式约束公众。

National Institute of Standards and Technology
U.S. Department of Commerce

本译本由机器翻译生成，供快速理解条文与内部培训使用；
涉及合规判断或法律适用时，请咨询专业顾问，并以官方英文文本为准。
翻译您自己的文件，请选择桐鸾译馆 · https://www.ivyivy.com.cn
扫码关注服务号

Executive Summary

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

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

- Building customers' trust by supporting ethical decision-making in product and service design or deployment that optimizes beneficial uses of data while minimizing adverse consequences for individuals' privacy and society as a whole;[1]
- Fulfilling current compliance obligations, as well as future-proofing products and services to meet these obligations in a changing technological and policy environment; and
- Facilitating communication about privacy practices with individuals, business partners, assessors, and regulators.

Deriving benefits from data while simultaneously managing risks to individuals' privacy is not well-suited to one-size-fits-all solutions. Like building a house, where homeowners make layout and design choices while relying on a well-engineered foundation, privacy protection should allow for individual choices, as long as effective privacy risk mitigations are already engineered into products and services. The Privacy Framework—through a risk- and outcome-based approach—is flexible enough to address diverse privacy needs, enable more innovative and effective solutions that can lead to better outcomes for individuals and organizations, and stay current with technology trends, such as artificial intelligence and the Internet of Things.

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

- The Core enables a dialogue—from the executive level to the implementation/operations level—about important privacy protection activities and desired outcomes.
- Profiles enable the prioritization of the outcomes and activities that best meet organizational privacy values, mission or business needs, and risks.

[1] There is no objective standard for ethical decision-making; it is grounded in the norms, values, and legal expectations in a given society.

执行摘要

二十多年来，互联网及相关信息技术推动了前所未有的创新、经济价值和社会服务的改善。这些效益中的许多都得益于在复杂生态系统中流动的个人数据。因此，个人在与系统、产品和服务交互时，可能无法理解其隐私可能面临的潜在后果。与此同时，组织也可能未充分认识到这些后果对个人、社会或其企业的影响，而这些影响可能波及品牌、利润底线以及未来增长前景。

在遵循透明、基于共识的流程(包括私营和公共部门的利益相关方)来制定这一自愿性工具之后，NIST 发布本隐私框架：通过企业风险管理改进隐私的工具(隐私

框架)，以支持更好的隐私工程实践，支持隐私设计理念，并帮助组织保护个人隐私。隐私框架可支持组织：

- 通过在产品和服务的设计或部署中支持伦理决策来建立客户信任，优化数据的有益使用，同时尽量减少对个人隐私和整个社会的不利后果；[1]
- 履行当前的合规义务，并使产品和服务具有前瞻性，以在不断变化的技术和政策环境中满足这些义务；以及
- 促进与个人、业务合作伙伴、评估人员和监管机构就隐私实践进行沟通。

在从数据中获益的同时管理个人隐私风险，并不适合采用一刀切的解决方案。如同建造房屋，房主在依赖精心设计的基础的同时做出布局和设计选择，隐私保护也应允许个人选择，只要有效的隐私风险缓解措施已被工程化融入产品和服务中。隐私框架通过基于风险和结果的方法，具有足够的灵活性，能够应对多样化的隐私需求，支持更具创新性和有效性的解决方案，从而为个人和组织带来更好的结果，并与人工智能和物联网等技术趋势保持同步。

隐私框架遵循《改进关键基础设施网络安全框架(网络安全框架)》的结构，以促进两个框架的共同使用。与网络安全框架一样，隐私框架由三个部分组成：核心、配置文件和实施层级。每个组件通过业务与使命驱动因素、组织角色与职责以及隐私保护活动之间的联系，强化隐私风险管理。

- 框架核心支持从执行层到实施/运营层就重要的隐私保护活动和期望结果进行对话。
- 概况支持对最能满足组织隐私价值观、使命或业务需求以及风险的结果和活动进行优先排序。

1 伦理决策没有客观标准；它基于特定社会中的规范、价值观和法律期望。

- Implementation Tiers support decision-making and communication about the sufficiency of organizational processes and resources to manage privacy risk.

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

Acknowledgements

This publication is the result of a collaborative effort between NIST and organizational and individual stakeholders in the public and private sectors. In developing the Privacy Framework, NIST has relied upon three public workshops, a request for information (RFI), a request for comment (RFC), five webinars, and hundreds of direct interactions with stakeholders.[2] NIST acknowledges and thanks all of those who have contributed to this publication.

[2] A complete development archive can be found at https://www.nist.gov/privacy-framework.

• 实施层级支持就组织流程和资源是否足以管理隐私风险进行决策和沟通。

总之，隐私框架旨在帮助组织将隐私风险与其更广泛的企业风险组合置于同等地位，从而建立更好的隐私基础。

致谢

本出版物是 NIST 与公共和私营部门的组织及个人利益相关方合作努力的成果。在制定隐私框架的过程中，NIST 依托了三场公开研讨会、一份信息征询书(RFI)、一份征求意见书(RFC)、五场网络研讨会以及与利益相关方的数百次直接互动。[2] NIST 感谢所有为本出版物做出贡献的人。

[2]完整的开发档案可在https://www.nist.gov/privacy-framework.找到

Table of Contents

Executive Summary ..... ***i***

Acknowledgements ..... ***ii***

1.0 Privacy Framework Introduction **1**
1.1 Overview of the Privacy Framework 2
1.2 Privacy Risk Management 2
1.2.1 Cybersecurity and Privacy Risk Management 3
1.2.2 Privacy Risk Assessment 4
1.3 Document Overview 5

2.0 Privacy Framework Basics **6**
2.1 Core 6
2.2 Profiles 8
2.3 Implementation Tiers 8

3.0 How to Use the Privacy Framework **9**
3.1 Mapping to Informative References 9
3.2 Strengthening Accountability 10
3.3 Establishing or Improving a Privacy Program 11
3.4 Applying to the System Development Life Cycle 12
3.5 Using within the Data Processing Ecosystem 13
3.6 Informing Buying Decisions 14

References ***15***

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

Appendix B: Glossary ***28***

Appendix C: Acronyms ***31***

Appendix D: Privacy Risk Management Practices ***32***

Appendix E: Implementation Tiers Definitions ***37***

List of Figures

Figure 1: Core, Profiles, and Implementation Tiers **2**
Figure 2: Cybersecurity and Privacy Risk Relationship **3**
Figure 3: Relationship Between Privacy Risk and Organizational Risk **4**
Figure 4: Privacy Framework Core Structure **6**
Figure 5: Using Functions to Manage Cybersecurity and Privacy Risks **7**
Figure 6: Relationship Between Core and Profiles **8**
Figure 7: Notional Collaboration and Communication Flows Within an Organization **10**
Figure 8: Data Processing Ecosystem Relationships **13**

List of Tables

Table 1: Privacy Framework Function and Category Unique Identifiers **19**
Table 2: Privacy Framework Core **20**
Table 3: Privacy Engineering and Security Objectives **34**

目录

执行摘要 ..... i 致谢 ii

1.0 **隐私框架简介** 1
1.1 隐私框架概述 2
1.2 隐私风险管理 2
1.2.1 网络安全与隐私风险管理 3
1.2.2 隐私风险评估 4
1.3 文档概述 5

2.0 **隐私框架基础** 6
2.1 框架核心 6
2.2 概况 8
2.3 实施层级 8

3.0 **如何使用隐私框架** 9
3.1 映射到资料性参考文献 9
3.2 加强问责 10
3.3 建立或改进隐私计划 11
3.4 应用于系统开发生命周期 12
3.5 在数据处理生态系统内使用 13
3.6 为购买决策提供信息 14

参考文献 15

附录A：隐私框架核心 17

附录 B：术语表 28

附录 C：缩略语 31

附录 D：隐私风险管理实践 32

附录 E：实施层级定义 37

图目录

图 1：核心、概要文件与实施层级 2
图 2：网络安全与隐私风险的关系 3
图 3：隐私风险与组织风险之间的关系 4
图 4：隐私框架核心结构 6
图 5：使用功能管理网络安全和隐私风险 7
图 6：核心与配置文件之间的关系 8
图 7：组织内概念性协作与沟通流程 10
图 8：数据处理生态系统关系 13

表格列表

表 1：隐私框架功能与类别唯一标识符 19
表 2：隐私框架核心 20
表 3：隐私工程与安全目标 34

1.0 Privacy Framework Introduction

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

Privacy is challenging because not only is it an all-encompassing concept that helps to safeguard important values such as human autonomy and dignity, but also the means for achieving it can vary.[3] For example, privacy can be achieved through seclusion, limiting observation, or individuals' control of facets of their identities (e.g., body, data, reputation).[4] Moreover, human autonomy and dignity are not fixed, quantifiable constructs; they are filtered through cultural diversity and individual differences. This broad and shifting nature of privacy makes it difficult to communicate clearly about privacy risks within and between organizations and with individuals. What has been missing is a common language and practical tool that is flexible enough to address diverse privacy needs.

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

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

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

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

1.0 隐私框架简介

二十多年来，互联网及相关信息技术推动了前所未有的创新、经济价值和社会服务的普及。这些效益中的许多都得益于在复杂生态系统中流动的关于个人的数据。因此，个人在与系统、产品和服务交互时，可能无法理解其隐私面临的潜在后果。组织也可能无法充分认识到这些后果。未能管理隐私风险可能对个人和社会层面产生直接的不利影响，并对组织的品牌、底线和未来增长前景产生后续影响。找到既能继续从数据处理中获益、又能同时保护个人隐私的方法具有挑战性，且不适合采用一刀切的解决方案。

隐私之所以具有挑战性，不仅因为它是一个包罗万象的概念，有助于保障人类自主与尊严等重要价值，而且实现隐私的手段也各不相同。[3]例如，隐私可以通过独处、限制观察或个人对其身份各方面(如身体、数据、声誉)的控制来实现。[4]此外，人类自主与尊严并非固定、可量化的构造；它们经过文化多样性和个体差异的过滤。隐私的这种宽泛且不断变化的性质，使得在组织内部、组织之间以及与个人之间清晰地沟通隐私风险变得困难。一直以来所缺失的是一种共同的语言和实用的工具，它足够灵活，能够应对多样化的隐私需求。

这份自愿性的 NIST 隐私框架：通过企业风险管理改进隐私的工具(隐私框架)旨在供各种规模的组织广泛使用，并且不依赖于任何特定技术、行业、法律或司法管辖区。隐私框架采用一种通用方法--可适应任何组织在数据处理生态系统中的角色--其目的是通过以下方式帮助组织管理隐私风险：

- 在设计和部署影响个人的系统、产品和服务时考虑隐私；
- 沟通其隐私实践；以及
- 通过制定概况、选择层级和实现结果，鼓励跨组织的员工协作--例如，在执行层、法律和信息技术(IT)人员之间。

3 自主和尊严是联合国《世界人权宣言》中涵盖的概念，见https://www.un.org/en/universal-Declaration-human-rights/.

4 有许多出版物深入探讨了隐私的背景或该概念的不同方面。例如，参见 Solove D(2010) *Understanding Privacy*(Harvard University Press, Cambridge, MA), https://ssrn.com/abstract=1127888； 和 Selinger E, Hartzog W(2017) Obscurity and Privacy, *Spaces for the Future: A Companion to Philosophy of Technology*, eds Pitt J, Shew A(Taylor & Francis, New York, NY), Chapter 12, 1 st Ed., https://doi.org/10.4324/9780203735657.

1.1 Overview of the Privacy Framework

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

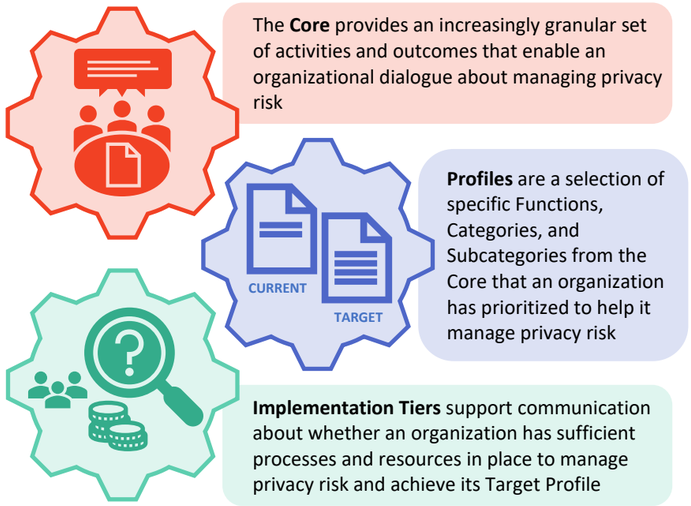


Figure 1: Core, Profiles, and Implementation Tiers

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

1.2 Privacy Risk Management

While some organizations have a robust grasp of *privacy risk management,* a common understanding of many aspects of this topic is still not widespread.[5] To promote broader understanding, this section covers concepts and considerations that organizations may use to develop, improve, or communicate

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

1.1 隐私框架概述

如**图 1**所示，隐私框架由三部分组成：框架核心、概况和实施层级。每个组成部分都通过业务或使命驱动因素、组织角色和职责以及隐私保护活动之间的联系，强化组织管理隐私风险的方式。如第 2 节进一步解释：



图1:框架核心、概况和实施层级

• 核心是一组隐私保护活动和结果，允许在整个组织内传达优先的隐私保护活动和结果，从执行层到实施/运营层传达优先排序的隐私保护活动和结果。框架核心进一步划分为每个功能的关键类别和子类别--这些是离散的结果。

• 概况代表组织当前的隐私活动或期望结果。为制定概况，组织可以审查核心中的所有结果和活动，根据业务或使命驱动因素、数据处理生态系统角色、数据处理类型以及个人的隐私需求，确定哪些是最需要重点关注的。组织可以根据需要创建或添加功能、类别和子类别。概况可用于通过比较"当前"概况("现状"状态)与"目标"概况("未来"状态)来识别改善隐私态势的机会。概况可用于开展自我评估，并在组织内部或组织之间就隐私风险的管理方式进行沟通。

• 实施层级("层级")提供了一个参考点，说明组织如何看待隐私风险，以及是否具备足够的流程和资源来管理该风险。层级反映了从非正式的、被动响应式的方法向敏捷且基于风险知情的方法的演进过程。在选择层级时，组织应考虑其目标概况，以及当前风险管理实践、隐私风险融入企业风险管理组合的程度、数据处理生态系统关系和员工构成及培训计划可能如何支持或阻碍目标的实现。

1.2 隐私风险管理

虽然一些组织对隐私风险管理有较深入的理解，但对该主题许多方面的共同理解仍未广泛普及。[5]为促进更广泛的理解，本节涵盖组织可用于制定、改进或传达的概念和考虑因素

[5]参见《*NIST*隐私框架信息请求回复摘要分析》[2]第7页。

about privacy risk management. Appendix D provides additional information on key privacy risk management practices.

1.2.1 Cybersecurity and Privacy Risk Management

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

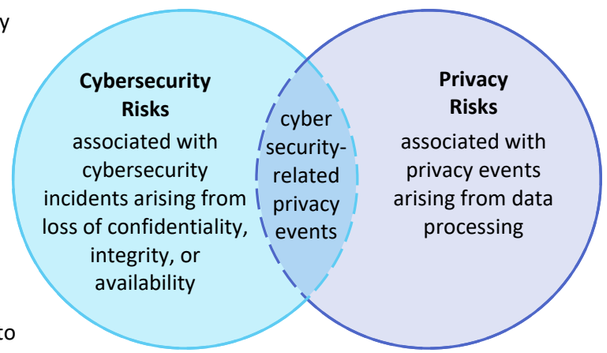


Figure 2: Cybersecurity and Privacy Risk Relationship

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

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

> ***Data Action***
> A data life cycle operation, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal.
>
> ***Data Processing***
> The collective set of data actions.

The basis for the problems that individuals may experience can vary. As depicted in **Figure 2**, problems arise as an adverse effect of data processing that organizations conduct to meet their mission or business objectives. An example is the concerns that certain communities had about the installation of "smart meters" as part of the Smart Grid, a nationwide technological effort to increase energy efficiency.[7] The ability of these meters to collect, record, and distribute highly granular information about household electrical use could provide insight into people's behavior inside their homes.[8] The meters were

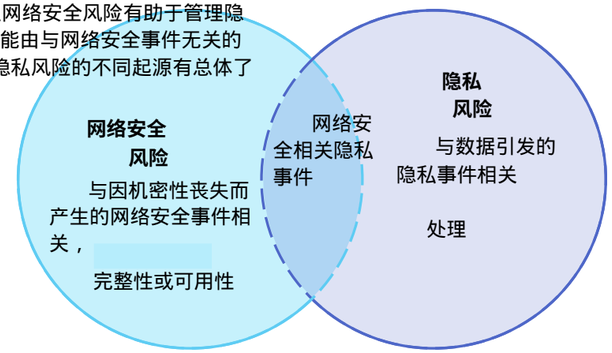
6 NIST has created an illustrative catalog of problems for use in privacy risk assessment. See *NIST Privacy Risk Assessment Methodology* [3]. Other organizations may have created other categories of problems, or may refer to them as adverse consequences or harms.

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

8 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 adverse effects on individuals of data processing, see Appendix E of NIST IR 8062.

关于隐私风险管理。附录D提供了关于关键隐私风险的额外信息管理实践。

1.2.1 网络安全与隐私风险管理自2014年发布以来，网络安全框架已帮助组织沟通和管理网络安全风险。[1]虽然管理网络安全风险有助于管理隐私风险，但这并不充分，因为隐私风险也可能由与网络安全事件无关的原因引起，如**图2**所示。对网络安全风险和隐私风险的不同起源有总体了解，对于确定最有效的解决方案至关重要



应对风险。

图2:网络安全与隐私风险

隐私框架对隐私风险的处理方式是将隐私事件视为个人可能因系统、产品或服务对数据(无论数字形式还是非数字形式)的操作而经历的潜在问题，涵盖从数据收集到处置的完整生命周期。

关系

隐私框架将这些数据操作单独称为数据动作，统称为作为数据处理。个人因数据处理而可能遇到的问题可以用多种方式表述，但NIST将其描述为从尊严类影响(如尴尬或污名化)到更实质性的损害(如歧视、经济损失或人身伤害)。[6]个人可能遇到的问题的成因各不相同。如**图2**所示，问题作为组织为满足其使命或业务目标而进行的数据处理的不利影响而产生。一个例子是某些社区对安装"智能电表"的担忧，这是智能电网--一项旨在提高能源效率的全国性技术努力--的一部分。[7]这些电表收集、记录和分发关于家庭用电的高度精细化信息的能力，可能提供对人们在家中行为的洞察。[8]这些电表

> **数据操作**
> 数据生命周期操作，包括但不限于收集、保留、记录、生成、转换、使用、披露、共享、传输，以及处置。
>
> **数据处理**
> 集体的一组数据操作。

6 NIST 创建了一个示例性问题目录，用于隐私风险评估。参见*NIST Privacy Risk assessment Methodology*[3]。其他组织可能创建了其他类别的问题，或将其称为不利后果或危害。

7 例如，参见 NIST 机构间或内部报告(IR) 7628 修订版 1 第 1 卷，*Guidelines for Smart Grid Cybersecurity: Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements*，见[4] p. 26.

8 参见 NIST IR 8062,*An Introduction to Privacy Engineering and Risk Management in Federal Systems*，见[5]第 2 页。有关数据处理对个人产生不利影响的其他类型隐私风险，参见 NIST IR 8062 附录 E。

operating as intended, but the data processing could lead to people feeling surveilled.

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

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



Figure 3: Relationship Between Privacy Risk and Organizational Risk

1.2.2 Privacy Risk Assessment

Privacy risk management is a cross-organizational set of processes that helps organizations to understand how their systems, products, and services may create problems for individuals and how to develop effective solutions to manage such risks. *Privacy risk assessment* is a sub-process for identifying and evaluating specific privacy risks. In general, privacy risk assessments produce the information that can help organizations to weigh the benefits of the data processing against the risks and to determine the appropriate response—sometimes referred to as proportionality.[10] Organizations may choose to

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

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

按预期运行，但数据处理可能导致人们感到被监视。

在日益互联的世界中，一些问题可能仅仅源于个人与系统、产品和服务的交互，即使所处理的数据与可识别的个人没有直接关联。例如，智慧城市技术可用于改变或影响人们的行为，如他们在城市中移动的地点和方式。[9] 在数据处理过程中的某些环节出现保密性、完整性或可用性丧失时，也可能产生问题，例如外部攻击者窃取数据或员工未经授权访问或使用数据。**图2**将这些类型的网络安全相关隐私事件展示为隐私风险与网络安全风险的重叠部分。

一旦组织能够识别数据处理中可能出现任何特定问题的可能性(隐私框架将其称为问题数据行为)，它就可以评估如果问题数据行为发生时应产生的影响。这种影响评估是隐私风险与组织风险交汇之处。个人，无论是单独还是群体(包括社会层面)，都会直接经历问题的影响。由于个人经历的问题，组织可能会经历诸如不合规成本、因客户放弃产品和服务而导致的收入损失，或对其外部品牌声誉或内部文化的损害等影响。组织通常在企业风险管理层面管理这些类型的影响；通过将个人经历的问题与这些易于理解的组织影响联系起来，组织可以使隐私风险与其在更广泛组合中管理的其他风险处于同等地位，并推动更明智的决策，以分配资源加强隐私计划。**图3**说明了隐私风险与组织风险之间的这种关系。



图3:隐私风险与组织风险之间的关系

1.2.2 隐私风险评估

隐私风险管理是一组跨组织的流程，帮助组织了解其系统、产品和服务可能如何给个人带来问题，以及如何制定有效的解决方案来管理此类风险。隐私风险评估是识别和评估特定隐私风险的子流程。一般来说，隐私风险评估产生信息，可帮助组织权衡数据处理的收益与风险，并确定适当的响应--有时称为比例性。[10]组织可以选择

9 参见 Newcombe T (2016)《智慧城市技术引发的安全、隐私与治理担忧日益加剧》。Government Technology。可访问 http://www.govtech.com/Security-Privacy-Governance-Concerns-AboutSmart-City-Technologies-Grow.html.

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

prioritize and respond to privacy risk in different ways, depending on the potential impact to individuals and resulting impacts to organizations. Response approaches include:[11]

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

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

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

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

1.3 Document Overview

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

- **Section 2** describes the Privacy Framework components: Core, Profiles, and Implementation Tiers.
- **Section 3** presents examples of how the Privacy Framework can be used.
- The **References section** lists the references for the document.

[11] See NIST Special Publication (SP) 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* [6].

根据对个人的潜在影响以及对组织产生的相应影响，以不同方式确定隐私风险的优先级并作出响应。响应方式包括：[11]

- 缓解风险(例如，组织可以对系统、产品或服务应用技术和/或政策措施，将风险降至可接受的程度);
- 转移或分担风险(例如，合同是将风险分担或转移给其他组织的一种方式，隐私声明和同意机制是与个人分担风险的一种方式);
- 规避风险(例如，组织可能认定风险大于收益，从而放弃或终止数据处理)；或
- 接受风险(例如，组织可能认定对个人的问题极小或不太可能发生，因此收益大于风险，无需投入资源进行缓解)。

隐私风险评估尤为重要，因为如上所述，隐私是一种保障多重价值的条件。保护这些价值的方法可能不同，而且可能相互冲突。根据其目标，如果组织试图通过限制观察来实现隐私，这可能导致实施分布式数据架构或隐私增强密码技术等措施，甚至对组织隐藏数据。如果组织还试图实现个人控制，这些措施可能会冲突。例如，如果个人请求访问数据，而数据以组织无法访问的方式分布或加密，组织可能无法提供数据。隐私风险评估可以帮助组织在特定背景下理解要保护的价值、要采用的方法，以及如何平衡不同类型措施的实施。

最后，隐私风险评估帮助组织区分隐私风险和合规风险。识别数据处理是否可能给个人带来问题，即使组织可能完全遵守适用法律或法规，也可以帮助在系统、产品和服务的设计或部署中做出道德决策。尽管道德决策没有客观标准，但它基于特定社会的规范、价值观和法律期望。这有助于优化数据的有益使用，同时最大限度地减少对个人隐私和整个社会的不利后果，并避免信任损失损害组织声誉、减缓采用或导致产品和服务被放弃。

有关隐私风险评估操作层面的更多信息，请参见附录D。

1.3 文档概述

本文件其余部分包含以下章节和附录：

- **第2节**描述了隐私框架的组成部分：核心、概况和实施层级。
- **第3节**给出了如何使用隐私框架的示例。
- **参考文献部分**列出了文档的参考文献。

11 参见 NIST 特别出版物(SP) 800-39,*Managing Information Security Risk: Organization, Mission, and Information System View*[6]。

- **Appendix A** presents the Privacy Framework Core in a tabular format: Functions, Categories, and Subcategories.
- **Appendix B** contains a glossary of selected terms.
- **Appendix C** lists acronyms used in this document.
- **Appendix D** considers key practices that contribute to successful privacy risk management.
- **Appendix E** defines the Implementation Tiers.

2.0 Privacy Framework Basics

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

2.1 Core

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

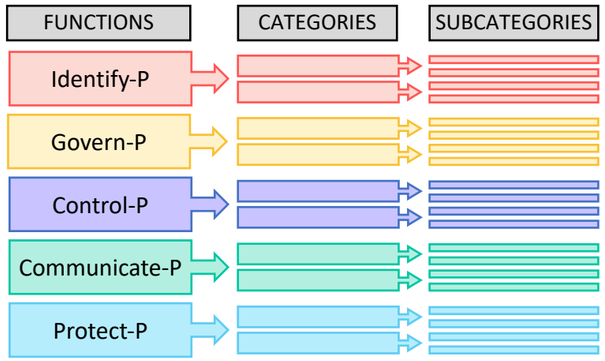


Figure 4: Privacy Framework Core Structure

The Core elements work together:

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

The five Functions, Identify-P, Govern-P, Control-P, Communicate-P, and Protect-P, defined below, can be used to manage privacy risks arising from data processing.[12] Protect-P is specifically focused on managing risks associated with cybersecurity-related privacy events (e.g., *privacy breaches*). The Cybersecurity Framework, although intended to cover all types of cybersecurity incidents, can be

[12] 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.

- **附录A**以表格形式呈现隐私框架核心：功能、类别、以及子类别。
- **附录 B**包含选定术语的词汇表。
- **附录 C**列出了本文件中使用的缩略语。
- **附录D**探讨了有助于成功实施隐私风险管理的关键实践。
- 附录 E 定义了实施层级。

2.0 隐私框架基础

隐私框架提供了一种通用语言，用于与内部和外部利益相关方理解、管理和沟通隐私风险。它可适应任何组织在数据处理生态系统中的角色。它可用于帮助识别和优先安排降低隐私风险的行动，并且是协调政策、业务和技术方法来管理该风险的工具。

2.1 核心

核心在附录A中列出，提供了一组日益细化的活动和结果，支持就管理隐私风险开展对话。如**图4**所示，核心由功能、类别和子类别组成。

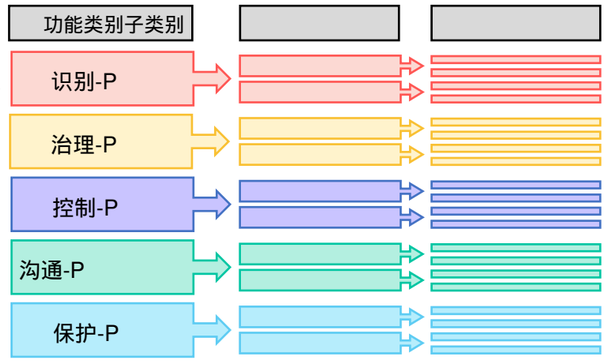


图4:隐私框架核心结构

核心要素协同运作：

- 功能在最高层级组织基础隐私活动。它们帮助组织表达其通过理解和管理数据处理来管理隐私风险，支持风险管理决策，确定如何与个人互动，并通过从以往活动中学习来改进。它们并非旨在形成一条串行路径或导向静态的期望终态。相反，各功能应同时且持续地执行，以形成或增强一种应对隐私风险动态特性的运营文化。
- 类别是功能细分为与以下密切相关的隐私结果组程序化需求与特定活动。
- 子类别进一步将类别划分为技术和/或管理活动的具体结果。它们提供了一组结果，虽非穷尽，但有助于支持实现每个类别中的结果。

下文定义的五项功能--识别-P、治理-P、控制-P、沟通-P和保护-P--可用于管理数据处理产生的隐私风险。[12] 保护-P特别侧重于管理与网络安全相关隐私事件(例如，隐私泄露)相关的风险。网络安全框架虽然旨在覆盖所有类型的网络安全事件，但可以

12 每个功能名称末尾的"-P"表示它来自隐私框架，以避免与网络安全框架功能混淆。

leveraged to further support the management of risks associated with cybersecurity-related privacy events by using the Detect, Respond, and Recover Functions. Alternatively, organizations may use all five of the Cybersecurity Framework Functions in conjunction with Identify-P, Govern-P, Control-P, and Communicate-P to collectively address privacy and cybersecurity risks. **Figure 5** uses the Venn diagram from section 1.2.1 to demonstrate how the Functions from both frameworks can be used in varying combinations to manage different aspects of privacy and cybersecurity risks. The five Privacy Framework Functions are defined as follows:

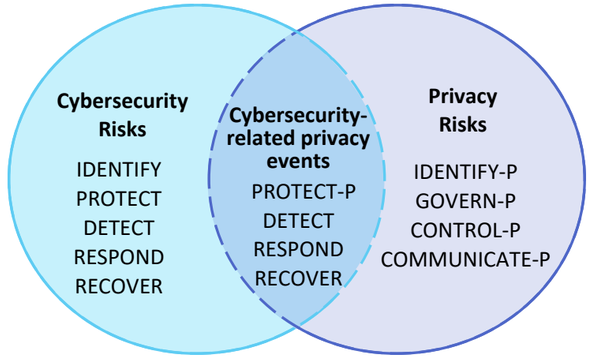


Figure 5: Using Functions to Manage Cybersecurity and Privacy Risks

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

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

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

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

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

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

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

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

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

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

利用检测、响应和恢复功能，进一步支持管理与网络安全相关的隐私事件的风险。或者，组织可以将所有五个网络安全框架功能与识别-P、治理-P、控制-P和沟通-P结合使用，共同应对隐私和网络安全风险。**图5**使用第1.2.1节中的维恩图来展示如何以不同组合使用两个框架的功能来管理隐私和

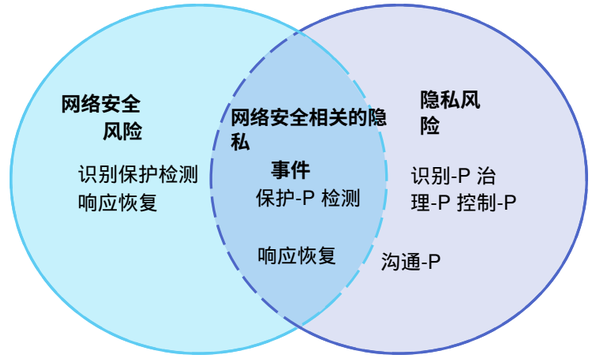


图5:使用功能来管理网络安全和隐私风险

网络安全风险。五项隐私框架功能定义如下：

• 识别-*P* - 发展组织理解，以管理个人的隐私风险由数据处理引起的。

  识别-P功能中的活动是有效使用隐私的基础框架的基础。清点数据处理所处的情形、理解组织直接或间接服务或影响的个人的隐私利益，以及开展风险评估，使组织能够理解其运营所处的业务环境，并识别和优先安排隐私风险。

• 治理-*P* - 制定并实施组织治理结构，以持续理解组织受隐私风险影响的风险管理优先事项。

  治理-P功能同样是基础性的，但侧重于组织层面的活动，例如确立组织隐私价值观和政策、识别法律/监管要求，以及理解组织风险容忍度，使组织能够按照其风险管理策略和业务需求聚焦并优先安排工作。

• 控制-*P* - 制定并实施适当的活动，使组织或个人能够以足够的粒度管理数据，以管理隐私风险。

  控制-P功能从组织和个人的角度考虑数据处理管理。

• 沟通-*P* - 制定并实施适当的活动，使组织和个人能够可靠地理解并参与关于数据处理方式及相关隐私风险的对话。

  沟通-P 功能认识到，组织和个人可能都需要了解数据处理方式，以便有效管理隐私风险。

• 保护-*P* - 制定并实施适当的数据处理保障措施。

  保护-P 功能涵盖数据保护，以防止与网络安全相关的隐私事件，即隐私与网络安全风险管理之间的重叠部分。

2.2 Profiles

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

The Privacy Framework does not prescribe Profile templates to allow for flexibility in implementation. Under the Privacy Framework's risk-based approach, organizations may not need to achieve every outcome or activity reflected in the Core. When developing a Profile, an organization may select or tailor the Functions, Categories, and Subcategories to its specific needs, including developing its own additional Functions, Categories, and Subcategories to account for unique organizational risks. An organization determines these needs by considering its mission or business objectives, privacy values, and risk tolerance; role(s) in the data processing ecosystem or industry sector; legal/regulatory requirements and industry best practices; risk management priorities and resources; and the privacy needs of individuals who are directly or indirectly served or affected by an organization's systems, products, or services.

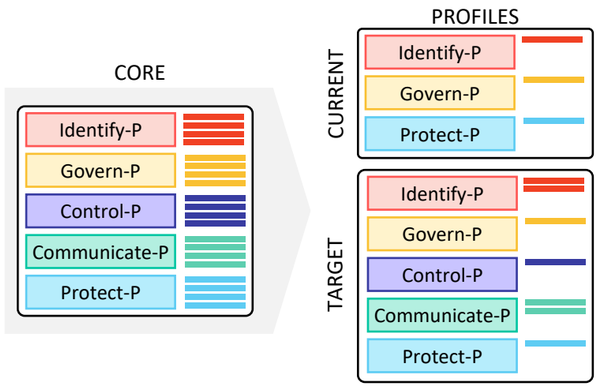


Figure 6: Relationship Between Core and Profiles

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

2.3 Implementation Tiers

Tiers support organizational decision-making about how to manage privacy risk by taking into account the nature of the privacy risks engendered by an organization's systems, products, or services and the sufficiency of the processes and resources an organization has in place to manage such risks. When selecting Tiers, an organization should consider its Target Profile(s) and how achievement may be supported or hampered by its current risk management practices, the degree of integration of privacy

2.2 概况

概况是从核心中选定的一组特定功能、类别和子类别，组织已将其列为优先事项，以帮助其管理隐私风险。概况可用于描述特定隐私活动的当前状态和期望的目标状态。当前概况表明组织当前正在实现的隐私结果，而目标概况表明实现期望的隐私风险管理目标所需的结果。两个概况之间的差异使组织能够识别差距、制定改进行动计划，并评估实现隐私结果所需的资源(例如人员配备、资金)。这构成了组织以具有成本效益、按优先级排序的方式降低隐私风险的计划基础。概况还可以帮助组织理解和比较隐私结果的当前状态和期望状态，从而有助于在组织内部和组织之间沟通风险。

隐私框架不规定概况模板，以便在实施中保持灵活性。根据隐私框架基于风险的方法，组织可能不需要实现核心中反映的每一项结果或活动。在制定概况时，组织可以根据其特定需求选择或调整功能、类别和

子类别，包括制定自己的附加功能、类别和子类别，以应对独特的组织风险。组织

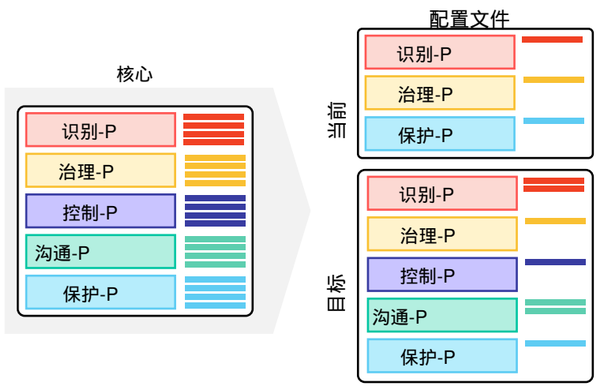


图6:核心与概况之间的关系

通过考虑其使命或业务目标、隐私价值观和风险容忍度；在数据处理生态系统或行业部门中的角色；法律/监管要求和行业最佳实践；风险管理优先事项和资源；以及直接或间接受组织系统、产品或服务服务或影响的个人的隐私需求，来确定这些需求。

如**图6**所示，概况的开发没有规定的顺序。组织可以先开发目标概况，以聚焦其期望的隐私结果，然后开发当前概况以识别差距；或者，组织可以先识别其当前活动，然后考虑如何为其中目标概况调整这些活动。组织可以选择为不同的角色、系统、产品或服务，或不同类别的个人(例如员工、客户)开发多个概况，以便在可能存在不同程度隐私风险的情况下更好地确定活动和结果的优先级。处于某一行业部门或在数据处理生态系统中具有类似角色的组织可以协调开发共同概况。

2.3 实施层级

层级通过考虑组织的系统、产品或服务所产生的隐私风险的性质，以及组织为管理此类风险而建立的流程和资源的充分性，支持组织就如何管理隐私风险做出决策。在选择层级时，组织应考虑其目标概况，以及其当前风险管理实践可能如何支持或阻碍目标的实现、隐私的整合程度

risk into its enterprise risk management portfolio, its data processing ecosystem relationships, and its workforce composition and training program.

There are four distinct Tiers, Partial (Tier 1), Risk Informed (Tier 2), Repeatable (Tier 3), and Adaptive (Tier 4), descriptions of which are in Appendix E. The Tiers represent a progression, albeit not a compulsory one. Although organizations at Tier 1 will likely benefit from moving to Tier 2, not all organizations need to achieve Tiers 3 or 4 (or may only focus on certain areas of these Tiers). Progression to higher Tiers is appropriate when an organization's processes or resources at its current Tier may be insufficient to help it manage its privacy risks.

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

3.0 How to Use the Privacy Framework

When used as a risk management tool, the Privacy Framework can assist an organization in its efforts to optimize beneficial uses of data and the development of innovative systems, products, and services while minimizing adverse consequences for individuals. The Privacy Framework can help organizations answer the fundamental question, "How are we considering the impacts to individuals as we develop our systems, products, and services?" To account for the unique needs of an organization, use of the Privacy Framework is flexible, although it is designed to complement existing business and system development operations. The decision about how to apply it is left to the implementing organization. For example, an organization may already have robust privacy risk management processes, but may use the Core's five Functions as a streamlined way to analyze and articulate any gaps. Alternatively, an organization seeking to establish a privacy program can use the Core's Categories and Subcategories as a reference. Other organizations may compare Profiles or Tiers to align privacy risk management priorities across different roles in the data processing ecosystem. The variety of ways in which the Privacy Framework can be used by organizations should discourage the notion of "compliance with the Privacy Framework" as a uniform or externally referenceable concept. The following subsections present a few options for use of the Privacy Framework.

3.1 Mapping to Informative References

Informative references are mappings to Subcategories to provide implementation support, including mappings of tools, technical guidance, standards, laws, regulations, and best practices. Crosswalks that map the provisions of standards, laws, and regulations to Subcategories can help organizations determine which activities or outcomes to prioritize to facilitate compliance. The Privacy Framework is technology neutral, but it supports technological innovation because any organization or industry sector can develop these mappings as technology and related business needs evolve. By relying on consensus-based standards, guidelines, and practices, the tools and methods available to achieve positive privacy outcomes can scale across borders and accommodate the global nature of privacy risks. The use of existing and emerging standards will enable economies of scale and drive the development of systems, products, and services that meet identified market needs while being mindful of the privacy needs of individuals.

风险纳入其企业风险管理组合、其数据处理生态系统关系，以及其员工构成和培训计划。

共有四个不同的层级：部分级(层级1)、风险知情级(层级2)、可重复级(层级3)和自适应级(层级4)，其描述见附录E。这些层级代表一种递进，尽管并非强制性的。虽然处于层级1的组织可能会从进入层级2中受益，但并非所有组织都需要达到层级3或层级4(或者可能只关注这些层级的某些方面)。

当组织在当前层级的过程或资源可能不足以帮助其管理隐私风险时，向更高层级推进是适当的。

组织可以使用层级在内部沟通推进到更高层级所需的资源分配，或作为衡量其管理隐私风险能力进展的一般基准。组织还可以使用层级来了解数据处理生态系统中其他组织的资源和流程规模，以及它们如何与组织的隐私风险管理优先事项保持一致。尽管如此，隐私框架的成功实施取决于实现组织目标概况中所述的结果，而不是取决于层级的确定。

3.0 如何使用隐私框架

当作为风险管理工具使用时，隐私框架可以帮助组织努力优化数据的有益使用以及创新系统、产品和服务的开发，同时最大限度地减少对个人的不利后果。隐私框架可以帮助组织回答一个基本问题："在我们开发系统、产品和服务时，我们如何考虑对个人的影响?"为了顾及组织的独特需求，隐私框架的使用是灵活的，尽管它旨在补充现有的业务和系统开发运营。关于如何应用它的决定留给实施组织。例如，组织可能已经拥有稳健的隐私风险管理流程，但可以使用核心的五个功能作为一种简化的方式来分析和阐明任何差距。或者，寻求建立隐私计划的组织可以使用核心的类别和子类别作为参考。其他组织可以比较概况或层级，以协调数据处理生态系统中不同角色的隐私风险管理优先事项。隐私

组织在使用框架时应避免将"遵守隐私框架"视为一种统一的或可外部参照的概念。以下小节介绍了使用隐私框架的几种选项。

3.1 映射到资料性参考文献

信息性参考是到子类别的映射，用于提供实施支持，包括工具、技术指南、标准、法律、法规和最佳实践的映射。将标准、法律和法规的条款映射到子类别的交叉对照表可以帮助组织确定应优先考虑哪些活动或结果，以促进合规。隐私框架是技术中立的，但它支持技术创新，因为任何组织或行业部门都可以随着技术和相关业务需求的发展而开发这些映射。通过依赖基于共识的标准、指南和实践，可用于实现积极隐私结果的工具和方法可以跨越国界扩展，并适应隐私风险的全球性质。使用现有和新兴标准将实现规模经济，并推动开发满足已识别市场需求的系统、产品和服务，同时顾及个人的隐私需求。

Gaps in mappings can also be used to identify where additional or revised standards, guidelines, and practices would help an organization to address emerging needs. An organization implementing a given Subcategory, or developing a new Subcategory, might discover that there is insufficient guidance for a related activity or outcome. To address that need, an organization might collaborate with technology leaders and/or standards bodies to draft, develop, and coordinate standards, guidelines, or practices.

A repository of informative references can be found at https://www.nist.gov/privacy-framework. These resources can support organizations' use of the Privacy Framework and achievement of better privacy practices.

3.2 Strengthening Accountability

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



Figure 7: Notional Collaboration and Communication Flows Within an Organization

[13] See, e.g., Organisation for Economic Co-operation and Development (OECD) (2013) *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, available at https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm; International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) (2011) *ISO/IEC 29100:2011 – Information technology – Security techniques – Privacy framework* (ISO, Geneva, Switzerland), available at https://standards.iso.org/ittf/PubliclyAvailableStandards/c045123_ISO_IEC_29100_2011.zip; and Alliance of Automobile Manufacturers, Inc., Association of Global Automakers, Inc. (2014) *Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technologies and Services*, available at https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services-03-21-19.pdf.

映射中的空白也可用于识别哪些新增或修订的标准、指南和实践将有助于组织应对新兴需求。实施给定子类别或开发新子类别的组织可能会发现，对相关活动或结果的指导不足。为满足该需求，组织可与技术领导者和/或标准机构合作，起草、制定和协调标准、指南或实践。信息性参考的存储库可在https://www.nist.gov/privacy-framework.找到。这些资源可支持组织使用隐私框架并实现更好的隐私实践。

3.2 加强问责

问责制通常被视为一项关键的隐私原则，尽管在概念上它并非隐私所独有。[13]问责制贯穿于整个组织，并可以在不同的抽象程度上表达，例如作为

文化价值，作为治理政策
和程序，或作为隐私要求与控制措施之间的可追溯关系。隐私风险管理可作为支持各组织层级问责制的一种手段，因为它将能够传达组织隐私价值观和风险容忍度的高级管理人员与业务/流程经理层级的人员联系起来，后者可协作制定和实施支持组织隐私价值观的治理政策和程序。然后，这些政策和程序可传达给实施/运营层级的人员，后者协作定义支持政策和程序表达的隐私要求，并

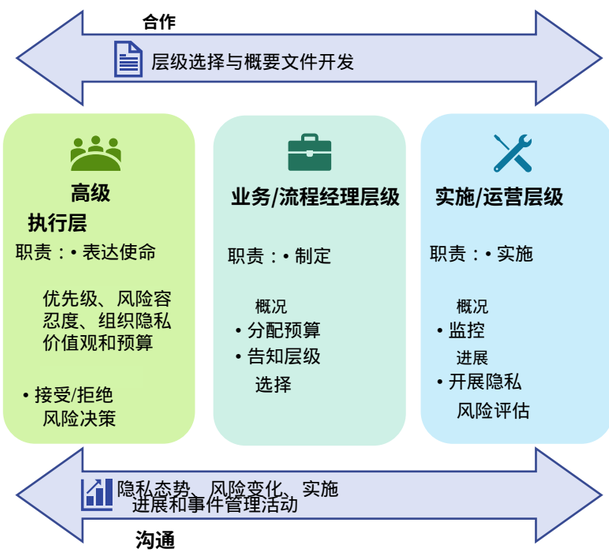


图7:概念性协作与沟通流程
在一个组织

组织系统、产品和服务中的程序。以下人员：

13 参见，例如，经济合作与发展组织(OECD)(2013)《*OECD* 隐私保护与个人数据跨境流动指南》，可访问https://www.oecd.org/internet/ieconomy/OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.htm;国际标准化组织(ISO)/国际电工委员会(IEC)(2011)*ISO/IEC 29100:2011* - 信息技术 - 安全技术 - 隐私框架(ISO，瑞士日内瓦),可访问https://standards.iso.org/ittf/PubliclyAvailableStandards/c045123_ISO_IEC_29100_2011.zip;；以及汽车制造商联盟公司、全球汽车制造商协会公司(2014)《消费者隐私保护原则：车辆技术与服务的隐私原则》，可访问https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principles for_Vehicle Technologies_Services-03-21-19.pdf。

implementation/operations level also select, implement, and assess controls as the technical and policy measures that meet the privacy requirements, and report on progress, gaps and deficiencies, incident management, and changing privacy risks so that those at the business/process manager level and the senior executives can better understand and respond appropriately.

Figure 7 provides a graphical representation of this bi-directional collaboration and communication and how elements of the Privacy Framework can be incorporated to facilitate the process. In this way, organizations can use the Privacy Framework as a tool to support accountability. They can also use the Privacy Framework in conjunction with other frameworks and guidance that provide additional practices to achieve accountability within and between organizations.[14]

3.3 Establishing or Improving a Privacy Program

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

Ready

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

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.

Set

An organization completes its Current Profile by indicating which Category and Subcategory outcomes from the remaining Functions are being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps by providing baseline information. Informed by the activities under Identify and Govern, such as organizational privacy values and policies, organizational risk tolerance, and privacy risk assessment results, an organization completes its Target Profile focused on the assessment of the Categories and Subcategories describing its desired privacy outcomes. An organization also may develop its own additional Functions, Categories, and Subcategories to account for unique organizational risks. It may also consider influences and requirements of external stakeholders such as

[14] See, e.g., NIST SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [7]; and Organization for the Advancement of Structured Information Standards (OASIS) (2016) Privacy Management Reference Model and Methodology (PMRM) Version 1.0, https://docs.oasis-open.org/pmrm/PMRM/v1.0/PMRM-v1.0.pdf.

[15] For additional information, see the "Prepare" step, Section 3.1, NIST SP 800-37, Rev. 2 [7].

实施/运营层级的人员还选择、实施和评估控制措施，作为满足隐私要求的技术和政策措施，并报告进展、差距和不足、事件管理以及不断变化的隐私风险，以便业务/流程经理层级的人员和高级管理人员能够更好地理解并适当应对。

图7以图形方式展示了这种双向协作与沟通，以及如何纳入隐私框架的要素以促进该过程。通过这种方式，组织可以将隐私框架用作支持问责制的工具。他们还可以将隐私框架与其他框架和指南结合使用，这些框架和指南提供了额外的实践，以在组织内部和组织之间实现问责制。[14]

3.3 建立或改进隐私计划

使用"准备、设置、执行"阶段的简单模型，隐私框架可以支持创建新的隐私计划或改进现有计划。当组织经历这些阶段时，它可以使用信息性参考来提供关于确定优先级或实现结果的指导。有关信息性参考的更多信息，请参见第3.1节。此外，可以在https://www.nist.gov/privacy-framework.找到存储库

准备

有效的隐私风险管理要求组织了解其使命或业务环境；其法律环境；其风险容忍度；其系统、产品或服务所产生的隐私风险；以及其在数据处理生态系统中的角色。组织可使用识别-P和治理-P功能，通过审查类别和子类别并开始制定其当前概况和目标概况来"做好准备"。[15]建立组织隐私价值观和政策、确定和表达组织风险容忍度以及开展隐私风险评估(有关隐私风险评估的更多信息，见附录D)等活动和结果为在"设定"中完成概况提供了基础。

建立或改进的简化方法

a 隐私计划

准备就绪： 使用识别-P 和治理-P 功能来实现"准备就绪"。

设置： 根据当前概况与目标概况之间的差异"设置"行动计划。

执行： 继续推进实施行动计划。

设置

组织通过指明正在实现其余功能中的哪些类别和子类别结果来完成其当前概况。如果某项结果已部分实现，记录这一事实将通过提供基线信息来帮助支持后续步骤。根据以下活动提供的信息

识别和治理，例如组织隐私价值观和政策、组织风险容忍度以及隐私风险评估结果，组织完成其目标概况，重点评估描述其期望隐私结果的类别和子类别。组织还可制定自己的附加功能、类别和子类别，以考虑独特的组织风险。它还可考虑外部利益相关方的影响和要求，例如

14 参见，例如，NIST SP 800-37,Rev.2,信息系统和组织的风险管理框架：安全和隐私的系统生命周期方法[7]；以及结构化信息标准促进组织(OASIS)(2016)隐私管理参考模型和方法(PMRM)1.0版，https://docs.oasis-open.org/pmrm/PMRM/v1.0/PMRM-v1.0.pdf.

[15]更多信息，请参见 NIST SP 800-37 Rev.2 第 3.1 节"准备"步骤[7]。

business customers and partners when creating a Target Profile. An organization can develop multiple Profiles to support its different business lines or processes, which may have different business needs and associated risk tolerances.

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

Go

With the action plan "set," an organization prioritizes which actions to take to address any gaps, and then adjusts its current privacy practices in order to achieve the Target Profile.[16]

An organization can go through the phases nonsequentially as needed to continuously assess and improve its privacy posture. For instance, an organization may find that more frequent repetition of the Ready phase improves the quality of privacy risk assessments. Furthermore, an organization may monitor progress through iterative updates to the Current Profile or the Target Profile to adjust to changing risks, subsequently comparing the Current Profile to the Target Profile.

3.4 Applying to the System Development Life Cycle

The Target Profile can be aligned with the system development life cycle (SDLC) phases of plan, design, build/buy, deploy, operate, and decommission to support the achievement of the prioritized privacy outcomes.[17] Beginning with the plan phase the prioritized privacy outcomes can be transformed into the privacy capabilities and requirements for the system, recognizing that requirements are likely to evolve during the remainder of the life cycle. A key milestone of the design phase is validating that the privacy capabilities and requirements match the needs and risk tolerance of an organization as expressed in the Target Profile. That same Target Profile can serve as an internal list to be assessed when deploying the system to verify that all privacy capabilities and requirements are implemented. The privacy outcomes determined by using the Privacy Framework should then serve as a basis for ongoing operation of the system. This includes occasional reassessment, capturing results in a Current Profile, to verify that privacy capabilities and requirements are still fulfilled.

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

16 NIST SP 800-37, Rev. 2 [7] provides additional information on steps to execute on the action plan, including control selection, implementation, and assessment to close any gaps.

17 Within the SDLC, organizations may employ a variety of development methodologies (e.g., waterfall, spiral, or agile).

在创建目标概况时的业务客户和合作伙伴。组织可以制定多个概况以支持其不同的业务线或流程，这些业务线或流程可能具有不同的业务需求和相关的风险容忍度。

组织比较当前概况和目标概况以确定差距。接下来，它制定一个优先行动计划来解决差距--反映任务驱动因素、成本和收益以及风险--以实现目标概况中的结果。同时使用网络安全框架和隐私框架的组织可以制定综合行动计划。然后，它确定解决差距所需的资源，包括资金和劳动力需求，这可以为选择适当的层级提供信息。以这种方式使用概况鼓励组织就隐私活动做出明智的决策，支持风险管理，并使组织能够执行具有成本效益的针对性改进。

执行

在"设置"行动计划后，组织确定采取哪些行动的优先级以解决任何差距，然后调整其当前的隐私实践以实现目标概况。[16]

组织可以根据需要非顺序地经历各阶段，以持续评估和改进其隐私态势。例如，组织可能会发现更频繁地重复"准备"阶段可以提高隐私风险评估的质量。此外，组织可以通过迭代更新当前概况或目标概况来监控进展，以适应不断变化的风险，随后将当前概况与目标概况进行比较。

3.4 应用于系统开发生命周期

目标概况可以与系统开发生命周期(SDLC)的阶段(计划、设计、构建/购买、部署、运行和退役)保持一致，以支持实现优先的隐私结果。[17]从计划阶段开始，优先的隐私结果可以转化为系统的隐私能力和需求，认识到需求可能会在生命周期的剩余时间内演变。设计阶段的一个关键里程碑是验证隐私能力和需求是否与目标概况中表达的组织需求和风险容忍度相匹配。同一目标概况可以作为内部清单，在部署系统时进行评估，以验证所有隐私能力和需求都已实施。然后，通过使用隐私框架确定的隐私结果应作为系统持续运行的基础。这包括偶尔的重新评估，将结果捕获到当前概况中，以验证隐私能力和需求仍然得到满足。

隐私风险评估通常关注数据生命周期，即数据经过的阶段，通常被描述为创建或收集、处理、传播、使用、存储和处置，包括销毁和删除。通过识别和理解在SDLC的所有阶段如何处理数据，使SDLC和数据生命周期保持一致，有助于组织更好地管理隐私风险，并为选择和实施隐私控制以满足隐私要求提供信息。

16 NIST SP 800-37,Rev.2[7]提供了关于执行行动计划步骤的更多信息，包括控制选择、实施和评估，以弥补任何差距。

17 在SDLC中，组织可以采用多种开发方法(例如，瀑布式、螺旋式或敏捷式)。

3.5 Using within the Data Processing Ecosystem

A key factor in the management of privacy risk is an entity's role(s) in the data processing ecosystem, which can affect not only its legal obligations, but also the measures it may take to manage privacy risk. As depicted in **Figure 8**, the data processing ecosystem encompasses a range of entities and roles that may have complex, multi-directional relationships with each other and individuals. Complexity can increase when entities are supported by a chain of sub-entities; for example, service providers may be supported by a series of service providers, or manufacturers may have multiple component suppliers. **Figure 8** displays entities as having distinct roles, but some may have multiple roles, such as an organization providing services to other organizations and providing retail products to consumers. The roles in **Figure 8** are intended to be notional classifications. In practice, an entity's role(s) may be legally codified—for example, some laws classify organizations as data controllers or data processors—or classifications may be derived from industry sector designations.



Figure 8: Data Processing Ecosystem Relationships

By developing one or more Profiles relevant to its role(s), an entity can use the Privacy Framework to consider how to manage privacy risk not only with regard to its own priorities, but also in relation to how the measures it may take affect other data processing ecosystem entities' management of privacy risk. For example:

- An organization that makes decisions about how to collect and use data about individuals may use a Profile to express privacy requirements to an external service provider (e.g., a cloud provider to which it is exporting data); the external service provider that processes the data may use its Profile to demonstrate the measures it has adopted to process data in line with contractual obligations.
- An organization may express its privacy posture through a Current Profile to report results or to compare with acquisition requirements.
- An industry sector may establish a common Profile that can be used by its members to customize their own Profiles.
- A manufacturer may use a Target Profile to determine the capabilities to build into its products so that its business customers can meet the privacy needs of their end users.
- A developer may use a Target Profile to consider how to design an application that enables privacy protections when used within other organizations' system environments.

The Privacy Framework provides a common language to communicate privacy requirements with entities within the data processing ecosystem. The need for this communication can be particularly

3.5 在数据处理生态系统内使用

隐私风险管理的一个关键因素是实体在数据处理生态系统中的角色，这可能

不仅影响其法律义务，还
它可能采取的管理措施
隐私风险。如**图8**所示，
数据处理生态系统涵盖一系列实体和角色，可能具有复杂、多方向的

与彼此的关系以及
个人。当实体由子实体链支持时，复杂性可能增加；例如，服务提供商可能由一系列

服务提供商或制造商的
可能有多个组件供应商。**图 8**显示实体具有

不同的角色，但有些可能具有
多个角色，例如向其他组织提供服务的组织



图8:数据处理生态系统关系

并向消费者提供零售产品。**图 8**中的角色旨在作为概念性分类。在实践中，实体的角色可能被法律编纂--例如，一些法律将组织分类为数据控制者或数据处理者--或者分类可能源自行业部门指定。

通过制定与其角色相关的一个或多个概况，实体可以使用隐私框架来考虑如何管理隐私风险，不仅涉及其自身优先事项，还涉及其可能采取的措施如何影响其他数据处理生态系统实体的隐私风险管理。例如：

- 就如何收集和使用个人数据做出决定的组织可以使用概况向外部服务提供商表达隐私要求(例如，向其导出数据的云提供商)；处理数据的外部服务提供商可以使用其概况来展示其为按照合同义务处理数据而采取的措施。
- 组织可以通过当前概况表达其隐私态势，以报告结果或与采购要求进行比较。
- 行业部门可以建立通用概况，供其成员定制自己的概况。
- 制造商可以使用目标概况来确定要构建到其产品中的能力，以便其商业客户能够满足其最终用户的隐私需求。
- 开发者可以使用目标概况来考虑如何设计应用程序，使其在其他组织的系统环境中使用时能够实现隐私保护。

隐私框架提供了一种通用语言，用于与数据处理生态系统内的实体沟通隐私要求。这种沟通的需求在以下情况下可能尤为

notable when the data processing ecosystem crosses national boundaries, such as with international data transfers. Organizational practices that support communication may include:

- Determining privacy requirements;
- Enacting privacy requirements through formal agreement (e.g., contracts, multi-party frameworks);
- Communicating how those privacy requirements will be verified and validated;
- Verifying that privacy requirements are met through a variety of assessment methodologies; and
- Governing and managing the above activities.

3.6 Informing Buying Decisions

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

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

显著：当数据处理生态系统跨越国界时，例如国际数据传输。支持沟通的组织实践可能包括：

- 确定隐私要求；
- 通过正式协议(例如合同、多方框架)制定隐私要求；
- 沟通如何验证和确认这些隐私要求；
- 通过各种评估方法验证隐私要求是否得到满足；以及
- 治理和管理上述活动。

3.6 为购买决策提供信息

由于当前概况或目标概况均可用于生成按优先级排序的隐私要求列表，这些概况也可用于为购买产品和服务的决策提供依据。组织首先选择与其隐私目标相关的结果，然后可以依据该结果评估合作伙伴的系统、产品或服务。例如，如果购买某设备用于森林环境监测，可管理性可能对于支持最大限度减少对使用森林人员数据处理的能力很重要，并应推动制造商依据核心中适用的子类别进行评估(例如，CT.DP-P4：系统或设备配置允许选择性收集或披露数据元素)。

在可能无法对供应商施加一组隐私要求的情况下，目标应当是在仔细确定的一组隐私要求下，在多个供应商之间做出最佳购买决策。通常，这意味着某种程度的权衡，即比较多个与概况存在已知差距的产品或服务。如果所购买的系统、产品或服务未满足概况中描述的所有目标，组织可以通过缓解措施或其他管理行动来应对剩余风险。

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 Interagency or Internal Report (IR) 7628, Rev. 1, Vol. 1. https://doi.org/10.6028/NIST.IR.7628r1

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

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

[7] 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

[8] Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-3, Includes updates as of December 1, 2017. https://doi.org/10.6028/NIST.SP.800-63-3

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

[10] Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015. https://doi.org/10.6028/NIST.SP.800-53r4

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

参考文献

[1] 美国国家标准与技术研究院(2018)《改进关键基础设施网络安全框架》1.1 版。(美国国家标准与技术研究院，马里兰州盖瑟斯堡)。https://doi.org/10.6028/NIST.CSWP.04162018

[2] 美国国家标准与技术研究院(2019)《NIST 隐私框架信息征询回应摘要分析》。(美国国家标准与技术研究院，马里兰州盖瑟斯堡)。9/02/27/rfi_response_analysis_privacyframework_2.27.19.pdf

[3] 美国国家标准与技术研究院(2019)NIST 隐私风险评估盖瑟斯堡)。https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources

[4] 智能电网互操作性小组-智能电网网络安全委员会(2014)《智能电网网络安全指南：第1卷--智能电网网络安全战略、架构与高层要求》。(NIST，马里兰州盖瑟斯堡),NIST机构间或内部报告(IR)7628，修订版1，第1卷。https://doi.org/10.6028/NIST.IR.7628r1

[5] Brooks SW, Garcia ME, Lefkovitz NB, Lightman S, Nadeau EM(2017)《联邦系统中的隐私工程与风险管理导论》。(美国国家标准与技术研究院，马里兰州盖瑟斯堡),NIST 机构间或内部报告(IR) 8062。https://doi.org/10.6028/NIST.IR.8062

[6] 联合任务组转型倡议(2011)《管理信息安全风险：组织、任务与信息系统视角》。(NIST，马里兰州盖瑟斯堡)。NIST特别出版物(SP)800-39。https://doi.org/10.6028/NIST.SP.800-39

[7] 联合工作组(2018)《信息系统和组织风险管理框架：安全与隐私的系统生命周期方法》。(美国国家标准与技术研究院，马里兰州盖瑟斯堡),NIST 特别出版物(SP)800-37 第2版。https://doi.org/10.6028/NIST.SP.800-37r2

[8] Grassi PA, Garcia ME, Fenton JL(2017)《数字身份指南》。(NIST，马里兰州盖瑟斯堡),NIST特别出版物(SP)800-63-3，包含截至2017年12月1日的更新。https://doi.org/10.6028/NIST.SP.800-63-3

[9] 管理和预算办公室(2017)《准备和应对个人可识别信息泄露》。(白宫，华盛顿特区),OMB备忘录M-17-12,2017年1月3日。可查阅https://www.White House.gov/sites/White House.gov/files/omb/memoranda/2017/m-17-12_0.pdf

[10] 联合任务组转型倡议(2013)联邦安全与隐私控制信息系统与组织。(美国国家标准与技术研究院，马里兰州盖瑟斯堡),NIST 特别出版物(SP)800-53，第4 修订版，包含截至 2015 年 1 月 22 日的更新。https://doi.org/10.6028/NIST.SP.800-53r4

[11] Grassi PA, Lefkovitz NB, Nadeau EM, Galluzzo RJ, Dinh AT(2018) 属性元数据：一项提议评估联邦属性的模式。(美国国家标准与技术研究院，马里兰州盖瑟斯堡),NIST 机构间或内部报告(IR)8112。https://doi.org/10.6028/NIST.IR.8112

[12] 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

[13] “Definitions,” Title 44 *U.S. Code*, Sec. 3542. 2011 ed. https://www.govinfo.gov/app/details/USCODE-2011-title44/USCODE-2011-title44-chap35-subchapIII-sec3542

[12] 联合任务组转型倡议(2012)风险评估实施指南。(国家标准与技术研究所,盖瑟斯堡,马里兰州),NIST 特别出版物(SP)800-30 第 1 修订版。https://doi.org/10.6028/NIST.SP.800-30r1

[13] “定义”，《美国法典》第44编第3542条，2011年版。https://www.govinfo.gov/app/details/USCODE-2011-title44/USCODE-2011-title44-chap35- 第三分章-第3542节

Appendix A: Privacy Framework Core

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

Note to Users

Risk-based Approach:

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

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

Roles:

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

附录A：隐私框架核心

本附录呈现核心内容：一张包含功能、类别和子类别的表格，描述当系统、产品和服务处理数据时，可支持管理隐私风险的具体活动和结果。

用户须知

基于风险的方法：

- **核心不是要执行的操作清单。组织根据其保护个人隐私的风险策略选择与类别说明中所述一致的子类别。**组织可能不需要实现核心中反映的每一项结果或活动。预期组织将通过考虑其目标、在数据处理生态系统或行业部门中的角色、法律/监管要求和行业最佳实践、风险管理优先事项，以及直接或间接受组织系统、产品或服务所服务或影响的个人的隐私需求，使用概况来选择并优先排序最能满足其特定需求的功能、类别和子类别。
- 不强制要求完整实现某一结果。组织可使用其概况来表达某一结果的部分实现，因为并非结果的所有方面都与该组织管理隐私风险相关，或者组织可使用目标概况来表达其当前尚不具备能力实现的某一结果的方面。
- 可能需要结合考虑多个结果以适当管理隐私风险。例如，响应个人数据访问请求的组织可为其概况同时选择子类别 CT.DM-P1:"数据元素可被访问以供审查"和类别"身份管理、身份验证与访问控制"(PR.AC-P)，以确保只有数据所属的个人才能获得访问权限。

实施：核心的表格格式并非意在暗示特定的实施顺序，也不意味着功能、类别和子类别之间存在重要性程度。实施可以是非顺序的、同时的或迭代的，取决于SDLC阶段、隐私计划的状态、员工规模或组织在数据处理生态系统中的角色。此外，核心并非穷尽性的；它是可扩展的，允许组织、行业部门和其他实体调整或向其概况添加额外的功能、类别和子类别。

角色：

- **生态系统角色：**核心旨在可供任何组织或实体使用，无论其在数据处理生态系统中的角色如何。尽管隐私框架未对生态系统角色进行分类，组织应从其在生态系统中的立场审视核心。组织的角色可能由法律明文规定--例如，一些法律将组织归类为数据控制者或数据处理者--或者分类可能源自行业称谓。由于核心要素并非按生态系统角色分配，组织可以使用其概况来选择与其角色相关的功能、类别和子类别。
- **组织角色：**组织劳动力的不同部分可能负责不同的类别或子类别。例如，法律部门可能负责执行"治理策略、流程和程序"下的活动，而 IT 部门则致力于"清单和映射"。理想情况下，核心鼓励跨组织协作以制定概况并实现结果。

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

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

Cybersecurity Framework Alignment:

- As noted in section 2.1, organizations can use the five Privacy Framework Functions—Identify-P, Govern-P, Control-P, Communicate-P, and Protect-P—to manage privacy risks arising from data processing. Protect-P is specifically focused on managing risks associated with security-related privacy events (e.g., privacy breaches). To further support the management of risks associated with security-related privacy events, organizations may choose to use Detect, Respond, and Recover Functions from the Cybersecurity Framework. For this reason, these Functions are included in **Table 1,** but are greyed out. Alternatively, organizations may use all five of the Cybersecurity Framework Functions in conjunction with Identify-P, Govern-P, Control-P, and Communicate-P to collectively address privacy and security risks. See **Figure 5** for an illustrated example of how the Functions from both frameworks can be used in varying combinations to manage different aspects of privacy and cybersecurity risks.
- Certain Functions, Categories, or Subcategories may be identical to or have been adapted from the Cybersecurity Framework. The following legend can be used to identify this relationship in **Table 2**. A complete crosswalk between the two frameworks can be found in the resource repository at https://www.nist.gov/privacy-framework.

▒	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.

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

可扩展性：结果的某些方面可能措辞含糊。例如，结果可能包含“已传达”或“已披露”等术语，但未说明向谁进行传达或披露。这种含糊是有意为之，以便具有不同用例的广泛组织能够确定在特定情境下什么是适当或必需的。

资源库：可提供关于如何优先排序或实现结果的更多信息的独立资源可在以下网址找到：https://www.nist.gov/privacy-framework.

网络安全框架对齐：

- 如第 2.1 节所述，组织可以使用隐私框架的五项功能--识别-P、治理-P、控制-P、沟通-P 和保护-P--来管理数据处理产生的隐私风险。保护-P 特别侧重于管理与安全相关隐私事件(例如隐私泄露)相关的风险。为了进一步支持管理与安全相关隐私事件相关的风险，组织可以选择使用网络安全框架中的检测、响应和恢复功能。因此，这些功能包含在**表 1**中，但以灰色显示。或者，组织可以将网络安全框架的全部五项功能与识别-P、治理-P、控制-P 和沟通-P 结合使用，共同应对隐私和安全风险。有关如何以不同组合使用两个框架中的功能来管理隐私和网络安全风险不同方面的示例说明，请参见**图 5**。
- 某些功能、类别或子类别可能与网络安全框架相同或改编自网络安全框架。以下图例可用于在**表 2**中识别这种关系。两个框架之间的完整对照表可在资源库中找到：https://www.nist.gov/privacy-framework.

▒	该功能、类别或子类别与网络安全框架一致，但文本已针对隐私框架进行了改编。
▓	该类别或子类别与网络安全框架相同。

核心标识符：为便于使用，核心的每个组成部分都被赋予唯一标识符。功能和类别各有一个唯一的字母标识符，如**表 1**所示。每个类别内的子类别在字母标识符后添加数字；每个子类别的唯一标识符包含在**表 2**中。

Table 1: Privacy Framework Function and Category Unique Identifiers

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.PO-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 Processing Policies, Processes, and Procedures
		CT.DM-P	Data Processing Management
		CT.DP-P	Disassociated Processing
CM-P	Communicate-P	CM.PO-P	Communication Policies, Processes, and Procedures
		CM.AW-P	Data Processing Awareness
PR-P	Protect-P	PR.PO-P	Data Protection Policies, Processes, and Procedures
		PR.AC-P	Identity Management, Authentication, and Access Control
		PR.DS-P	Data Security
		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

表1:隐私框架功能和类别唯一标识符

功能 唯一 标识符	功能	类别 唯一 标识符	类别
ID-P	识别-P	ID.IM-P	清单与映射
		ID.BE-P	商业环境
		ID.RA-P	风险评估
		ID.DE-P	数据处理生态系统风险管理
GV-P	治理-P	GV.PO-P	治理政策、流程和程序
		GV.RM-P	风险管理策略
		GV.AT-P	意识和培训
		GV.MT-P	监测与审查
CT-P	控制-P	CT.PO-P	数据处理政策、流程和程序
		CT.DM-P	数据处理管理
		CT.DP-P	分离处理
CM-P	沟通-P	CM.PO-P	沟通政策、流程和程序
		CM.AW-P	数据处理意识
PR-P	保护-P	PR.PO-P	数据保护政策、流程和程序
		PR.AC-P	身份管理、认证和访问 控制
		PR.DS-P	数据安全
		PR.MA-P	维护
		PR.PT-P	保护技术
DE	检测	DE.AE	异常与事件
		DE.CM	安全持续监控
		DE.DP	检测流程
RS	响应	RS.RP	响应规划
		RS.CO	通信
		RS.AN	分析
		RS.MI	缓解
		RS.IM	改进
RC	恢复	RC.RP	恢复规划
		RC.IM	改进
		RC.CO	通信

Table 2: Privacy Framework Core

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

表2:隐私框架核心

功能	类别	子类别
识别-P(ID-P):制定组织理解管理隐私风险，针对个人源于数据处理。	**清单与映射(ID.IM-P):**数据处理由系统、产品或服务被理解并指导管理隐私风险。	**ID.IM-P1:**处理数据的系统/产品/服务已已编目。
		ID.IM-P2:处理数据的系统/产品/服务及组件(例如内部或外部)的所有者或运营者(例如组织或服务提供商、合作伙伴、客户和开发者等第三方)及其角色已 已编目。
		ID.IM-P3:其数据正被处理的个人类别(例如客户、员工或潜在员工、消费者) 已编目。
		ID.IM-P4:数据操作系统/产品/服务的已编目。
		ID.IM-P5:已清点数据操作的目的。
		ID.IM-P6:数据元素在数据操作中被清点。
		ID.IM-P7:数据处理环境被识别(例如，地理位置、内部、云、第三
		ID.IM-P8:数据处理已被映射，说明系统/产品/服务的数据操作及相关数据元素，包括组件；组件所有者/运营者的角色；以及个人或第三方与 系统/产品/服务。
	业务环境(ID.BE-P):该组织的使命、目标、利益相关方和活动被理解并确定优先级；此信息用于为隐私角色、职责和风险提供依据管理决策。	**ID.BE-P1:**组织在数据处理生态系统中的角色已被识别并沟通。
		ID.BE-P2:组织使命、目标和活动的优先级已确立并沟通。
		ID.BE-P3:支持组织优先级的系统/产品/服务已被识别，关键要求已沟

Function	Category	Subcategory
	Risk Assessment (ID.RA-P): The organization understands the privacy risks to individuals and how such privacy risks may create follow-on impacts on organizational operations, including mission, functions, other risk management priorities (e.g., compliance, financial), reputation, workforce, and culture.	**ID.RA-P1:** Contextual factors related to the systems/products/services and the data actions are identified (e.g., individuals' demographics and privacy interests or perceptions, data sensitivity and/or types, visibility of data processing to individuals and third parties).
		ID.RA-P2: Data analytic inputs and outputs are identified and evaluated for bias.
		ID.RA-P3: Potential problematic data actions and associated problems are identified.
		ID.RA-P4: Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.
		ID.RA-P5: Risk responses are identified, prioritized, and implemented.
	Data Processing Ecosystem Risk Management (ID.DE-P): The organization's priorities, constraints, risk tolerance, 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.	**ID.DE-P1:** Data processing ecosystem risk management policies, processes, and procedures are identified, established, assessed, managed, and agreed to by organizational stakeholders.
		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.
		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.
		ID.DE-P4: Interoperability frameworks or similar multi-party approaches are used to manage data processing ecosystem privacy risks.
		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, interoperability framework, or other obligations.

功能	类别	子类别
	风险评估(ID.RA-P):该组织了解隐私风险个人以及此类隐私风险如何可能对组织运营产生后续影响，包括使命、职能、其他风险管理优先级(例如，合规性、财务)，声誉、员工队伍和文化。	**ID.RA-P1:**与系统/产品/服务及数据操作相关的背景因素已被识别(例如个人的人口统计特征和隐私利益或看法、数据敏感性及/或类型、数据处理对个人和第三方的可见性)。
		ID.RA-P2:数据输入和输出被识别并评估偏见。
		ID.RA-P3:潜在的问题数据操作及相关问题被识别。
		ID.RA-P4:问题数据操作、可能性及影响被用于确定风险并排定优先级
		ID.RA-P5:风险应对措施已识别、排定优先级，并实施。
	数据处理生态系统风险管理(ID.DE-P):该组织的优先事项、限制条件、风险容忍度和假设被确立并用于支持与管理相关的风险隐私风险及第三方在数据处理生态系统。组织已建立并实施了识别、评估和管理隐私风险，在数据处理生态系统内。	**ID.DE-P1:**数据处理生态系统的风险管理政策、流程和程序由组织利益相关方识别、建立、评估、管理并达成一致。
		ID.DE-P2:数据处理生态系统各方(例如，服务提供商、客户、合作伙伴、产品制造商、应用程序开发者)使用隐私风险评估过程的决策。
		ID.DE-P3:与数据处理生态系统各方的合同被用于实施旨在满足组织隐私计划目标的适当措施。
		ID.DE-P4:互操作性框架或类似的多方方法被用于管理数据处理生态系统风险。
		ID.DE-P5：数据处理生态系统各方通过审计、测试结果或其他形式的评估进行例行评估，以确认其正在履行合同、互操作性框架或其他义务。

Function	Category	Subcategory
GOVERN-P (GV-P): Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.	**Governance Policies, Processes, and Procedures (GV.PO-P):** The policies, processes, and procedures to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk.	**GV.PO-P1:** Organizational privacy values and policies (e.g., conditions on data processing such as data uses or retention periods, individuals' prerogatives with respect to data processing) are established and communicated.
		GV.PO-P2: Processes to instill organizational privacy values within system/product/service development and operations are established and in place.
		GV.PO-P3: Roles and responsibilities for the workforce are established with respect to privacy.
		GV.PO-P4: Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners).
		GV.PO-P5: Legal, regulatory, and contractual requirements regarding privacy are understood and managed.
		GV.PO-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-P1:** Risk management processes are established, managed, and agreed to by organizational stakeholders.
		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(s) 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-P1:** The workforce is informed and trained on its roles and responsibilities.
		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.

功能	类别	子类别
治理-P(GV-P): 制定并实施组织治理结构，以持续理解由隐私风险提供信息的组织风险管理优先级。	**治理政策、流程和程序(GV.PO-P):**政策、用于管理和监控组织监管、法律、风险、环境和运营要求的流程和程序已被理解，并为隐私风险的管理提供信息。	**GV.PO-P1:**组织隐私价值观和政策(例如数据处理的条件，如数据使用或保留期限、个人在数据处理方面的权利)已确立并沟通。
		GV.PO-P2:在系统/产品/服务开发和运营中灌输组织隐私价值观的流程已确立并到位。
		GV.PO-P3:员工在隐私方面的角色和职责已确立。
		GV.PO-P4:隐私角色和职责与第三方利益相关方(例如服务提供商、客户、合作伙伴)协调并保持一致。
		GV.PO-P5:有关隐私的法律、监管和合同要求已被理解和管理。
		GV.PO-P6:治理和风险管理策略、流程和程序应对隐私风险。
	风险管理策略(GV.RM-P): 组织的优先级、约束、风险容忍度和假设已确立，并用于支持运营风险决策。	**GV.RM-P1:**风险管理流程已建立、管理，并经组织利益相关方同意。
		GV.RM-P2:组织风险容忍度已确定并明确表达。
		GV.RM-P3:组织对风险容忍度的确定以其在数据处理生态系统中的角色为依据。
	意识与培训(GV.AT-P):该组织的员工队伍和第三方参与数据处理的人员获得隐私意识教育以及培训以执行其隐私相关与.....一致的职责和责任相关政策、流程、程序和协议以及组织隐私价值观。	**GV.AT-P1:**员工了解并接受其角色和职责。
		GV.AT-P2:高级管理人员了解其角色和职责。
		GV.AT-P3:隐私人员了解其角色和职责。
		GV.AT-P4:第三方(例如服务提供商、客户、合作伙伴)了解其角

	Function	Category	Subcategory
		Monitoring and Review (GV.MT-P): The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.	**GV.MT-P1:** Privacy risk is re-evaluated on an ongoing basis and as key factors, including the organization's business environment (e.g., introduction of new technologies), governance (e.g., legal obligations, risk tolerance), data processing, and systems/products/services change.
			GV.MT-P2: Privacy values, policies, and training are reviewed and any updates are communicated.
			GV.MT-P3: Policies, processes, and procedures for assessing compliance with legal requirements and privacy policies are established and in place.
			GV.MT-P4: Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place.
			GV.MT-P5: Policies, processes, and procedures are established and in place to receive, analyze, and respond to problematic data actions disclosed to the organization from internal and external sources (e.g., internal discovery, privacy researchers, professional events).
			GV.MT-P6: Policies, processes, and procedures incorporate lessons learned from problematic data actions.
			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	**Data Processing Policies, Processes, and Procedures (CT.PO-P):** Policies, processes, and procedures are maintained and used to manage data processing (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) consistent with the organization's risk strategy to protect individuals' privacy.	**CT.PO-P1:** Policies, processes, and procedures for authorizing data processing (e.g., organizational decisions, individual consent), revoking authorizations, and maintaining authorizations are established and in place.
			CT.PO-P2: Policies, processes, and procedures for enabling data review, transfer, sharing or disclosure, alteration, and deletion are established and in place (e.g., to maintain data quality, manage data retention).
			CT.PO-P3: Policies, processes, and procedures for enabling individuals' data processing preferences and requests are established and in place.

	功能	类别	子类别
		监控与审查(GV.MT-P)：该政策、流程和程序，用于对组织隐私的持续审查态势被理解并为隐私风险的管理。	**GV.MT-P1:**隐私风险在持续基础上以及当关键因素发生变化时重新评估，包括组织的业务环境(例如引入新技术)、治理(例如法律义务、风险容忍度)、数据处理以及系统/产品/服务变更提供依据。
			GV.MT-P2：隐私价值观、政策和培训经过审查，任何更新均予以传达。
			GV.MT-P3：评估遵守法律要求和隐私政策的政策、流程和程序已建立并到位。
			GV.MT-P4:已建立并落实用于沟通隐私风险管理进展的政策、流程和程
			GV.MT-P5:已建立并落实相关政策、流程和程序，以接收、分析并响应从内部和外部来源(例如内部发现、隐私研究人员、专业活动)向组织披露的问题数据操作。
			GV.MT-P6:政策、流程和程序纳入从问题数据行为中吸取的教训。
			GV.MT-P7:接收、跟踪并响应个人关于组织隐私实践的投诉、关切和问题的政策、流程和程序已建立并到位。
	控制-P(CT-P)：制定并实施适当的活动以支持组织或个人以.....方式管理数据充分的粒度以	数据处理政策、流程和**程序(CT.PO-P):**策略、流程、并维护和使用相关程序，以管理数据处理(例如，目的、数据中的范围、角色和职责处理生态系统及管理承诺）与组织的风险保护策略个人的隐私。	**CT.PO-P1:**授权数据处理(例如组织决策、个人同意)、撤销授权和维持授权的政策、流程和程序已建立并到位。
			CT.PO-P2:支持数据审查、传输、共享或披露、更改和删除的政策、流程和程序已建立并到位(例如以维持数据质量、管理数据保留）。
			CT.PO-P3:支持个人数据处理偏好和请求的政策、流程和程序已建立并到位.

	Function	Category	Subcategory
	manage privacy risks.		**CT.PO-P4:** A data life cycle to manage data is aligned and implemented with the system development life cycle to manage systems.
		Data Processing Management (CT.DM-P): Data are managed consistent with the organization's risk strategy to protect individuals' privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization).	**CT.DM-P1:** Data elements can be accessed for review.
			CT.DM-P2: Data elements can be accessed for transmission or disclosure.
			CT.DM-P3: Data elements can be accessed for alteration.
			CT.DM-P4: Data elements can be accessed for deletion.
			CT.DM-P5: Data are destroyed according to policy.
			CT.DM-P6: Data are transmitted using standardized formats.
			CT.DM-P7: Mechanisms for transmitting processing permissions and related data values with data elements are established and in place.
			CT.DM-P8: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.
			CT.DM-P9: Technical measures implemented to manage data processing are tested and assessed.
			CT.DM-P10: Stakeholder privacy preferences are included in algorithmic design objectives and outputs are evaluated against these preferences.
		Disassociated Processing (CT.DP-P): Data processing solutions increase disassociability consistent with the organization's risk strategy to protect individuals' privacy and enable implementation of privacy principles (e.g., data minimization).	**CT.DP-P1:** Data are processed to limit observability and linkability (e.g., data actions take place on local devices, privacy-preserving cryptography).
			CT.DP-P2: Data are processed to limit the identification of individuals (e.g., de-identification privacy techniques, tokenization).
			CT.DP-P3: Data are processed to limit the formulation of inferences about individuals' behavior or activities (e.g., data processing is decentralized, distributed architectures).
			CT.DP-P4: System or device configurations permit selective collection or disclosure of data elements.
			CT.DP-P5: Attribute references are substituted for attribute values.

	功能	类别	子类别
	管理隐私风险。		**CT.PO-P4:**用于管理数据的数据生命周期与系统开发生命周期保持一致的系统。
		数据处理管理(CT.DM-P): 数据的管理与组织的风险保护策略个人的隐私，提高可管理性，并支持隐私原则的实施(例如，个人参与、数据质量、数据最小化）。	**CT.DM-P1:**数据元素可供查阅。
			CT.DM-P2:数据元素可被访问以进行传输或披露。
			CT.DM-P3:数据元素可被访问以进行更改。
			CT.DM-P4:数据元素可被访问以进行删除。
			CT.DM-P5:数据按照策略进行销毁。
			CT.DM-P6:数据使用标准化格式传输。
			CT.DM-P7:已建立并落实用于随数据元素传输处理权限及相关数据值的机制。
			CT.DM-P8:依据政策确定、记录、实施并审查审计/日志记录，并纳入数据最小化原则。
			CT.DM-P9:为管理数据处理而实施的技术措施经过测试和评估。
			CT.DM-P10:利益相关方的隐私偏好被纳入算法设计目标，并根据这些偏好评估输出。
		分离处理(CT.DP-P):数据处理解决方案提高去关联性，与组织的风险保持一致保护个人隐私的策略以及支持实施隐私原则（例如，数据最小化）。	**CT.DP-P1:**数据的处理方式限制可观察性和可链接性(例如，数据操作在本地设备上进行、隐私保护密码学）。
			CT.DP-P2:数据的处理方式限制对个人的识别(例如，去标识化隐私技术、
			CT.DP-P3:数据的处理方式限制对个人行为或活动进行推断(例如，数据处理去中心化、分布式架构)。
			CT.DP-P4:系统或设备配置允许选择性收集或披露数据元素。
			CT.DP-P5:属性引用被替换为属性值。

Function	Category	Subcategory
COMMUNICATE-P (CM-P): Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks.	**Communication Policies, Processes, and Procedures (CM.PO-P):** Policies, processes, and procedures are maintained and used to increase transparency of the organization's data processing practices (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) and associated privacy risks.	**CM.PO-P1:** Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established and in place.
		CM.PO-P2: Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established.
	Data Processing Awareness (CM.AW-P): Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the organization's risk strategy to protect individuals' privacy.	**CM.AW-P1:** Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place.
		CM.AW-P2: Mechanisms for obtaining feedback from individuals (e.g., surveys or focus groups) about data processing and associated privacy risks are established and in place.
		CM.AW-P3: System/product/service design enables data processing visibility.
		CM.AW-P4: Records of data disclosures and sharing are maintained and can be accessed for review or transmission/disclosure.
		CM.AW-P5: Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem.
		CM.AW-P6: Data provenance and lineage are maintained and can be accessed for review or transmission/disclosure.
		CM.AW-P7: Impacted individuals and organizations are notified about a privacy breach or event.
		CM.AW-P8: Individuals are provided with mitigation mechanisms (e.g., credit monitoring, consent withdrawal, data alteration or deletion) to address impacts of problematic data actions.
PROTECT-P (PR-P): Develop and implement	**Data Protection Policies, Processes, and Procedures (PR.PO-P):** Security and privacy policies (e.g., purpose, scope, roles	**PR.PO-P1:** A baseline configuration of information technology is created and maintained incorporating security principles (e.g., concept of least functionality).

功能	类别	子类别
沟通-P (CM-P) :制定并实施适当的活动以支持组织和个人能够可靠地理解并参与关于以下内容的对话 数据如何被处理并相关的隐私风险。	**沟通政策、流程和程序(CM.PO-P):**政策、流程、并维护和使用相关程序，以提高组织的透明度数据处理实践(例如，目的、数据处理生态系统中的范围、角色和职责，以及管理承诺)和相关的隐私风险。	**CM.PO-P1:**用于传达数据处理目的、实践及相关内容的透明度策略、流程，并且隐私风险已确立并落实到位。
		CM.PO-P2:用于传达数据处理目的、实践和相关隐私风险的角色和职责(例如，公共关系)已建立。
	数据处理意识(CM.AW-P):个人和组织拥有可靠的关于数据处理实践的知识以及与相关的隐私风险，以及有效的机制被使用和维护以提高可预测性，与组织的风险战略以保护个人的隐私。	**CM.AW-P1:**用于传达数据处理目的、实践、相关隐私风险以及支持个人数据处理偏好的选项的机制(例如，通知、内部或公开报告)并且请求已建立并落实到位。
		CM.AW-P2:用于获取个人关于数据处理和相关隐私的反馈的机制(例如，调查或焦点小组)关于数据处理和相关隐私风险已确立并到位。
		CM.AW-P3:系统/产品/服务设计支持数据处理可见性。
		CM.AW-P4:数据披露和共享的记录被维护，并可被访问以进行审查或传输/披露。
		CM.AW-P5:数据更正或删除可以传达给数据处理生态系统中的个人或组织(例如，数据源)。
		CM.AW-P6:数据来源和谱系被维护，并可被访问以进行审查或传输/披露。
		CM.AW-P7:受影响的个人和组织被告知隐私泄露或事件。
		CM.AW-P8:向个人提供缓解机制(例如，信用监控、撤回同意、数据更改或删除)，以应对有问题的数据操作的影响。
保护-P (PR-P):开发并实施	**数据保护政策、流程和程序(PR.PO-P):**安全与隐私政策(例如，目的、范围、角色)	**PR.PO-P1:**创建并维护信息技术的基线配置，纳入安全原则(例如，最小功能概念) 。

Function	Category	Subcategory
appropriate data processing safeguards.	and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data.	**PR.PO-P2:** Configuration change control processes are established and in place.
		PR.PO-P3: Backups of information are conducted, maintained, and tested.
		PR.PO-P4: Policy and regulations regarding the physical operating environment for organizational assets are met.
		PR.PO-P5: Protection processes are improved.
		PR.PO-P6: Effectiveness of protection technologies is shared.
		PR.PO-P7: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed.
		PR.PO-P8: Response and recovery plans are tested.
		PR.PO-P9: Privacy procedures are included in human resources practices (e.g., deprovisioning, personnel screening).
		PR.PO-P10: A vulnerability management plan is developed and implemented.
	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.	**PR.AC-P1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.
		PR.AC-P2: Physical access to data and devices is managed.
		PR.AC-P3: Remote access is managed.
		PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
		PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).
		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	**PR.DS-P1:** Data-at-rest are protected.
		PR.DS-P2: Data-in-transit are protected.

功能	类别	子类别
适当的数据处理保障措施。	以及数据处理中的职责生态系统，以及管理承诺）、流程和程序被维护并用于管理数据的保护。	**PR.PO-P2:**已建立配置变更控制流程并到位。
		PR.PO-P3:信息的备份被执行、维护，并且经过测试。
		PR.PO-P4:满足有关组织资产物理运行环境的政策和法规要求。
		PR.PO-P5:保护流程得到改进。
		PR.PO-P6:保护技术的有效性得到共享。
		PR.PO-P7:已建立、落实并管理响应计划(事件响应和业务连续性)与恢复计划(事件恢复和灾难恢复)。
		PR.PO-P8:响应和恢复计划经过测试。
		PR.PO-P9:隐私程序被纳入人力资源实践(例如，取消配置、人员筛
		PR.PO-P10:制定漏洞管理计划并实施。
	身份管理、身份验证、与访问控制(PR.AC-P):对数据和设备仅限于授权个人、流程和设备，并且是以与评估的风险相一致的方式进行管理未经授权访问的。	PR.AC-P1：为经授权的个人、流程和设备。
		PR.AC-P2:对数据和设备的物理访问受到管理。
		PR.AC-P3:远程访问受到管理。
		PR.AC-P4:访问权限和授权得到管理，纳入最小权限和职责分离原则职责。
		PR.AC-P5:网络完整性受到保护(例如，网络隔离、网络分段)。
		PR.AC-P6:个人和设备经过验证并绑定到凭证，且根据交易风险进行相应身份验证(例如，个人的安全和隐私风险以及其他组织风险)。
	数据安全(PR.DS-P):数据是按照以下方式管理，与	**PR.DS-P1:**静态数据受到保护。
		PR.DS-P2:传输中的数据受到保护。

Function	Category	Subcategory
	organization's risk strategy to protect individuals' privacy and maintain data confidentiality, integrity, and availability.	**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.
	Maintenance (PR.MA-P): System maintenance and repairs are performed consistent with policies, processes, and procedures.	**PR.MA-P1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.
		PR.MA-P2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.
	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.	**PR.PT-P1:** Removable media is protected and its use restricted according to policy.
		PR.PT-P2: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
		PR.PT-P3: Communications and control networks are protected.
		PR.PT-P4: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.

功能	类别	子类别
	组织的风险战略以保护 个人隐私并维护数据 保密性、完整性和可用性。	**PR.DS-P3:**在移除、传输和处置的全过程中，对系统/产品/服务及相关数
		PR.DS-P4:维护充足容量以确保可用性。
		PR.DS-P5:已实施针对数据泄露的防护措施。
		PR.DS-P6:使用完整性检查机制来验证软件、固件和信息完整性
		PR.DS-P7:开发和测试环境与生产环境分离。
		PR.DS-P8:使用完整性检查机制来验证硬件完整性。
	维护(PR.MA-P):系统 维护和修理按照 与政策、流程和 程序保持一致。	**PR.MA-P1:**使用经批准且受控的工具执行组织资产的维护和修理，并
		PR.MA-P2:组织资产的远程维护须经批准、记录日志，并以防 止未经授权访问的方式执行。
	保护技术(PR.PT-P): 技术安全解决方案得到管理 以确保以下方面的安全性和韧性： 系统/产品/服务及相关 数据，与相关政策、 流程、程序和协议保持一致。	**PR.PT-P1:**可移动介质受到保护，其使用受到限制 按照政策。
		PR.PT-P2:通过配置系统仅提供必要功能来纳入最小功能原则。
		PR.PT-P3:通信和控制网络受到保护。
		PR.PT-P4:实施机制(例如故障保护、负载均衡、热插拔)，以满足正常 和不利情况下的韧性要求。

Appendix B: Glossary

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

Attribute Reference (NIST SP 800-63-3 [8])	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 [8])	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 (44 U.S.C. [13])	Ensuring timely and reliable access to and use of information.
Category	The subdivision of a Function into groups of privacy outcomes closely tied to programmatic needs and particular activities.
Communicate-P (Function)	Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks.
Confidentiality (44 U.S.C. [13])	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	
(Framework for Improving Critical Infrastructure Cybersecurity [1])	A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.
(OMB 17-12 [9])	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.

附录 B：术语表

本附录定义了本出版物所使用的部分术语。

属性参考(NIST SP 800-63-3[8])	一种独立于格式的陈述，断言订阅者的某项属性，但不一定包含身份信息。例如，对于属性"生日"，引用可以是"年满18岁"或"出生于12月"。
属性值(NIST SP 800-63-3[8])	一种独立于格式的完整陈述，断言订阅者的某项属性。例如，对于属性"生日"，值可以是"12/1/1980"或"December 1, 1980"。
可用性(44 U.S.C.[13])	确保及时、可靠地访问和使用信息。
类别	将功能细分为与计划需求和特定活动密切相关的隐私结果组。
沟通-P(功能)	制定并实施适当的活动，使组织和个人能够可靠地理解并就数据处理方式及相关隐私风险进行对话。
保密性(44 U.S.C.[13])	维护对信息访问和披露的授权限制，包括保护个人隐私和专有信息的手段。
控制-P(功能)	制定并实施适当的活动，使组织或个人能够以足够的粒度管理数据以管理隐私风险。
核心	一组隐私保护活动和结果。框架核心包含三个要素：功能、类别和子类别。
网络安全事件	
(提升关键基础设施网络安全框架[1])	一种已确定对组织产生影响、促使需要响应和恢复的网络安全事件。
(OMB 17-12[9])	一种事件，其(1)实际或即将在无合法权限，信息或信息系统的完整性、保密性或可用性；或(2)构成对法律、安全策略、安全程序或可接受使用策略的违反或即将违反的威胁。
数据	信息的表示，包括数字和非数字格式。

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.
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.
Govern-P (Function)	Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.
Identify-P (Function)	Develop the organizational understanding to manage privacy risk for individuals arising from data processing.
Implementation Tier	Provides a point of reference on how an organization views privacy risk and whether it has sufficient processes and resources in place to manage that risk.
Individual	A single person or a group of persons, including at a societal level.
Integrity (44 U.S.C. [13])	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 [10])	Information describing the characteristics of data. This may include, for example, structural metadata describing data structures (i.e., data format, syntax, semantics) and descriptive metadata describing data contents.
Predictability (Adapted from NIST IR 8062 [5])	Enabling reliable assumptions by individuals, owners, and operators about data and their processing by a system, product, or service.

数据动作(改编自 NIST IR 8062[5])	系统/产品/服务数据生命周期操作，包括但不限于收集、保留、记录、生成、转换、使用、披露、共享、传输和处置。
数据元素	传达有意义信息的最小命名数据项。
数据处理(改编自 NIST IR 8062[5])	数据操作的集合(即完整的数据生命周期，包括但不限于收集、保留、记录、生成、转换、使用、披露、共享、传输和处置)。
数据处理生态系统	参与创建或部署系统、产品或服务或任何处理数据的组件的实体之间复杂且相互关联的关系。
不可关联性(改编自 NIST IR 8062[5])	在不超出系统操作要求的情况下，实现与个人或设备无关联的数据或事件处理。
功能	核心的组成部分，为将基本隐私活动组织为类别和子类别提供最高级别的结构。
治理-P(功能)	制定并实施组织治理结构，以便持续理解组织在隐私风险影响下的风险管理优先事项。
识别-P(功能)	发展组织理解，以管理数据处理所产生的个人隐私风险。
实施层级	提供参考点，说明组织如何看待隐私风险以及是否具备足够的流程和资源来管理该风险。
个人	个人或一群人，包括社会层面。
完整性 (44 U.S.C. [13])	防止不当的信息修改或破坏，并包括确保信息的不可否认性和真实性。
数据沿袭	数据元素的处理历史，可能包括点对点数据流以及对该数据元素执行的数据操作。
可管理性(改编自 NIST IR 8062[5])	提供对数据进行细粒度管理的能力，包括更改、删除和选择性披露。
元数据(改编自 NIST SP 800-53[10])	描述数据特征的信息。 这可能包括，例如，描述数据结构(即数据格式、语法、语义)的结构元数据和描述数据内容的描述性元数据。
可预测性(改编自 NIST IR 8062[5])	使个人、所有者和操作者能够对数据及其由系统、产品或服务进行的处理做出可靠的假设。

Privacy Breach (Adapted from OMB M-17-12 [9])	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 [7])	The administrative, technical, and physical safeguards employed within an organization to satisfy privacy requirements.
Privacy Event	The occurrence or potential occurrence of problematic data actions.
Privacy Requirement	A specification for system/product/service functionality to meet stakeholders' desired privacy outcomes.
Privacy Risk	The likelihood that individuals will experience problems resulting from data processing, and the impact should they occur.
Privacy Risk Assessment	A privacy risk management sub-process for identifying and evaluating specific privacy risks.
Privacy Risk Management	A cross-organizational set of processes for identifying, assessing, and responding to privacy risks.
Problematic Data Action (Adapted from NIST IR 8062 [5])	A data action that could cause an adverse effect for individuals.
Processing	See *Data Processing*.
Profile	A selection of specific Functions, Categories, and Subcategories from the Core that an organization has prioritized to help it manage privacy risk.
Protect-P (Function)	Develop and implement appropriate data processing safeguards.
Provenance (Adapted from NIST IR 8112 [11])	Metadata pertaining to the origination or source of specified data.
Risk (NIST SP 800-30 [12])	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Risk Management	The process of identifying, assessing, and responding to risk.
Risk Tolerance (NIST SP 800-39 [6])	The level of risk or degree of uncertainty that is acceptable to organizations.
Subcategory	The further divisions of a Category into specific outcomes of technical and/or management activities.

隐私泄露(改编自 OMB M-17-12[9])	控制丧失、泄露、未经授权的披露、未经授权的获取或任何类似事件，其中(1)非授权用户访问或可能访问数据，或(2)授权用户出于非授权目的访问数据。
隐私控制(改编自 NIST SP 800-37[7])	组织内部为满足隐私要求而采用的管理、技术和物理保障措施。
隐私事件	问题数据操作的发生或潜在发生。为满足利益相关方期望的隐私结果而对系统/产品/服务功能进行的规范说明。
隐私要求	
隐私风险	个人因数据处理而经历问题的可能性，以及问题发生时应产生的影响。
隐私风险评估用于识别和评估的隐私风险管理子流程	特定的隐私风险。
隐私风险管理	用于识别、评估和应对隐私风险的跨组织流程集合。
问题性数据行为(改编自 NIST IR 8062[5])	可能对个人造成不利影响的数据操作。
处理	参见数据处理。
配置文件	从核心中选择组织已优先考虑以帮助其管理隐私风险的特定功能、类别和子类别。制定并实施适当的数据处理保障措施。与指定数据的来源或出处相关的元数据。
保护-P(功能)	
来源(改编自 NIST IR 8112[11])	
风险 （NIST SP 800-30 [12] ）	衡量实体受潜在情况或事件威胁程度的指标，通常取决于：(i) 如果情况或事件发生将产生的不利影响；以及(ii) 发生的可能性。
风险管理	识别、评估和应对风险的过程。组织可接受的风险水平或不确定性程度。
风险容忍度(NIST SP 800-39[6])	
子类别	类别进一步划分为技术和/或管理活动的具体结果。

Appendix C: Acronyms

This appendix defines selected acronyms used in the publication.

IEC	International Electrotechnical Commission
IR	Interagency or Internal Report
ISO	International Organization for Standardization
IT	Information Technology
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OECD	Organisation for Economic Co-operation and Development
OMB	Office of Management and Budget
PMRM	Privacy Management Reference Model and Methodology
PRAM	Privacy Risk Assessment Methodology
RFC	Request for Comment
RFI	Request for Information
SDLC	System Development Life Cycle
SP	Special Publication

附录 C：缩略语

本附录定义了出版物中使用的选定缩略语。

IEC 国际电工委员会 IR 跨机构或内部报告

ISO 国际标准化组织 IT 信息技术

NIST 美国国家标准与技术研究院
OASIS 结构化信息标准促进组织 OECD 经济合作与发展组织 OMB 管理和预算办公室

PMRM 隐私管理参考模型和方法论 PRAM 隐私风险评估方法论 RFC 征求意见稿

信息征询书
SDLC 系统开发生命周期 SP 特别出版物

Appendix D: Privacy Risk Management Practices

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

Organizing Preparatory Resources

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

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

- **Risk management role assignments** (GV.PO-P3, GV.PO-P4)

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

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

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

- **Key stakeholders** (GV.PO-P4, ID.DE-P)

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

附录 D：隐私风险管理实践

第1.2节介绍了围绕隐私风险管理的一些考虑因素，包括网络安全与隐私风险之间的关系以及隐私风险评估的作用。本附录考虑了有助于成功实施隐私风险管理的一些关键实践，包括组织准备性资源、确定隐私能力、定义隐私要求、开展隐私风险评估、创建隐私要求可追溯性以及监测不断变化的隐私风险。文中包含类别和子类别引用，以便使用核心来支持这些实践；这些引用出现在括号中。

组织准备资源

适当的资源有助于在组织各层级就隐私风险做出知情决策。从实践角度来看，各类资源的开发责任可能属于组织的不同组成部分。因此，依赖某些资源的组织组成部分可能会发现这些资源要么不存在，要么可能不足以应对隐私问题。在这些情况下，依赖方可以考虑该资源的目的，并通过其他来源寻求信息，或利用现有信息做出其所能做的最佳决策。简而言之，良好的资源是有帮助的，但任何缺陷都不应阻止组织组成部分在其能力范围内做出最佳风险决策。以下资源虽非详尽无遗，但为更好的决策奠定了基础。

- **风险管理角色分配**(GV.PO-P3, GV.PO-P4)

  在组织内建立并促成对谁负责隐私风险管理以及组织内其他风险管理任务的跨组织理解，有助于改善决策的协调性和问责制。此外，广泛的观点可以改进识别、评估和应对隐私风险的流程。一个多元化的跨职能团队可以帮助识别对个人隐私更全面的风险范围，并选择更广泛的缓解措施。确定哪些角色应参与风险管理讨论取决于组织背景和构成，尽管组织隐私与网络安全项目之间的协作将非常重要。如果一个人被分配多个角色，则应考虑管理潜在的利益冲突。

- 企业风险管理策略(GV.RM-P)

  组织的企业风险管理策略有助于将组织的使命和价值观与组织风险容忍度、假设、约束和优先级保持一致。为实现使命或业务目标以及管理广泛风险组合的资源限制很可能需要权衡取舍。使参与隐私风险管理流程的人员更好地理解组织的风险容忍度，应有助于指导有关如何分配资源的决策，并改善有关风险应对的决策。

- **关键利益相关方**(GV.PO-P4, ID.DE-P)

  隐私利益相关方是指那些对系统、产品或服务的隐私结果有利益或关注的人。例如，法律方面的关注可能集中在系统、产品或服务的运行方式是否会导致组织违反隐私法律或法规或其业务协议。希望最大化使用率的业务所有者可能担心因隐私保护不佳而导致对系统、产品或服务的信任丧失

due to poor privacy. Individuals whose data are being processed or who are interacting with the system, product, or service will be interested in not experiencing problems or adverse consequences. Understanding the stakeholders and the types of privacy outcomes they are interested in will facilitate system/product/service design that appropriately addresses stakeholders' needs.

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

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

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

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

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

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

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

Determining Privacy Capabilities

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

其数据正在被处理或正在与系统、产品或服务交互的个人，会关注不经历问题或不利后果。理解利益相关方及其感兴趣的隐私结果类型，将有助于系统/产品/服务的设计适当地满足利益相关方的需求。

- **组织级隐私要求**(GV.PO-P)

  组织级隐私要求是表达组织打算遵守的法律义务、隐私价值观和政策的一种手段。理解这些要求是确保系统/产品/服务设计符合其义务的关键。组织级隐私要求可能来源于多种渠道，包括：

  o 法律环境(例如，法律、法规、合同);o 组织政策或文化价值观；o 相关标准；以及

  o 隐私原则。

- **系统/产品/服务设计工件**(ID.BE-P3)

  设计工件可以采取多种形式，例如系统设计架构或数据流图。这些工件帮助组织确定其系统、产品和服务将如何运行。因此，它们可以帮助隐私项目理解系统、产品和服务需要如何运作，以便能够以在保护隐私的同时维持功能性的方式选择和实施有助于缓解隐私风险的控制或措施。

- **数据映射**(ID.IM-P)

  数据映射图说明数据处理以及个人与系统、产品和服务的交互。数据映射图展示数据处理环境，并包括处理数据或个人与之交互的组件、组件的所有者或运营者，以及离散的数据操作和正在处理的特定数据元素。数据映射图可以用不同方式呈现，详细程度可能因组织需求而异。为方便起见并便于组织各组成部分之间的沟通，数据映射图可以叠加在现有系统/产品/服务设计工件上。如下文所述，数据映射图是隐私风险评估中的重要工件。

确定隐私能力

隐私能力可用于描述实现预期隐私结果的系统、产品或服务属性或特征(例如，"该服务支持数据最小化")。保密性、完整性和可用性等安全目标以及安全需求用于为系统、产品或服务的安全能力提供信息。如**表3**所述，一组额外的隐私工程目标可以支持隐私能力的确定。组织还可以将隐私工程目标用作高层级优先级排序工具。可预测性、可管理性或可分离性较低的系统、产品或服务可能是隐私风险增加的信号，因此值得进行更全面的隐私风险评估。

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

Table 3: Privacy Engineering and Security Objectives[18]

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

Defining Privacy Requirements

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

[18] The privacy engineering objectives are adapted from NIST IR 8062 [5]. The security objectives are from NIST SP 800-37, Rev. 2 [7].

在确定隐私能力时，组织可以考虑哪些隐私工程和安全目标对其使命或业务需求、风险容忍度和组织级隐私要求最为重要(参见上文"组织准备资源")。并非所有目标都可能同等重要，或者可能需要在它们之间进行权衡。尽管隐私能力通过支持风险优先级排序决策为隐私风险评估提供信息，但隐私能力也可以从风险评估中获得信息，并进行调整以支持特定隐私风险的管理或应对环境变化，包括系统、产品或服务的设计变更。

表3:隐私工程与安全目标[18]

	目标	定义	主要相关方功能来自隐私框架核心
隐私工程目标	可预测性	使个人、所有者和操作者能够对数据及其由系统进行的处理	识别-P、治理-P、控制-P、沟通-P、保护-P
	可管理性	提供对数据进行细粒度管理的能力，包括收集、更改、删除和选择性披露	识别-P、治理-P、控制-P
	可分离性	支持在超出运营要求的情况下处理数据或事件，而不与个人或设备关联系统	识别-P、治理-P、控制-P
安全目标	保密性	维护对信息访问和披露的授权限制，包括保护个人隐私和专有信息的手段	识别-P、治理-P、保护-P
	完整性	防止不当的信息修改或破坏；包括确保信息的不可否认性和真实性	识别-P、治理-P、保护-P
	可用性	确保及时、可靠地访问和使用信息的	识别-P、治理-P、保护-P

定义隐私要求

隐私要求规定了系统、产品或服务需要如何运作以满足利益相关方期望的隐私结果(例如，"应用程序配置为允许用户选择特定数据元素")。要定义隐私要求，需考虑组织级隐私要求(参见上文"组织准备资源")和隐私风险评估的输出。此过程帮助组织回答两个问题：1)系统、产品或服务在数据处理和与个人交互方面能够做什么?2)它应该做什么?然后，组织可以分配资源，以能够实现所定义要求的方式设计系统、产品或服务。最终，定义隐私要求可以促成以下内容的制定：

18 隐私工程目标改编自 NIST IR 8062[5]。安全目标来自 NIST SP 800-37, Rev.2[7]。

systems, products, and services that are more mindful of individuals' privacy, and are based on informed risk decisions.

Conducting Privacy Risk Assessments

Conducting a privacy risk assessment helps an organization to identify privacy risks engendered by the system, product, or service and prioritize them to be able to make informed decisions about how to respond to the risks (ID.RA-P, GV.RM-P). Methodologies for conducting privacy risk assessments may vary, but organizations should consider the following characteristics:[19]

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

  Risk models define the risk factors to be assessed and the relationships among those factors.[20] If an organization is not using a pre-defined risk model, an organization should clearly define which risk factors it will be assessing and the relationships among these factors. Although cybersecurity has a widely used risk model based on the risk factors of threats, vulnerabilities, likelihood, and impact, there is not one commonly accepted privacy risk model. NIST has developed a privacy risk model to calculate risk based on the likelihood of a problematic data action multiplied by the impact of a problematic data action; each of the three risk factors are explained below.

  Privacy Risk Factors:
  Problematic Data Action | Likelihood | Impact

  - A problematic data action is any action a system takes to process data that could result in a problem for individuals. Organizations consider the type of problems that are relevant to the population of individuals. Problems can take any form and may consider the experience of individuals.[21]
  - Likelihood is defined as a contextual analysis that a data action is likely to create a problem for a representative set of individuals. Context can include organizational factors (e.g., geographic location, the public perception about participating organizations with respect to privacy), system factors (e.g., the nature and history of individuals' interactions with the system, visibility of data processing to individuals and third parties), or individual factors (e.g., individuals' demographics, privacy interests or perceptions, data sensitivity).[22] A data map can help with this contextual analysis (see Organizing Preparatory Resources).
  - Impact is an analysis of the costs should the problem occur. As noted in section 1.2, organizations do not experience these problems directly. Moreover, individuals' experiences may be subjective. Thus, impact may be difficult to assess accurately. Organizations should

19 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].

20 See NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments* [12] at p. 8.

21 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.

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

更加关注个人隐私的系统、产品和服务，并且基于知情的风险决策。

开展隐私风险评估

开展隐私风险评估有助于组织识别由系统、产品或服务产生的隐私风险，并对其进行优先级排序，以便能够就如何应对风险做出知情决策(ID.RA-P、GV.RM-P)。开展隐私风险评估的方法可能各不相同，但组织应考虑以下特征：[19]

- **风险模型**(ID.RA-P, GV.MT-P1)

  风险模型定义了要评估的风险因素以及这些因素之间的关系。[20]如果组织未使用预定义的风险模型，组织应明确界定其将评估哪些风险因素以及这些因素之间的关系。尽管网络安全有一个基于威胁、等风险因素的广泛使用的风险模型，

  漏洞、可能性与影响，

  隐私风险因素：
  有问题的数据操作 | 可能性 | 影响

  但并没有一个普遍接受的隐私风险模型。NIST 开发了一个隐私风险模型，基于有问题数据行为的可能性乘以有问题数据行为的影响来计算风险；下面解释这三个风险因素中的每一个。

  o 有问题数据行为是系统为处理数据而采取的任何可能导致
  个人问题的行为。组织考虑与个人群体相关的问题类型。问题可以采取任何形式，并可能考虑个人的体验。[21]

  o 可能性被定义为一种上下文分析，即数据行为可能产生问题
  针对一组具有代表性的个人。情境可以包括组织因素(例如，地理位置、公众对参与组织的隐私看法)、系统因素(例如，个人与系统交互的性质和历史、数据处理对个人和第三方的可见性)或个人因素(例如，个人的人口统计特征、隐私利益或看法、数据敏感性)。[22]数据映射可以帮助进行这种情境分析(参见"组织准备资源")。o 影响是对问题发生时成本的分析。如第1.2节所述，

  组织不会直接经历这些问题。此外，个人的体验可能是主观的。因此，影响可能难以准确评估。组织应

19 NIST 开发了隐私风险评估方法(PRAM)，可帮助组织识别、评估和应对隐私风险。它由一组工作表组成，可在[3]获取。

[20]参见 NIST SP 800-30 Rev.1,风险评估实施指南[12]第 8 页。

21 作为其 PRAM 的一部分，NIST 创建了一个供参考的问题数据操作和问题示例目录[3]。其他组织可能创建了额外的问题集，或将其称为不利后果或危害。

[22]有关上下文因素的更多信息，请参见 NIST PRAM。同上，工作表 2。

consider the best means of internalizing impact to individuals in order to appropriately prioritize and respond to privacy risks.[23]

- **Assessment approach**

  The assessment approach is the mechanism by which identified risks are prioritized. Assessment approaches can be categorized as quantitative, semi-quantitative, or qualitative.[24] [25]

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

  Given the applicable limits of an organization's resources, organizations prioritize the risks to facilitate communication about how to respond.[26]

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

  As described in section 1.2.2, response approaches include mitigation, transfer/sharing, avoidance, or acceptance.[27]

Creating Privacy Requirements Traceability

Once an organization has determined which risks to mitigate, it can refine the privacy requirements and then select and implement controls (i.e., technical, physical, and/or policy safeguards) to meet the requirements.[28] An organization may use a variety of sources to select controls, such as NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations.*[29] After implementation, an organization iteratively assesses the controls for their effectiveness in meeting the privacy requirements and managing privacy risk. In this way, an organization creates traceability between the controls and the privacy requirements, and demonstrates accountability between its systems, products, and services and its organizational privacy goals.

Monitoring Change

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

23 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.

24 See NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments* at [12] p. 14.

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

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

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

28 See NIST SP 800-37, Rev. 2 [7].

29 See NIST SP 800-53 as updated [10].

考虑将个人影响内部化的最佳方式，以便适当地优先排序和应对隐私风险。[23]

- **评估方法**

  评估方法是已识别风险被优先排序的机制。评估方法可分为定量、半定量或定性。[24][25]

- **优先考虑风险**(ID.RA-P4)

  在组织资源的适用限制下，组织对风险进行优先级排序，以促进关于如何响应的沟通。[26]

- **应对风险**(ID.RA-P5)

  如第1.2.2节所述，响应方法包括缓解、转移/分担、规避或接受。[27]

创建隐私需求可追溯性

一旦组织确定了要缓解哪些风险，就可以细化隐私要求，然后选择并实施控制措施(即技术、物理和/或策略保障措施)以满足要求。[28]组织可以使用多种来源来选择控制措施，例如 NIST SP 800-53,《信息系统和组织的安全与隐私控制》。[29]实施后，组织迭代评估控制措施在满足隐私要求和管理隐私风险方面的有效性。通过这种方式，组织在控制措施与隐私要求之间建立可追溯性，并展示其系统、产品和服务与其组织隐私目标之间的问责制。

监测变更

隐私风险管理不是一个静态过程。组织监控其业务环境的变化--包括新的法律法规和新兴技术--以及对其系统、产品和服务的相应变化可能如何影响隐私风险，并迭代地使用本附录中的实践进行相应调整。(GV.MT-P1)

23 NIST PRAM 使用组织成本(如不合规成本、直接业务成本、声誉成本和内部文化成本)作为驱动因素，来考虑如何评估个人影响。同上，工作表 3，影响选项卡。[24]参见 NIST SP 800-30, Rev.1, 风险评估实施指南第[12]14 页。[25] NIST PRAM 使用基于 1-10 量表的半定量方法。

26 NIST PRAM 提供各种优先级排序表示形式，包括热图。参见[3]工作表3。27 NIST PRAM 提供了响应已优先级排序的隐私风险的过程。同上，工作表4。28 参见 NIST SP 800-37, Rev.2 [7]。29 参见 NIST SP 800-53 更新版 [10]。

Appendix E: Implementation Tiers Definitions

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

Tier 1: Partial

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

Tier 2: Risk Informed

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

附录 E：实施层级定义

下文概述的四个层级各由四个要素定义：层级1：部分

- **隐私风险管理过程**-组织隐私风险管理实践未正式化，风险以临时且有时是被动的方式进行管理。隐私活动的优先级排序可能不直接依据组织风险管理优先级、隐私风险评估或任务或业务目标。
- **集成隐私风险管理计划**-组织层面对隐私风险的意识有限。组织由于来自外部来源的不同经验或信息，以不规则的、逐案的方式实施隐私风险管理。组织可能没有能够在组织内部共享有关数据处理及由此产生的隐私风险信息的流程。
- **数据处理生态系统关系** - 对于组织在更大生态系统中相对于其他实体(例如，买方、供应商、服务提供商、业务关联方、合作伙伴)的角色，理解有限。组织没有用于识别隐私风险如何在整个生态系统中扩散的流程，也没有用于向生态系统中其他实体传达隐私风险或要求的流程。
- **员工队伍**-部分人员可能对隐私风险或隐私风险管理过程的理解有限，但没有具体的隐私职责。如果存在隐私培训，也是临时的，且内容未与最佳实践保持同步更新。

第2级：风险知情

- **隐私风险管理过程** - 风险管理实践经管理层批准，但可能未确立为组织范围内的政策。隐私活动的优先级排序直接依据组织风险管理优先级、隐私风险评估或任务或业务目标。
- **集成隐私风险管理计划** - 组织层面已具备隐私风险意识，但尚未建立全组织范围的隐私风险管理方法。有关数据处理及由此产生的隐私风险的信息在组织内部以非正式方式共享。在组织目标和计划中对隐私的考量可能发生在组织的某些层面，但并非所有层面。会开展隐私风险评估，但通常不可重复或非周期性发生。
- **数据处理生态系统关系** - 对于组织在更大生态系统中相对于其他实体(例如，买方、供应商、服务提供商、业务关联方、合作伙伴)的角色，有一定程度的理解。组织了解与其提供和使用的产品和服务相关的隐私生态系统风险，但未一致地或正式地针对这些风险采取行动。
- **员工队伍** - 有具备具体隐私职责的人员，但他们可能同时承担非隐私职责。定期为隐私人员开展隐私培训，但没有一致的流程来更新最佳实践。

Tier 3: Repeatable

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

Tier 4: Adaptive

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

第 3 级：可重复

- **隐私风险管理过程** - 组织的风险管理实践经正式批准并表述为政策。组织隐私实践基于风险管理过程对任务或业务目标变化以及不断变化的风险、政策和技术格局的应用而定期更新。
- **集成隐私风险管理计划** - 已建立全组织范围的方法来管理隐私风险。风险知情政策、流程和程序已定义、按预期实施并接受审查。已建立一致的方法来有效应对风险变化。组织持续且准确地监控隐私风险。高级隐私高管和非隐私高管定期就隐私风险进行沟通。高级高管确保在组织所有运营环节中考虑隐私。
- **数据处理生态系统关系** - 组织了解其在更大生态系统中的角色、依赖关系和受其影响方，并可能为社区更广泛地理解风险作出贡献。组织知晓其提供和使用的产品与服务相关的隐私生态系统风险。此外，组织通常对这些风险采取正式行动，包括通过书面协议等机制传达隐私要求、治理结构以及政策实施与监控。
- **员工队伍**-专职隐私人员具备履行其指定角色和职责的知识和技能。为所有人员提供定期、最新的隐私培训。

第4级：自适应

- **隐私风险管理过程** - 组织基于从隐私事件中吸取的教训以及对新隐私风险的识别来调整其隐私实践。通过纳入先进隐私技术和实践的持续改进过程，组织积极适应不断变化的政策和技术格局，并及时有效地响应不断演变的隐私风险。
- **集成隐私风险管理计划** - 已建立全组织范围的隐私风险管理方法，使用风险知情政策、流程和程序来处理有问题的数据操作。隐私风险与组织目标之间的关系得到清晰理解，并在决策时予以考虑。高级高管在与网络安全风险、财务风险和其他组织风险相同的背景下监控隐私风险。组织预算基于对当前和预期风险环境及风险容忍度的理解。业务部门在组织风险容忍度的背景下执行高管愿景并分析系统级风险。隐私风险管理是组织文化的一部分，并从经验教训以及对数据处理及由此产生的隐私风险的持续认知中演进。组织能够快速高效地说明业务/任务目标变化对风险处理方式和沟通方式的影响。
- **数据处理生态系统关系**-组织了解其在更大生态系统中的角色、依赖关系和受其影响方，并为社区更广泛地理解风险作出贡献。组织使用实时或近实时信息来理解并持续应对其提供和使用的产品与服务相关的隐私生态系统风险。此外，组织主动沟通，使用正式(例如协议)和非正式机制来发展和维持强大的生态系统关系。

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

- **员工队伍**-组织在整个组织结构中拥有专业化的隐私技能组合；具有多元视角的人员为隐私风险管理做出贡献。为所有人员提供定期、最新的专业化隐私培训。各级人员都理解组织的隐私价值观及其在维护这些价值观中的作用。

How this file was made

This is a complete Chinese translation of the NIST Privacy Framework 1.0. Tables, captions, headers, footers and numbering all keep their original positions. Nothing has been cut.

If you have documents of your own

- Contracts, tenders, standards, patents, reports: original layout kept, CNY 0.15/page
- PDF to Word: free up to 100 pages, CNY 0.10/page beyond that
- Scanned or image-only PDFs: OCR to Word, free
- No sign-up, no login: upload and download

Open the address below and try it with your own file:

https://www.ivyivy.com.cn/nist-privacy-fw-1-0-zh

On-premise deployment available (subject to model and compliance review)

Machine translation, provided for reading reference only. For professional judgement and compliance citation, please refer to the original English source.

This page is a translator's note; it is not part of the original document.

这份文件是怎么做出来的

本译本是《隐私框架 1.0》的中文全译本，共 43 页。表格、图注、页眉页脚、编号层级都按原文位置一一还原，未做任何删节。

你手上如果也有英文文件要处理

- 合同、标书、标准、专利、报告：翻译后保留原版式，0.15 元/页
- PDF 转 Word：100 页内免费，超出 0.1 元/页
- 扫描件、图片版 PDF：先 OCR 再转 Word，免费
- 不用注册、不用登录，传上去直接下载

打开下面这个地址，把你自己的文件传上去试试：

https://www.ivyivy.com.cn/nist-privacy-fw-1-0-zh

支持私有化部署（需按贵方模型与合规要求评估）

本译本由机器翻译生成，仅供阅读参考；专业技术判断与合规引用，请以英文原文为准。

本页为译制说明，不属于原文件内容。