安全加社区

公益译文项目

2020

NIST 隐私框架：通过企业风险管理促进隐私保护

第 1 版

美国商务部国家标准与技术研究院（NIST）

2020 年 1 月

文档信息			
原文名称	NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management（V1.0）		
原文作者	美国商务部国家标准与技术研究院（NIST）	原文发布日期	2020 年 1 月
原文发布单位	美国商务部国家标准与技术研究院（NIST）		
原文出处	https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf		
译者	小蜜蜂公益翻译组	校对者	小蜜蜂公益翻译组

执行摘要

在过去的二十多年间，互联网和相关信息技术驱动了前所未有的创新，创造了经济价值，促进了社会服务。这些益处大多源自复杂生态系统中的个人数据，这个系统是如此复杂以至于个人很难认识到与系统/产品/服务交互时可能会对自己的隐私造成什么样的后果。同时，组织也很难充分意识到这些交互对个人、社会或自己造成的后果以及这些后果对其品牌、收入和未来增长预期的影响。

国家标准与技术研究院（NIST）与公私有利益相关者合作，采用基于共识的透明流程，开发了《隐私框架：通过企业风险管理促进隐私保护》（简称《隐私框架》）。这是一个自愿性隐私管理工具，用以优化隐私工程实践，支持“隐私设计”（Privacy by Design）概念，帮助组织保护个人隐私。《隐私框架》在以下几个方面为组织提供支撑：

- 支持产品、服务设计或部署中的道德决策，推动数据的有益使用，将对个人隐私和全社会的负面影响降至最低，从而建立客户信任1；
- 履行当前合规义务，设计面向未来的产品、服务，以适应不断变化的技术和政策环境；及
- 与个人、业务合作伙伴、评估人和监管者就隐私实践进行沟通。

在利用数据的同时，还要管理个人隐私风险，对此并没有一刀切的解决方案。就像盖房子一样，只要地基设计合理，房主可自主选择房间布局和设计。至于隐私保护，只要在产品、服务中加入了有效的隐私风险保护措施，剩下的就由个人来选择了。《隐私框架》采用了基于风险和结果的方法，具有足够的灵活性，可以满足多样化隐私需求，提供更具创新性的有效解决方案，帮助个人和企业达成更好的结果，并紧跟人工智能和物联网等方面的最新技术趋势。

《隐私框架》采用了与《提升关键基础设施网络安全框架》（《网络安全框架》[1]）同样的架构，便于组织同时使用这两个框架。

与《网络安全框架》一样，《隐私框架》也包含三个组件：核心（Core）、Profile、实现层级（Implementation Tiers）。各组件将业务/任务驱动因素、组织角色及其职责和隐私保护活动关联起来，以此加强隐私风险管理。

- 核心组件促成各级人员（从管理层到执行/运营层）在重要隐私保护活动和预期结果方面进行沟通；
- Profile 组件按照组织隐私价值、任务/业务需求和风险情况，确定各项结果和活动的优先级；
- 实现层级就组织流程和资源是否足以管理隐私风险提供决策和沟通支撑。

总而言之，《隐私框架》旨在将隐私风险与企业的风险机制对齐，帮助组织夯实隐私基础。

致谢

本框架是 NIST 与公私有部门的组织和个人利益相关者之间的合作成果。在编写过程中，NIST 组织了三次公开研讨会、一次信息征询（RFI）、一次意见征求（RFC）以及五次网络研讨会，并与利益相关者进行了数百次的直接互动[2]。NIST 在此感谢所有为本框架做出贡献的人。

1 道德决策没有客观标准；它建立在特定社会的规范、价值观和法律期望的基础上。
2 完整框架开发过程记录，请访问 https://www.nist.gov/privacy-framework。

1. 《隐私框架》介绍

在过去的二十多年间，互联网和相关信息技术驱动了前所未有的创新，创造了经济价值，让社会服务更为便利。这些益处大多源自复杂生态系统中的个人数据，这个系统是如此复杂以至于个人很难认识到与系统/产品/服务交互时可能会对自己的隐私造成什么样的后果。即使是组织也未必能充分意识到这种后果。对隐私风险放任不管会对个人和社会造成直接的不利影响，后续会持续影响组织的品牌、收入和未来增长预期。数据处理一方面为组织带来益处，另一方面，带来了隐私风险，如何在此过程中保护个人隐私，这个任务颇具挑战，没有一刀切的解决方案。

之所以说隐私保护具有挑战性，是因为：（1）隐私保护是个含义宽泛的概念，旨在帮助维护诸如人的自主权和尊严之类的重要价值观；（2）隐私保护实现方式各有不同[3]，例如，可以通过隔离、限制查看或个人控制其身份相关信息（身体、数据、声誉等[4]）来实现隐私。此外，人的自主权和尊严并非是一成不变、可量化的概念，而是经过文化多样性和个体差异的过滤。隐私的这种宽泛、易变的性质让组织内部、组织之间以及组织和个人之间很难明确传达隐私风险，原因是缺少了通用语言和可满足各种隐私需求的灵活的实用工具。

该自愿性《NIST 隐私框架：通过企业风险管理促进隐私保护》（《隐私框架》）适用于各种规模的组织，不局限于特定的技术、行业、法律或司法管辖区域。框架采用了通用方法（可适应数据处理生态系统中的各种组织角色），旨在帮助组织从如下方面着手管理隐私风险：

- 在设计和部署影响到个人的系统/产品/服务时考虑隐私；
- 宣讲隐私实践；
- 鼓励各类组织人员（例如高管、法务和 IT 人员）在开发 Profile、选择实现层级、实现结果过程中紧密协作。

1.1 隐私框架概述

如图 1 所示，隐私框架由三部分组成：核心、Profile 和实现层级。各组件将业务/任务驱动因素、组织角色及其职责和隐私保护活动关联起来，以此加强隐私风险管理。如第 2 章所述：

图 1：核心、Profile 和实现层级

3 自主权和尊严的概念，见联合国《世界人权宣言》，https://www.un.org/en/universal-declaration-human-rights/。

4 有不少文献对隐私背景或概念的各个方面做过深入研究，例如，Solove D 的《了解隐私》（Understanding Privacy），哈佛大学出版社，马萨诸塞州剑桥，2010 年，https://ssrn.com/abstract=1127888；Selinger E 和 Hartzog W 的《模糊与隐私》（Obscurity and Privacy），未来空间：技术哲学伴侣（Spaces for the Future: A Companion to Philosophy of Technology），编辑 Pitt J 和 Shew A（泰勒-弗朗西斯出版集团，纽约州纽约市），2017 年，第 1 版第 12 章，https://doi.org/10.4324/9780203735657。

- “核心”指一系列的隐私保护活动和结果，通过这个组件，可在整个组织范围内（从管理层到执行/运营层）将划分好优先级的隐私保护活动和结果进行扩散。核心组件的每项功能细分为关键大类和子类，描述的是互无关联的各种结果。
- “Profile”涵盖组织当前的隐私保护活动或期望的结果。要制作 Profile，组织须检视核心组件所涵盖的所有结果和活动，基于业务/任务驱动因素、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，确定其中最需要关注的事项。组织可根据需要创建或添加功能、大类和子类。通过将“当前”Profile（即现状）与“目标”Profile（即未来状况）进行比较，组织可识别机会，改善隐私状况。Profile 适用于自查以及组织内部或组织之间就当前隐私风险管理方法进行沟通。
- “实现层级”（层级）反映了组织对隐私风险的看法以及组织的现有流程和资源是否足以管理隐私风险。层级逐级递升，最低级表示组织对风险只是毫无计划的被动回应，最高级表示组织采用了虑及风险的敏捷方法。在选择层级时，组织应考虑目标 Profile，还要考虑当前风险管理实践、隐私风险融入企业风险管理的程度、数据处理生态系统关系、人力组成以及培训项目是否支持或妨碍实现目标结果。

1.2 隐私风险管理

尽管某些组织对隐私风险管理有透彻理解，但这一领域的许多方面尚未达成普遍共识[5]。为促进更多组织达成共识，本节介绍了组织可用于开发、改进或沟通隐私风险管理的概念和注意事项。有关关键隐私风险管理实践的更多信息，参见附录 D。

1.2.1 网络安全与隐私风险管理

《网络安全框架》自 2014 年发布以来，成为了组织沟通和管理网络安全风险的得力助手[1]。管理网络安全风险有助于管理隐私风险，但这还不够，因为隐私风险或与网络安全事件无关，如图 2 所示。全面了解网络安全风险和隐私风险，明了各自来源，才能选择最有效的风险解决方案。

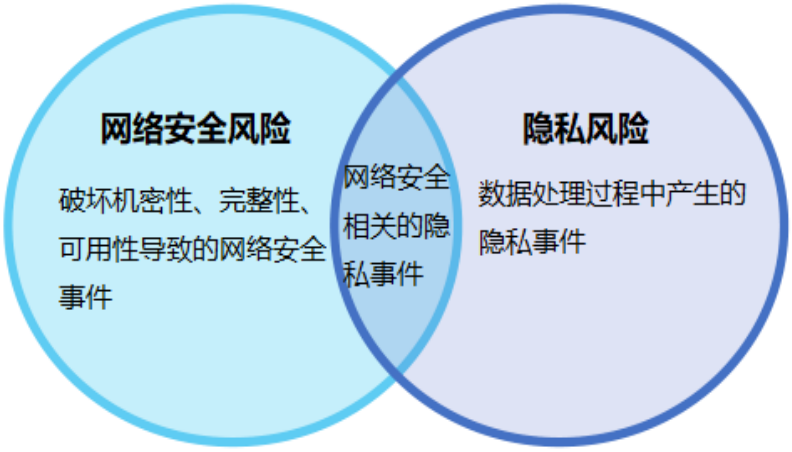

图 2：网络安全风险与隐私风险之间的关系

5 见《对 NIST 隐私框架信息征询结果的简要分析》[2]，第 7 页。

《隐私框架》的隐私风险处理方法考虑的是从数据搜集到废弃的整个生命周期中，个人因系统/产品/服务运营中的数据（数字形式或非数字形式的数据）处理而遭遇隐私事件的可能性。

《隐私框架》同时提到数据操作和数据处理，两者本质上相同。个人在数据处理中遇到的问题有多种分类的方法，NIST 按影响将其划分为几类，轻则影响尊严（如令人难堪或败坏名声），重则造成更明显的危害（如歧视、经济损失或人身伤害）[6]。

数据操作

在数据生命周期内进行的操作，包括但不限于搜集、保留、记录、生成、转换、使用、公开、共享、传输和废弃。

数据处理

一系列数据操作的集合。

个人之所以会遭遇隐私问题，原因不一。如图 2 所示，组织为完成任务/业务目标而进行数据处理时会产生副作用，例如，国家为提高能源效率进行全国性的技术改造，部署智能电网，安装智能电表[7]，而某些人群对此表示不安，因为这些电表会搜集、记录和传送精确的家庭用电信息，让他人窥探自己在家中的行为[8]。智能电表如期推行，却因涉及数据处理让人感到被监视。

在万物互联的今天，有些问题可能仅仅是由于个人与系统/产品/服务的交互所产生，即使所处理的数据与个人并无直接联系。例如，智慧城市技术可用于改变或影响人们的行为，比如在城市中的位置或出行方式[9]。如果在数据处理过程中破坏了保密性、完整性或可用性（外部攻击者窃取数据或员工未经授权访问或使用数据），也会出现问题。这类与网络安全相关的隐私事件是隐私风险和网络安全风险的重叠之处，如图 2 所示。

若能确定数据处理引起特定问题（《隐私框架》将其称为可疑数据操作）的概率，组织就可以评估此类操作的影响。影响评估在隐私风险和组织风险管理中均会涉及。个人—无论是单独一人还是身处集体（包括社会）之中—都会直观感受到这些问题的影响。个人遇到问题时，组织可能会受到波及，承受诸如违规成本、产品/服务客户流失造成的收入减少或外部品牌声誉/内部文化损害等方面的影响。组织通常将这类影响作为企业风险进行管理。通过将个人遭遇的问题与这些易于理解的组织影响联系起来，组织可以像管理风险管理项目中的其他风险一样去管理隐私风险，促进对资源分配进行更明智的决策，推动隐私计划实施。隐私风险和组织风险之间的关系如图 3 所示。

图 3：隐私风险与组织风险之间的关系

6 NIST 编写了一个说明性问题集，用于隐私风险评估，见《NIST 隐私风险评估方法》[3]。有些组织可能有其他分类方法，也有些组织会将这些问题称为不良后果或危害。

7 请参阅 NIST 跨部门或内部报告（IR）7628（修订版 1）第 1 卷《智能电网网络安全指南：第 1 卷–智能电网网络安全战略、架构及概括要求》[4]，第 26 页。

8 请参见 NIST IR 8062《联邦系统中的隐私工程和风险管理介绍》[5]，第 2 页。有关与数据处理不良后果相关的其他类型的隐私风险，请参阅 NIST IR 8062 的附录 E。

9 Newcombe T，智慧城市技术发展过程中的安全、隐私、治理问题，政务技术，2016，http://www.govtech.com/Security-Privacy-Governance-Concerns-About- Smart-City-Technologies-Grow.html。

1.2.2 隐私风险评估

隐私风险管理涉及一系列跨组织流程。通过这些流程，组织可了解其系统/产品/服务为个人带来的问题以及如何开发有效的解决方案来管理此类风险。隐私风险评估是其中的一个子流程，用于识别、评估特定的隐私风险。一般来说，基于隐私风险评估产生的信息，组织可权衡数据处理的好处和风险，按照所谓的“相称性”原则[10]，确定合理的应对措施。组织可根据对个人的潜在影响以及对组织的附带影响确定风险优先级，选择不同的方法应对隐私风险。应对方法包括[11]：

- 缓解风险（例如，组织可对系统/产品/服务采取技术和/或政策措施，将风险降低到可接受的程度）；
- 转移或分担风险（例如，可利用合同将风险分担或转移给其他组织，利用隐私声明和同意机制将风险转嫁给个人）；
- 规避风险（例如，组织在确定风险大于收益时可选择放弃或终止数据处理）；或
- 接受风险（例如，组织认为问题对个人的影响极低或几近于零，因而确定收益大于风险，无需投入资源进行防护）。

如上所述，隐私是维护多项价值的条件，因而隐私风险评估极为重要。维护方法会有所不同，彼此之间可能互相制约。例如，若组织试图通过限制查看来保护隐私，则可能会实施诸如分布式数据架构或增强隐私的加密技术之类的措施，这些措施甚至会对组织隐匿数据。若组织同时想控制个人，则这些措施可能会发生冲突。假设用户请求访问数据，而该数据的分发、加密方式限制组织访问，则组织无法输出所请求的数据。隐私风险评估有助于组织了解特定背景下要保护的价值、采用的方法以及平衡各种措施的实施方式。

最后，隐私风险评估可帮助组织区分隐私风险与合规风险。即使组织完全遵守了适用的法律法规，确定数据处理是否会给个人带来问题也能为系统/产品/服务设计或部署中的道德决策提供支撑。道德决策没有客观标准；它建立在特定社会的规范、价值观和法律期望的基础上。这有助于促进数据的正面使用，同时最大程度地降低对个人隐私和整个社会的不利影响，并避免因信任受损而破坏组织的声誉或使得客户推迟采用或放弃产品/服务。

有关隐私风险评估的操作，参见附录 D。

1.3 章节介绍

本文档其他部分包括：

- **第 2 章：**介绍了隐私框架组件：核心、Profile 和实现层级。
- **第 3 章：**举例说明如何使用隐私框架。
- **参考文件：**列举了本文所参考的文件。
- **附录 A：**用表格形式介绍隐私框架核心：功能、大类和子类。
- **附录 B：**术语表。
- **附录 C：**列举了本文出现的缩略语。
- **附录 D：**介绍可促进隐私风险管理的关键做法。
- **附录 E：**定义了实现层级。

10 欧洲数据保护主管，必要性与相称性，2019，https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en。

11 NIST SP 800-39，管理信息安全风险：组织、任务、信息系统视角[6]

2. 《隐私框架》基本要素

《隐私框架》提供通用语言，方便内外部利益相关者理解、管理、沟通隐私风险，可根据组织在数据处理生态系统中的角色进行修改。它用以确定哪些活动可降低隐私风险并为这些活动定义优先级，还可调整风险管理的政策、业务和技术方法。

2.1 核心

如附录 A 所述，核心组件将各种活动和结果细化，为沟通隐私风险管理提供了通用语言。如图 4 所示，该组件由功能、大类和子类组成。

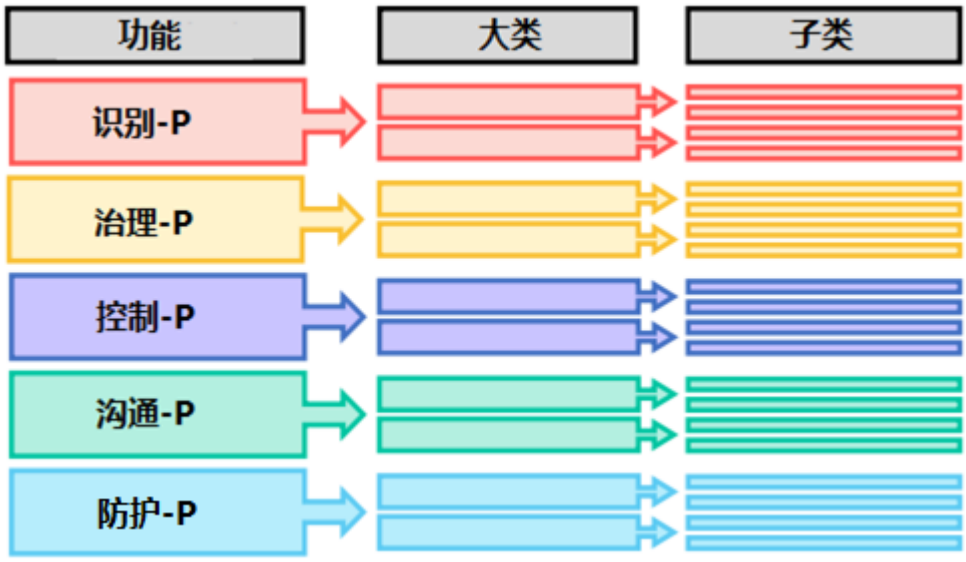

图 4：隐私框架核心结构

核心组件各元素协同工作：

- 功能是对基本隐私活动的最粗略分类，有助于组织了解并管理数据处理，描述隐私风险管理，进而推动风险管理决策，确定如何与个人互动，并且吸取过去的经验教训，吃一堑，长一智。这些功能并不需要一步步顺序执行，也不是为了实现最终的静态目标。实际上，这些功能应同时进行且长期持续，形成有效机制以应对动态的隐私风险。
- 大类是对功能的细分，一个功能会被分为多个隐私结果组（即大类），与计划需求和特定活动密切相关，
- 大类进一步细分为子类，描述具体的技术及/或管理活动结果。这些结果虽然并非巨细无遗，却可支撑各大类结果的实现。

这五大核心功能（定义如下），即识别-P、治理-P、控制-P、沟通-P、防护-P，可用于管理数据处理过程中的隐私风险[12]。防护-P 针对的是网络安全类隐私事件（如隐私泄露）的风险管理。《网络安全框架》覆盖了各种类型的网络安全事件，其中的检测、响应、恢复功能可用于进一步支持网络安全类隐私事件的风险管理。或者，组织可将《网络安全框架》的全部五个功能与识别-P、治理-P、控制-P、沟通-P 结合使用，共同解决隐私和网络安全风险。图 5 使用了 1.2.1 节中的文氏图来演示如何将这两个框架中的功能组合使用，管理隐私和网络安全风险的各个方面。《隐私框架》的五大功能定义如下：

12 功能名称末尾的“-P”表示来自《隐私框架》，以避免与《网络安全框架》中的功能混淆。

- 识别-P – 在全组织范围内达成共识，管理数据处理中的个人隐私风险。
- 识别-P 功能下的活动为有效利用隐私框架奠定了基础。通过记录数据处理环境、了解直接或间接接受组织服务或受其影响的个人的隐私利益、进行风险评估，组织能够认清其所处的业务环境，识别隐私风险并确定优先级。
- 治理-P – 构造并实施组织治理架构，把握组织基于隐私风险确定的风险管理重点事项。
- 治理-P 类似于基础功能，但更侧重于组织级别的活动，例如建立组织范围内的隐私价值和政策、确定法律/法规要求以及了解组织的风险承受能力，使组织能够集中精力，根据风险管理战略和业务需求确定工作重点。
- 控制-P – 合理规划并展开活动，帮助组织或个人以足够细的粒度来管理数据，进而管理隐私风险。
- 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 – 合理规划并展开相应活动，促进组织和个人对数据处理方式和相关隐私风险的理解和沟通。
- 沟通-P 功能强调了这一事实：要有效管理隐私风险，组织和个人均须了解数据的处理方式。
- 防护-P – 制定并实施合理的数据处理防护措施。
- 防护-P 功能涉及数据保护，目的是防止网络安全类隐私事件，这是隐私风险和网络安全风险管理的重叠之处。

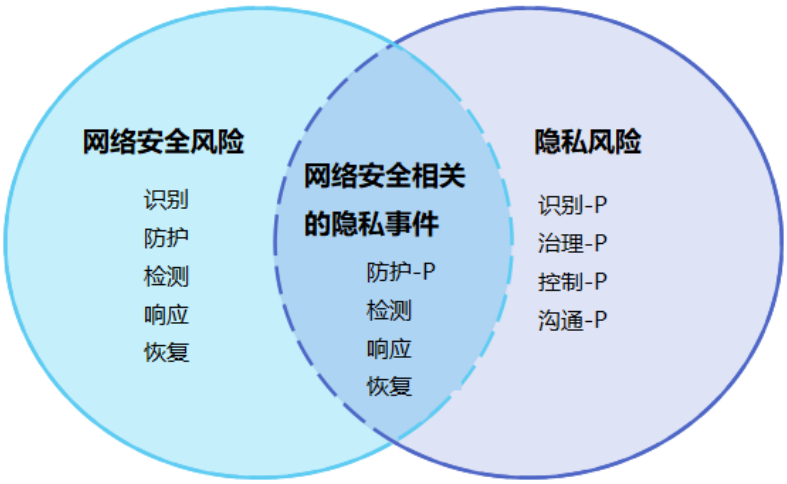

图 5：利用功能管理网络安全风险和隐私风险

2.2 Profiles

Profile 提供了从核心组件中提取的、组织认为在管理隐私风险时须重点考虑的特定功能、大类和子类，用于描述特定隐私活动的当前状态或期望状态。当前 Profile 表示组织当前要实现的隐私结果，而目标 Profile 表示期望实现的隐私风险管理目标结果。通过两者之间的差异，组织能够识别差距，制定改进行动方案并评估实现隐私目标所需的资源（例如人员配置、资金等）。组织基于此制定计划，经济有效地降低隐私风险，并为这些风险确定优先级。Profile 还可以让组织了解、比较隐私结果的当前和期望状态，在组织内部和组织之间进行风险交流。

考虑到实现上的灵活性，《隐私框架》没有提供 Profile 模板。根据《隐私框架》所提出的基于风险的方法，组织并不一定需要实现核心组件所囊括的所有结果或活动。

在开发 Profile 时，组织可根据其特定需求选择或定制功能、大类和子类，也可以根据组织所面临的独特风险，开发其他功能、大类和子类。组织要基于如下因素确定自己的需求：任务/业务目标、隐私价值和风险承受能力；在数据处理生态系统或行业部门中的角色；法律/法规要求和行业最佳实践；风险管理优先事项和资源；直接或间接使用组织的系统/产品/服务或受该系统/产品/服务影响的个人的隐私需求。

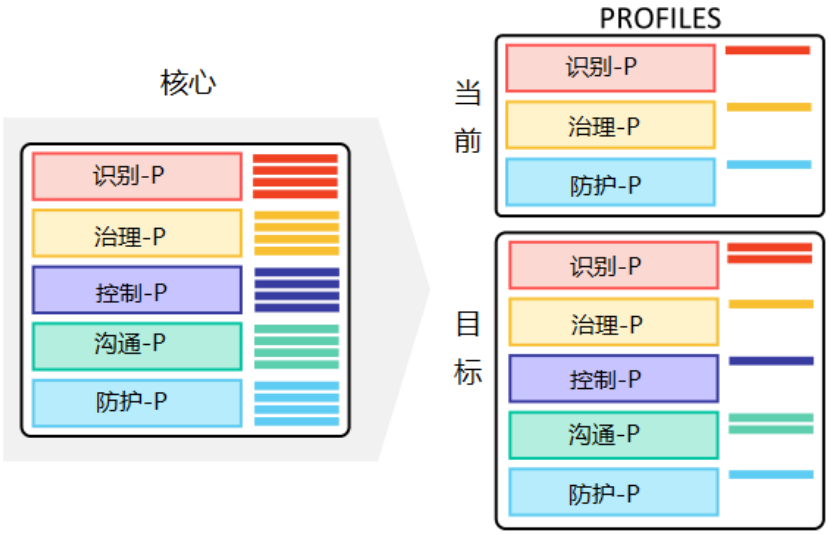

图 6：核心与 Profile 之间的关系

如图 6 所示，开发 Profile 时不用遵循特定的顺序。组织可以首先编写目标 Profile，阐述其对隐私的期望结果，然后编写当前 Profile，确定现状与目标之间的差距。组织也可以先确定当前活动，然后再考虑如何根据目标 Profile 调整这些活动。组织可以为不同的角色、系统/产品/服务或个人类别（例如员工、客户等）开发不同的 Profile，以便根据具体的隐私风险情况为活动和结果确定更合理的优先级。特定行业部门的组织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通用 Profile。

2.3 实现层级

根据组织的系统/产品/服务引起的隐私风险的性质以及组织为管理此类风险而使用的流程和资源的充足性，决定实现层级，为组织的隐私风险管理提供决策支撑。在选择层级时，组织应考虑目标 Profile，还要考虑当前风险管理实践、隐私风险融入企业风险管理的程度、数据处理生态系统关系、人力组成以及培训项目是否支持或妨碍实现目标结果。

有四个不同的层级：局部（1 级）、有风险意识（2 级）、可复用（3 级）和自适应（4 级），具体定义见附录 E。这些层级逐级递进，但并不强制要求全部实现。从 1 级发展到 2 级对组织来说是件好事，但并非所有组织都需要达到 3 级或 4 级，有时可能只需要关注这些层级中的某些方面。

当组织在其当前层级上的流程或资源不足以管理隐私风险时，应向更高层级发展。

在向更高层级发展时，组织可以在内部沟通中使用这些层级概念说明所需的资源。组织也可以用层级作为衡量其隐私风险管理能力发展的总体基准。此外，组织还可以使用层级来揭示数据处理生态系统中其他组织的资源规模和流程。同时，组织所在层级也能反映组织的隐私风险管理优先事项。当然，《隐私框架》是否成功实现取决于目标 Profile 中描述的结果是否达成，而非所定的级别。

3. 如何使用《隐私框架》

当《隐私框架》用作风险管理工具时，可以帮助组织优化数据的有益使用并开发创新的系统/产品/服务，同时最大程度地减少对个人的不利影响。组织可以利用《隐私框架》回答以下基本问题："在开发系统/产品/服务时，如何考虑对个人的影响？"开发《隐私框架》的目的是完善现有的业务和系统开发运营，但考虑到各组织的独特需求，框架可灵活使用，至于如何使用，由各组织自行决定。

例如，某组织已拥有健全的隐私风险管理流程，但可能会使用核心组件的五大功能来分析、阐明差距；打算建立隐私计划的组织可以参考核心组件的大类和子类；有些组织可能会根据数据处理生态系统中的不同角色所要求的风险管理优先级来确定合适的 Profile 或实现层级。组织使用《隐私框架》的方式多种多样，因此，不应将"遵守《隐私框架》"作为统一的或外部参考概念。以下各节介绍了使用《隐私框架》的一些方法。

3.1 引用参考资料

参考资料对应子类，为框架实现提供支持，包括工具、技术指南、标准、法律、法规和最佳实践方面的相关引用。对照表（Crosswalk）将标准、法律和法规的规定与子类对应，帮助组织确定重点活动或结果，以满足合规要求。《隐私框架》遵循技术中立原则，但支持技术创新，任何组织或行业都可以随着技术和相关业务需求的演进而更新对照表。依靠公认的标准、指南和实践，使用可实现积极隐私结果的工具和方法能够跨越国界，适应隐私风险的全球性质。使用现有和新兴标准能够实现规模经济，推动系统/产品/服务满足现有市场需求，同时顾及个人的隐私需求。

若发现参考资料有不足，还可确定应补充或修订哪些标准、指南和实践，以助力组织满足新需求。组织在实现特定的子类或开发新子类时，针对相关活动或结果可能仅有少量的指导材料可用。为解决此问题，组织可与业界技术龙头和/或标准机构合作，起草、开发并协调制定标准、指南或实践。

https://www.nist.gov/privacy-framework 网站上有大量的参考资料，可支持组织使用《隐私框架》优化隐私实践。

3.2 加强问责

问责通常被视为关键的隐私原则，尽管从概念上讲，问责并非隐私所特有[13]。问责在整个组织中无处不在，表达时可抽象为各种说法，例如文化价值、治理政策和程序、隐私要求与控制措施之间的可追溯关系等。隐私风险管理将高管（传达组织的隐私价值和风险承受能力）与业务/流程管理人员（在开发和实施支持组织隐私价值的治理政策和程序方面进行协作）联结起来，为组织各级别的问责提供支持。政策和程序传达给执行/运营人员后，由这些人员合作定义隐私要求，最终在组织的系统/产品/服务中体现。执行/运营人员还要选择、实施和评估满足隐私要求的技术和政策控制措施，上报进度、差距和缺陷以及不断变化的隐私风险，以便业务/流程管理人员和高管了解实情，进行相应响应。

13 例如，经济合作与发展组织（OECD）的《OECD 保护隐私和个人数据的跨境流通指南》（2013），网址为 https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm；国际标准化组织（ISO）/国际电工委员会（IEC）的 ISO/IEC 29100:2011《信息技术–安全技术–隐私框架》（ISO，瑞士日内瓦），网址为 https://standards.iso.org/ittf/PubliclyAvailableStandards/c045123_ISO_IEC_29100_2011.zip；汽车制造商联盟（AAM）和全球汽车制造商协会（AGA）的《消费者隐私保护原则：车辆技术和服务的隐私原则》（2014），网址为 https://autoalliance.org/wpcontent/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services-03-21 -19.pdf。

图 7 展示了这种双向协作和沟通以及如何合入《隐私框架》元素以拉通流程。采用这种操作，组织便可用《隐私框架》支持问责。此外，组织还可将《隐私框架》与提供不同实践的其他框架和指南结合使用，以实现组织内部和组织之间的问责[14]。

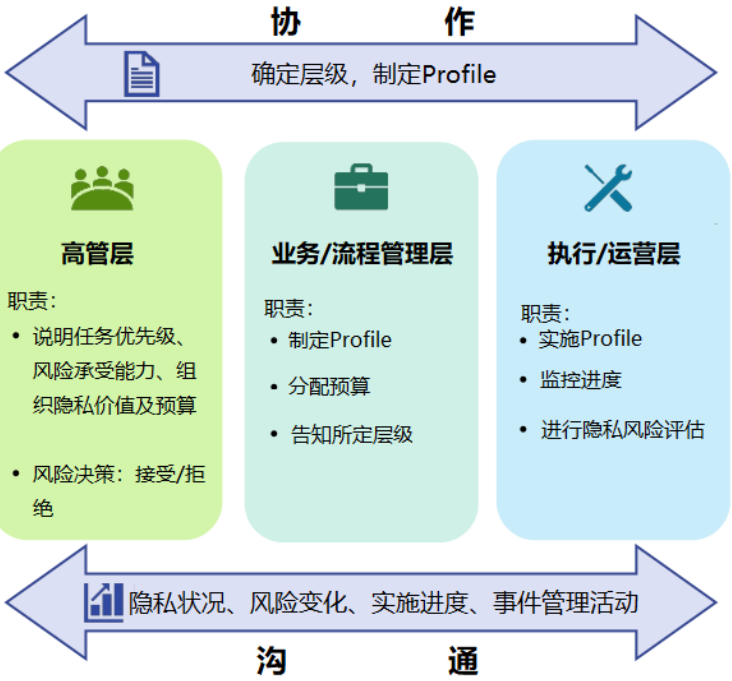

图 7：组织内部协作与沟通概念性流程

3.3 制定/改进隐私计划

《隐私框架》大致划分为“准备、启动、实施”（Ready, Set, Go）三个阶段，可基于此制定或改进隐私计划。在这些阶段，组织可参考相关资料确定优先级、实现结果。有关参考资料的更多信息，见 3.1 节。此外，可访问 https://www.nist.gov/privacy-framework 获取相关资料。

准备

要进行有效的隐私风险管理，组织须了解其业务/任务环境、法律环境、风险承受能力、系统/产品/服务带来的隐私风险以及它在数据处理生态系统中的角色。组织的“准备”工作包括识别-P 和治理-P，具体说，要评估大类和子类，然后撰写当前 Profile 和目标 Profile。[15]建立组织隐私价值和政策、确定并传达组织的风险承受能力、进行隐私风险评估（参见附录 D）等活动和结果为“启动”阶段的 Profile 制定奠定了基础。

制定/改进隐私计划的简化方法

准备：执行识别-P 和治理-P 功能，做好准备。

启动：根据当前 Profile 和目标 Profile 之间的差距，制定行动方案。

实施：着手实施行动方案。

14 例如，NIST SP 800-37（修订版 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]；结构化信息标准促进组织（OASIS）的《隐私管理参考模型和方法（PMRM）》1.0 版，网址为 https://docs.oasis-open.org/pmrm/PMRM/v1.0/PMRMv1.0.pdf。

15 更多信息，参见 NIST SP 800-37（修订版 2）3.1 节的“准备”步骤[7]。

启动

组织创建当前 Profile，明示现阶段要实现其他功能的哪些大类和子类。若某结果已部分达成，会为后续步骤提供基线信息。组织根据实现“识别”和“治理”功能时所输出的信息（如组织隐私价值和政策、组织风险承受能力和隐私风险评估结果等）制定目标 Profile，重点评估大类和子类，阐述组织预期达到的隐私结果。此外，组织还可以开发自己的功能、大类和子类，以应对本组织特有的风险。在制定目标 Profile 时，组织还要考虑外部利益相关者（例如商业客户和合作伙伴）的影响和要求。不同的业务线或流程可能会有不同的业务需求和风险承受能力，因此可开发多个 Profile 进行对应支持。

组织将当前 Profile 和目标 Profile 进行比较，找出差距。接下来，制定优先行动方案，解决差距（阐明任务驱动因素、成本效益和风险），以实现目标 Profile 中列出的结果。组织可同时使用《网络安全框架》和《隐私框架》，制定综合行动方案，然后，确定解决差距所需的资源（包括资金和人力），为之后确定适当的层级提供参考。这样，通过 Profile，组织可对隐私活动作出明智决策，进行风险管理，实现低成本、高效率的针对性改进。

实施

行动方案确定后，要考虑优先采取哪些行动来解决差距，然后调整现有隐私措施，实现目标 Profile[16]。

根据需要，组织可按任意顺序持续评估和改善其隐私状况。例如，有些组织会发现，“准备”阶段反复进行可提升风险评估质量。此外，可通过迭代更新当前 Profile 或目标 Profile 来把控进度，应对不断变化的风险，再将两者进行比较。

3.4 贯穿系统开发生命周期

目标 Profile 可与系统开发生命周期（SDLC）中的各阶段（规划、设计、构建/采购、部署、运行、停用）对齐，支持重点隐私结果的实现[17]。从规划阶段开始，重点隐私结果可转化为系统的隐私功能和对系统的隐私要求，在生命周期的后续阶段，隐私要求可能会发生变化。设计阶段的一个关键里程碑是验证隐私功能和要求是否符合目标 Profile 所描述的组织需求和风险承受能力。在部署系统时，将该目标 Profile 作为内部列表进行评估，以验证是否所有隐私功能和要求均得以实现。接下来，将《隐私框架》确定的隐私结果作为系统持续运行的基础，包括不定期重新评估，核查当前 Profile 所列举结果的实现情况，确保系统始终满足隐私功能和要求。

隐私风险评估通常侧重于数据生命周期，即数据经过的阶段，包括创建/搜集、处理、传播、使用、存储、处置和销毁/删除。欲将 SDLC 与数据生命周期对齐，需要识别和了解数据在 SDLC 各阶段的处理方法。这样，组织才能更好地管理隐私风险，从而对隐私控制措施进行明智选择，有效实施，满足隐私要求。

3.5 在数据处理生态系统中使用

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，角色不仅决定了组织的法律义务，还决定了应该采取什么样的隐私风险管理措施。如图 8 所示，数据处理生态系统包含一系列实体和角色，这些实体和角色彼此之间以及与个人之间具有复杂的多向关系。当实体由一系列子实体支持时，关系就会更为复杂。例如，服务提供商可能由多个其他服务提供商支持，制造商可能拥有多个组件供应商。图 8 中，每类实体被赋予特定角色。实际上，一个实体可能具有多种角色，例

16 NIST SP 800-37[7]就行动方案实施步骤提供了补充信息，包括为弥补差距而进行的控制措施选择、执行与评估。
17 在 SDLC 期间，组织可采用多种开发方法（如瀑布、螺旋、敏捷等）。

如，向其他组织提供服务的同时向消费者提供零售产品。图 8 中的角色只是概念上的分类。实际情况是，实体的角色或有法律定义（例如，有些法律将组织分类为数据控制者或数据处理者），或根据行业进行分类。

图 8：数据处理生态系统关系

实体基于《隐私框架》，根据其角色开发一个或多个 Profile，在管理隐私风险时，不仅要考虑自己的重要事项，还要考虑所采取的措施对数据处理生态系统中其他实体隐私风险管理的影响。例如：

- 在就如何搜集、使用个人数据决策时，组织可以使用 Profile 向外部服务提供商（例如接收组织输出数据的云提供商）传达隐私要求；处理数据的外部服务提供商可以使用 Profile 来证明其履行了合同义务，对数据处理采取了隐私措施。
- 组织可通过当前 Profile 描述其网络安全状态，上报结果数据，与采集需求对齐。
- 行业部门可建立通用 Profile，成员组织可基于此定制自己的 Profile。
- 组织可基于目标 Profile 确定产品内置功能，让业务客户满足其最终用户的隐私要求。
- 开发人员可以基于目标 Profile 设计应用程序，考虑程序在其他组织的系统环境中使用时的隐私保护。
- 《隐私框架》为数据处理生态系统内的各实体沟通隐私要求提供了通用语言。当数据处理生态系统跨越国界（例如国际数据传输）时，这种沟通就显得尤其必要。在进行隐私方面的沟通时，要做到以下几点：
- 确定隐私要求；
- 将隐私要求形成正式协议（例如合同、多方框架等）条文；
- 明确如何验证和确认这些隐私要求；
- 通过各种评估方法来验证是否满足隐私要求；
- 管控上述活动。

3.6 支撑采购决策

当前 Profile 和目标 Profile 均可用于生成组织隐私要求列表（按优先级排序），还可用于支撑产品和服务采购决策。首先选择与隐私目标相关的结果，然后根据这些结果评估合作伙伴的系统/产品/服务。例如，在购买用于森林环境监测的设备时，可管理性很重要，有助于最大程度地减少有关森林使用者的数据处理，所以，要基于核心组件中的相应子类（例如，CT.DP-P4：系统或设备配置允许有选择地搜集或公开数据元素）对制造商进行评估。

若无法对某一供应商强加隐私要求，则应基于周密的隐私要求列表，在多个供应商中做出最优购买决策。通常，这意味着要进行某种程度的取舍，将与 Profile 尚有差距的多个产品、服务进行择优选取。若购买的系统/产品/服务无法完全满足 Profile 中的目标，组织可通过缓解措施或其他管理活动来解决残余风险。

参考资料

[1] 国家标准与技术研究院（2018），提升关键基础设施网络安全框架，1.1 版.（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] 国家标准与技术研究院（2019），对 NIST 隐私框架信息调查结果的简要分析.（国家标准与技术研究院，马里兰州盖瑟斯堡），https://www.nist.gov/sites/default/files/documents/2019/02/27/rfi_response_analysis_privacyframework_2.27.19.pdf

[3] 国家标准与技术研究院（2019），隐私风险评估方法（PRAM）.（国家标准与技术研究院，马里兰州盖瑟斯堡），https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources

[4] 智能电网互通专家组—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、架构及概括要求.（国家标准与技术研究院，马里兰州盖瑟斯堡）. NIST IR 7628，第 1 版，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和风险管理介绍.（国家标准与技术研究院，马里兰州盖瑟斯堡）. NIST IR 8062，https://doi.org/10.6028/NIST.IR.8062

[6] 联合特遣队转型计划（2011），管理信息安全风险：组织、任务、信息系统视角，(国家标准与技术研究院，马里兰州盖瑟斯堡）.NIST SP 800-39，https://doi.org/10.6028/NIST.SP.800-39

[7] 联合特遣队（2018），信息系统与组织风险管理框架：安全与隐私系统生命周期方法.（国家标准与技术研究院，马里兰州盖瑟斯堡）.NIST SP 800-37，修订版 2，https://doi.org/10.6028/NIST.SP.800-37r2

[8] Grassi PA，Garcia ME，Fenton JL（2017），数字身份识别指南.（国家标准与技术研究院，马里兰州盖瑟斯堡）. NIST SP 800-63-3，包括截止 2017 年 12 月 1 日所做的更新，https://csrc.nist.gov/publications/detail/sp/800-63/3/final

[9] 行政管理预算局（OMB）（2017），积极准备，应对个人身份信息泄露，（华盛顿特区白宫）OMB 备忘录 17-12，2017 年 1 月 3 日，https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf

[10] 联合特遣队转型计划（2013），联邦信息系统与组织的安全和隐私控制.（国家标准与技术研究院，马里兰州盖瑟斯堡）.NIST SP 800-53，修订版 4，包括截止到 2015 年 1 月 22 日所做的更新，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：联合属性评估建议方案. (国家标准与技术研究院，马里兰州盖瑟斯堡）.NIST IR 8112，https://doi.org/10.6028/NIST.IR.8112

[12] 联合特遣队转型计划（2012），风险评估指南.(国家标准与技术研究院，马里兰州盖瑟斯堡）.NIST SP 800-30，修订版 1，https://doi.org/10.6028/NIST.SP.800-30r1

[13] 美国法典 44 篇第 3542 节“定义”，2011，https://www.govinfo.gov/app/details/USCODE-2011-title44/USCODE-2011-title44-chap35-subchapIII-sec3542

附录 A：《隐私框架》核心

本附录介绍了框架核心，给出了功能、大类和子类表，该表描述了特定隐私活动和结果，为系统/产品/服务处理数据时的隐私风险管理提供支持。

用户须知：

基于风险的方法：

- **核心组件并非行动列表。组织要根据自己的风险战略选取子类，保护个人隐私。**组织不一定要实现核心中的所有结果或活动。组织在使用 Profile 来选择最能满足其特定需求的功能、大类和子类并划分优先级时须考虑如下因素：自己的目标、在数据处理生态系统或行业中的角色、法律/法规要求和行业最佳实践、风险管理优先事项、直接或间接使用组织的系统/产品/服务或受系统/产品/服务直接或间接影响的个人的隐私需求。
- 无须完整实现各结果。组织可使用 Profile 来描述结果的局部实现情况，因为管理隐私风险时不一定会涉及结果的各个方面。组织可以在目标 Profile 中明示其目前尚无能力实现的某一方面结果。
- 必要时，要综合考虑多种结果，以妥善管理隐私风险。例如，需要响应个人数据访问请求的组织可以为 Profile 选择子类 CT.DM-P1：“可访问并查看数据元素”和大类“身份管理、认证和访问控制”（PR.AC-P），以确保只有与数据相关的个人才能访问。

实施：

核心部分采用了表格形式，功能、大类和子类在表格中的顺序与重要性无关，使用者也不必按顺序实施。根据所处 SDLC 阶段、隐私计划状态、人力规模、组织在数据处理生态系统中的角色，组织可灵活变动各功能、大类和子类的实施顺序，亦可同时实施多个功能、大类和子类或反复实施某一功能、大类和子类。此外，核心部分并未囊括所有功能，可以对其进行扩展，允许组织、部门等实体在 Profile 中修改或添加其他功能、大类和子类。

角色：

- **生态系统角色：**任何组织或实体，无论其在数据处理生态系统中的角色如何，均可使用核心组件。尽管《隐私框架》未对生态系统角色进行分类，但组织应根据其在生态系统中的定位来评审核心内容。实际情况是，组织的角色或有法律定义（例如，有些法律将组织分类为数据控制者或数据处理者），或根据行业进行分类。因为核心组件元素未按生态系统角色进行分类，组织可选择与其角色相关的功能、大类和子类，制定自己的 Profile。
- **组织角色：**组织内不同部门的员工可负责不同的大类或子类。例如，法务部门负责执行“治理政策、流程和程序”下的活动，而 IT 部门则负责“盘点与绘图”。理想的核心组件能促进跨组织合作开发 Profile，达成结果。

可扩展性：

某些结果可能措辞含糊，例如，可能包括诸如“传达”或“公开”之类的词汇，却没有说明向谁传达或公开。这种模糊处理是有意为之，允许不同组织根据实际情况因地制宜。

资源库：关于如何划分优先级、实现结果，可参考 https://www.nist.gov/privacy-framework 网站提供的相关资源。

对齐网络安全框架：

- 如 2.1 节所述，组织可以使用《隐私框架》的五大功能（识别-P、治理-P、控制-P、沟通-P 和防护-P-来管理数据处理过程中产生的隐私风险。防护-P 针对的是安全类隐私事件（如隐私泄露）的风险管理。为了进一步支持安全类隐私事件的风险管理，组织可以选用《网络安全框架》中的检测、响应和恢复功能。由于这个原因，表 1 中列举了这些功能，用灰色显示。组织还可以将《网络安全框架》中的功能与识别-P、治理-P、控制-P 和沟通-P 结合使用，同时应对隐私和安全风险。如图 5 所示，这两个框架中的功能可以以各种方式组合使用，管理隐私和网络安全风险的不同方面。
- 某些功能、大类、子类与《网络安全框架》相同或在后者基础上修改，表 2 使用下面的图例标示这种关系。有关两个框架之间的完整对比，可参考 https://www.nist.gov/privacy-framework 网站的资源库。

功能、大类、子类与《网络安全框架》一致，但文字针对《隐私框架》做了修改。

大类、子类与《网络安全框架》相同。

核心标识符：

为方便使用，框架核心各组件具有唯一 ID。各功能和大类的唯一 ID 由字母构成，如表 1 所示。子类 ID 在对应大类 ID 后加上数字，如表 2 所示。

功能ID	功能	大类ID	大类
ID-P	识别-P	ID.IM-P	盘点与绘图
		ID.BE-P	业务环境
		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	风险管理战略
		GV.AT-P	意识与培训
		GV.MT-P	监控与评审
CT-P	控制-P	CT.PO-P	数据保护政策、流程和程序
		CT.DM-P	数据处理管理
		CT.DP-P	隔离处理
CM-P	沟通-P	CM.PO-P	沟通政策、流程和程序
		CM.AW-P	数据处理安全意识
PR-P	防护-P	PR.PO-P	数据保护政策、流程和程序
		PR.AC-P	身份管理、认证与访问控制
		PR.DS-P	数据安全
		PR.MA-P	维护
		PR.PT-P	防护技术
DE	检测	DE.AE	异常与事件
		DE.CM	持续性安全监控
		DE.DP	检测流程

	RS	响应	RS.RP	响应计划
			RS.CO	沟通
			RS.AN	分析
			RS.MI	缓解
			RS.IM	改进
	RC	恢复	RC.RP	恢复计划
			RC.IM	改进
			RC.CO	沟通

表 1：隐私框架功能和大类唯一标识符

	功能	大类	子类
	识别-P（ID-P）在全组织范围内达成共识，管理数据处理中的个人隐私风险。	**编目与绘图（ID.IM-P）**：了解系统/产品/服务的数据处理流程，促进隐私风险管理。	**ID.IM-P1：**对处理数据的系统/产品/服务进行盘点。
			ID.IM-P2：对所有人/运营方（如组织或第三方，包括服务提供方、合作伙伴、客户和开发者）及其处理数据的系统/产品/服务和组件（包括内外部）进行盘点。
			ID.IM-P3：个人数据被处理时，对个人所属大类（如客户、员工或准员工、消费者等）进行盘点。
			ID.IM-P4：对系统/产品/服务的数据操作进行盘点。
			ID.IM-P5：对数据操作目的进行盘点。
			ID.IM-P6：对数据操作涉及的数据元素进行盘点。
			ID.IM-P7：标识数据处理环境（如地理位置、内部、云、第三方等）。
			ID.IM-P8：对数据处理进行绘图，示意系统/产品/服务中的数据操作和相关数据元素，包括组件、组件所有人/运营方角色以及个人或第三方与系统/产品/服务的交互。
		业务环境（ID.BE-P）：了解组织的任务、目标、利益相关者和活动，并对其进行优先级排序。在此基础上，定义隐私角色和职责，对风险管理进行决策。	**ID.BE-P1：**确定组织在数据处理生态系统中的角色并进行通告。
			ID.BE-P2：确定组织任务、目标和活动的优先顺序并进行通告。
			ID.BE-P3：确定哪些系统/产品/服务可支持组织优先事项，输出关键要求。
		风险评估（ID.RA-P）：组织了解个人隐私风险以及此类风险对组织运营（包括任务）、职能、其他风险管理优先事项（如合规和财务）、声誉、人力及文化的后续影响。	**ID.RA-P1：**识别与系统/产品/服务和数据操作相关的环境因素（例如，人群构成、个人隐私权益、个人对隐私的看法、数据敏感性及/或类型、数据处理过程对个人和第三方的可见性）。
			ID.RA-P2：甄别数据分析输入和输出，评估是否存在偏差。
			ID.RA-P3：识别潜在可疑数据操作及相关问题。
			ID.RA-P4：基于可疑数据操作、可能性和影响来确定风险并为其划分优先级。
			ID.RA-P5：确定风险响应动作，为其划分优先级，进行风险响应。
		数据处理生态系统风险管理（ID.DE-P）：确定组织的重点事项、制约因素、风险承受能力和假设，用于支撑与隐私风险管理和数据处理生态系统内第三方相关的决策。组织建立、执行流程以识别、评估和管理数据处理生态系统内的隐私风险。	**ID.DE-P1：**确定、建立、评估、管理数据处理生态系统风险管理政策、流程和程序，并取得组织利益相关者的许可。
			ID.DE-P2：采用隐私风险评估流程，确定、评估数据处理生态系统相关各方（如服务提供商、客户、合作伙伴、产品制造商、应用开发商等）并为其分配优先级。
			ID.DE-P3：与数据处理生态系统相关各方签订合同，采用合理措施，实现组织隐私计划目标。
			ID.DE-P4：采用互通框架或类似多方方案管理数据处理生态系统隐私风险。
			ID.DE-P5：利用审计、测试或其他审核方式定期评估数据处理生态系统相关各方，确保他们履行合约、互通框架等义务。

功能	大类	子类
治理-P（GV-P）构造并实施组织治理架构，时刻了解组织基于隐私风险确定的风险管理重点事项。	**治理政策、流程和程序（GV.PO-P）：** 了解用于管理和监控组织的法律法规、风险、环境和运营要求的政策、流程和程序，支撑隐私风险管理。	**GV.PO-P1：**确定组织的隐私价值和政策（如数据处理条件（数据使用、保留期限等）和个人的数据处理权限）并进行通告。
		GV.PO-P2：建立并落实流程，将组织的隐私价值注入系统/产品/服务开发和运营过程。
		GV.PO-P3：新建隐私相关角色并分配职责。
		GV.PO-P4：协调隐私角色与职责，将其与第三方利益相关者（如服务提供商、客户、合作伙伴等）对齐。
		GV.PO-P5：了解并管理与隐私相关的法律法规与合同要求。
		GV.PO-P6：采用治理及风险管理政策、流程和程序应对隐私风险。
	风险管理战略（GV.RM-P）： 确定组织的各种优先事项、约束、风险承受能力和假设，为运营风险决策提供支持。	**GV.RM-P1：**建立并管理风险管理流程，并征得组织利益相关者的同意。
		GV.RM-P2：确定并清晰阐述组织的风险承受能力。
		GV.RM-P3：组织根据自己在数据处理生态系统中的角色确定风险承受能力。
	意识培养与培训（GV.AT-P）： 为从事数据处理的组织人员与第三方提供隐私意识教育与培训，确保这些人群按照相关政策、流程、程序、协议与组织的隐私价值履行隐私义务与职责。	**GV.AT-P1：**让员工了解其角色和职责并接受相关培训。
		GV.AT-P2：高管了解自己的角色和职责。
		GV.AT-P3：隐私人员了解自己的角色和职责。
		GV.AT-P4：第三方（如服务提供商、客户、合伙伙伴等）了解自己的角色和职责。
	监控与评审（GV.MT-P）： 了解组织就隐私状况所采取的持续评审政策、流程和程序，支持隐私风险管理。	**GV.MT-P1：**定期复审隐私风险，重点关注下列各项：组织的业务环境（如引入新技术）、治理（如法律义务、风险承受能力）、数据处理和系统/产品/服务变化。
		GV.MT-P2：评审隐私价值、政策和培训，如有更新，及时通告。
		GV.MT-P3：建立并落实法律及隐私政策合规评审政策、流程和程序。
		GV.MT-P4：建立并落实隐私风险管理进度沟通政策、流程和程序。
		GV.MT-P5：建立并落实政策、流程和程序，以接收、分析并响应组织发现的内外部来源（内部发现、隐私研究人员等）的可疑数据操作。
		GV.MT-P6：政策、流程和程序中合入可疑数据操作相关的经验教训。
		GV.MT-P7：建立并落实政策、流程和程序，以接收、追踪和响应个人就组织隐私做法而提出的投诉、疑问与关注问题。

功能	大类	子类
控制-P（CT-P）合理规划并展开活动，帮助组织或个人以足够细的粒度来管理数据，进而管理隐私风险。	**数据处理政策、流程和程序（CT.PO-P）：** 依照组织的风险战略，维护并执行政策、流程和程序，对数据处理进行管理（如目的、范围、在数据处理生态系统中的角色和职责、管理承诺等），保护个人隐私。	**CT.PO-P1：**建立并落实数据处理授权（如组织决策、个人同意等）、取消授权、维护授权政策、流程和程序。
		CT.PO-P2：建立并落实数据评审、传送、共享/公布、修改和删除政策、流程和程序（如保证数据质量、管理数据保留问题等）。
		CT.PO-P3：建立并落实政策、流程和程序，以支持个人的数据处理偏好和请求。
		CT.PO-P4：根据系统开发生命周期，调整、实施数据的生命周期管理，完善系统管理。
	数据处理管理（CT.DM-P）： 根据组织的风险战略管理数据，保护个人隐私，提高可管理性，确保隐私原则得以执行（如个人参与度、数据质量、数据最小化等）。	**CT.DM-P1：**允许访问并查看数据元素。
		CT.DM-P2：允许访问并传输/公开数据元素。
		CT.DM-P3：允许访问并修改数据元素。
		CT.DM-P4：允许访问并删除数据元素。
		CT.DM-P5：根据政策销毁数据。
		CT.DM-P6：用标准格式传输数据。
		CT.DM-P7：建立并落实机制，确保处理权限及相关数据值和数据元素一同传输。
		CT.DM-P8：根据政策并结合数据最小化原则，控制、记载、实施并审核审计/日志记录。
		CT.DM-P9：测试、评估用以管理数据处理的技术措施。
		CT.DM-P10：在算法设计目标中考虑利益相关者的隐私偏好，根据这些偏好评估输出。
	隔离处理（CT.DP-P）： 根据组织的风险战略，使用数据处理方案提升隔离性，保护个人隐私，执行隐私原则（如数据最小化）。	**CT.DP-P1：**处理数据时，限制数据的可见性或链接（例如，在本地设备上操作数据、采用密码保护隐私等）。
		CT.DP-P2：处理数据时，限制个人标识（如差分隐私技术、令牌化等）。
		CT.DP-P3：处理数据时，限制对个人行为或活动的推导（如分散型数据处理、分布式结构等）。
		CT.DP-P4：配置系统或设备允许选择性收集/公布数据元素。
		CT.DP-P5：用属性引用代替属性值。

	功能	大类	子类
	沟通-P（CM-P）合理规划并展开活动，促进组织和个人准确理解并沟通数据处理过程及其相关隐私风险。	**沟通政策、流程和程序（CM.PO-P）：**维护并执行政策、流程和程序，提升组织的数据处理实践（如目的、范围、在数据处理生态系统中的角色和职责、管理承诺等）以及相关隐私风险的透明度。	**CM.PO-P1：**建立并落实透明度政策、流程和程序，以沟通数据处理目的、实践和相关隐私风险。
			CM.PO-P2：建立角色，分配职责（如公关），传达数据处理目的、实践和相关隐私风险。
		数据处理安全意识（CM.AW-P）：个人和组织对数据处理实践和相关隐私风险有准确了解；根据组织的风险战略，使用并维护有效机制，提升可预测性，保护个人隐私。	**CM.AW-P1：**建立并落实机制（如通知、内部或公开报告），传达数据处理目的、实践、相关隐私风险和方案，支持个人的数据处理偏好和请求。
			CM.AW-P2：建立并落实机制，获取个人对于数据处理和相关隐私风险的反馈（如调查或焦点小组（Focus Group））。
			CM.AW-P3：系统/产品/服务设计有助于提升数据处理透明度。
			CM.AW-P4：维护数据披露与共享记录，允许访问并查看或传输/公开这些记录。
			CM.AW-P5：可通知数据处理生态系统中的个人或组织（如数据源）数据已修改或删除。
			CM.AW-P6：维护数据来源与沿袭，允许访问并查看或传输/公开这些记录。
			CM.AW-P7：发生隐私泄露或事件时，通知受影响个人和组织。
			CM.AW-P8：为个人提供缓解机制（如信用监控、批准撤销、数据修改或删除等），减轻数据处理对个人的影响。

	功能	大类	子类
	防护-P（PR-P）制定并实施合理的数据处理防护措施。	**数据保护政策、流程和程序（PR.PO-P）：**维护安全和隐私政策（涉及目的、范围、数据处理生态系统中的角色和职责、管理承诺等）、流程和程序，保护数据。	**PR.PO-P1：**结合安全原则（如“最小功能”概念），建立、维护信息技术的配置基线。
			PR.PO-P2：建立并落实配置更改控制流程。
			PR.PO-P3：备份信息，并对此种备份进行维护、测试。
			PR.PO-P4：遵守组织资产物理运营环境的相关政策和规定。
			PR.PO-P5：改进防护流程。
			PR.PO-P6：共享有效的防护技术。
			PR.PO-P7：建立、落实、管理响应计划（事件响应和业务连续性）和恢复计划（事件恢复和灾难恢复）。
			PR-PO-P8：测试响应和恢复计划。
			PR.PO-P9：将隐私步骤纳入人力资源实践中（如取消访问权限、人员筛选等）
			PR.PO-P10：制定、实施漏洞管理计划。
		身份管理、认证与访问控制（PR.AC-P）：仅允许授权个人、流程和设备访问数据和设备，根据未授权访问风险评估结果对访问进行管控。	**PR.AC-P1：**为授权个人、流程和设备下发、管理、验证、撤销并审计身份与凭证。
			PR.AC-P2：管理对数据和设备的物理访问。
			PR.AC-P3：管理远程访问。
			PR.AC-P4：结合最小特权和职责分离原则，管理访问权限和授权。
			PR.AC-P5：保护网络完整性（如网络隔离、网络分段等）。
			PR.AC-P6：对个人和设备进行验证并绑定凭证，并根据交易风险（例如个人的安全和隐私风险以及其他组织风险）进行身份认证。
		数据安全（PR.DS-P）：根据组织的风险战略管理数据，保护个人隐私，维护数据的机密性、完整性和可用性。	**PR.DS-P1：**保护静态数据。
			PR.DS-P2：保护传输数据。
			PR.DS-P3：在删除、传输和处置的整个过程中，对系统/产品/服务和相关数据进行正式管理。
			PR.DS-P4：保持足够空间，确保可用性。
			PR.DS-P5：实施保护措施，防止数据泄露。
			PR.DS-P6：采用完整性检查机制验证软件、固件和信息的完整性。
			PR.DS-P7：将开发测试环境与生产环境隔离。
			PR.DS-P8：采用完整性检查机制验证硬件完整性。
		维护（PR.MA-P）：根据政策、流程和程序维护、修复系统。	**PR.MA-P1：**用经过批准的受控工具对组织资产进行维护和修复并作相关记录。
			PR.MA-P2：对组织资产进行远程维护时须经过批准、记录，以防止未授权访问。
		防护技术（PR.PT-P）：依照相关政策、流程、程序和协议，管理技术安全方案，确保系统/产品/服务以及相关数据的安全性和恢复能力。	**PR.PT-P1：**根据策略，保护和限制使用移动媒体。
			PR.PT-P2：采用“最小功能”原则，配置系统只提供最基本功能。
			PR.PT-P3：保护通信与控制网络。
			PR.PT-P4：建立各种机制（如故障保护、负载均衡、热切换等），确保在正常、异常情况下均能满足恢复要求。

表 2：《隐私框架》核心

附录 B 学术表

附录对文中出现的部分术语进行了定义。

属性引用 （NIST SP 800-63-3[8]）	用户属性陈述，不一定包含身份信息，且不受格式限制。例如，对于属性“生日”，引用可以是“18 岁以上”或“12 月出生”。
属性值 （NIST SP 800-63-3[8]）	对用户属性的完整陈述，不受格式限制。例如，对于属性“生日”，值可以是“12/1/1980”或“1980 年 12 月 1 日”。
可用性 （44 U.S.C.[13]）	确保可及时、可靠地访问并使用信息。
大类	与计划性需求和特定活动紧密相关的、某一功能下的隐私结果组。
沟通-P（功能）	合理规划并展开活动，促进组织和个人对数据处理方式和相关隐私风险的理解和沟通。
机密性 （44 U.S.C.[13]）	通过授权，限制信息访问及披露，包括个人隐私与私有信息保护方法。
控制-P（功能）	合理规划并展开活动，帮助组织或个人以足够细的粒度来管理数据，进而管理隐私风险。
核心	隐私保护活动和结果的集合。框架核心组件包含三个要素：功能、大类和子类。
网络安全事件 （提升关键基础设施的网络安全框架[1]） （OMB 17-12[9]）	确认对组织造成影响、需要响应恢复的与网络安全相关的事件。 以下两种情况构成网络安全事件：（1）未经合法授权、确已或即将危害信息或信息系统的完整性、机密性或可用性；（2）违反或即将违反法律、安全政策、安全程序或可接受使用政策。
数据	对信息的数字和非数字形式的表示。
数据操作 （基于 NIST IR 8062[5]修改）	在系统/产品/服务的整个数据生命周期内进行的操作，包括但不限于搜集、保留、记录、生成、转换、使用、公开、共享、传输和处置。
数据元素	传达有意义信息的最小的命名数据项。
数据处理 （基于 NIST IR 8062[5]修改）	数据操作集合，即完整数据生命周期，包括但不限于搜集、保留、记录、生成、转换、使用、公开、共享、传输和处置。
数据处理生态系统	创建或部署系统/产品/服务或任何数据处理组件时所涉及到的实体间的复杂互联关系。
隔离 （基于 NIST IR 8062[5]修改）	保证处理数据或事件时不涉及与系统操作无关的个人或设备。
功能	核心组件的构成元素，是基本隐私活动的最粗略分类，可进一步分为大类和子类。
治理-P（功能）	构造并实施组织治理架构，保持对基于隐私风险所确定的组织的重点风险管理事项深度了解。
识别-P（功能）	在全组织范围内达成共识，管理数据处理中的个人隐私风险。
实现层级	为组织评估隐私风险以及组织的流程和资源是否足以管理隐私风险提供参考依据。
个人	一个人或一群人，包括社会层面含义。
完整性 （44 U.S.C.[13]）	防止信息被不当修改或破坏，包括保证信息的抗抵赖性与真实性。
沿袭	数据元素的处理历史，其中或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 （基于 NIST IR 8062[5]修改）	提供数据精细管理功能，包括更改、删除和选择性公开。
元数据 （基于 NIST SP 800-53[10]修改）	描述数据特征的信息，有各种分类，例如描述数据结构的结构元数据（即数据格式、语法和语义）和描述数据内容的描述性元数据。
可预测性 （基于 NIST IR 8062[5]修改）	支持个人、所有人和运营方对数据以及系统/产品/服务处理数据的可靠假设。
隐私泄露 （基于 OMB M-17-12[9]修改）	对数据失去控制或数据遭入侵、非法披露或获取，或存在下述情况：（1）非授权用户访问或有可能访问数据，或（2）授权用户为非授权目的访问数据。
隐私控制 （基于 NIST SP 800-37[7]修改）	组织内部为满足隐私要求而采取的管理、技术和物理防护措施。
隐私事件	出现或可能出现可疑数据操作。
隐私要求	对于系统/产品/服务功能的规范要求，目的是达成利益相关者期望的隐私结果。
隐私风险	个人遭遇数据处理引起的问题的可能性以及此类问题（若有）的影响。
隐私风险评估	隐私风险管理子流程，用于识别、评估、响应特定的隐私风险并为其划分优先级。
隐私风险管理	用以识别、评估和响应隐私风险的跨组织流程集合。
可疑数据操作 （基于 NIST IR 8062[5]修改）	可对个人造成负面影响的数据操作。
处理	见“数据操作”。
Profile	从核心组件中提取的、组织认为在管理隐私风险时须重点考虑的特定功能、大类和子类。
防护-P（功能）	制定并实施合理的数据处理防护措施。
来源 （基于 NIST IR 8112[11]修改）	与特定数据的源头或来源有关的元数据。
风险 （NIST SP 800-30[12]）	衡量实体受到潜在情况或事件威胁的程度，衡量因素包括：（i）若情况或事件发生，将会产生多大的不利影响；（ii）发生的可能性。
风险管理	对风险进行识别、评估和响应的过程。
风险承受能力 （NIST SP 800-39[6]）	组织可接受的风险级别或不确定性。
子类	对大类的细分，表示具体的技术及/或管理活动结果。

附录 C 缩略词

IEC	International Electrotechnical Commission	国际电工委员会
IR	Interagency or Internal Report	跨部门或内部报告
ISO	International Organization for Standardization	国际标准化组织
IT	Information Technology	信息技术
NIST	National Institute of Standards and Technology	国家标准与技术研究院
OASIS	Organization for the Advancement of Structured Information Standards	结构化信息标准促进组织
OECD	Organisation for Economic Co-operation and Development	经济合作与发展组织
OMB	Office of Management and Budget	行政管理预算局
PMRM	Privacy Management Reference Model and Methodology	隐私管理参考模型和方法
PRAM	Privacy Risk Assessment Methodology	隐私风险评估方法
RFC	Request for Comment	意见征求
RFI	Request for Information	信息征询
SDLC	System Development Life Cycle	系统开发生命周期
SP	Special Publication	特别刊物

附录 D 隐私风险管理实践

1.2 节介绍了隐私风险管理中的诸多考虑事项，包括网络安全和隐私风险之间的关系以及隐私风险评估的作用。本附录针对的是可促进有效隐私风险管理的一些关键实践，包括筹措资源、确定隐私功能、定义隐私要求、评估隐私风险、实现隐私要求的可追溯性以及监控不断变化的隐私风险等。为方便使用核心组件来支持这些实践，加入了大类和子类引用（放在括号中）。

筹措资源

合理配置资源后，组织内各级部门方可就隐私风险做出明智决策。实际操作中，各类资源的开发可能会由组织内部的不同部门负责。因此，依赖于某些资源的部门可能会发现资源缺失或不足以解决隐私问题。这种情况发生时，该部门可针对资源用途，通过其他途径查找信息或利用手头信息做出最优决策。简而言之，有充足的资源固然是好，资源不足，部门也应该做出其能力范围之内的最佳风险决策。

部分隐私管理资源列举如下。基于这些资源，组织可做出更合理的决策。

- **风险管理角色分配（GV.PO-P3, GV.PO-P4）**

  要更好地协调决策，使决策有据可依，跨组织了解组织内隐私风险管理及其他风险管理任务的责任人非常重要。此外，多角度审视问题能够优化隐私风险的识别、评估和响应流程。跨部门的多元化团队有助于更全面地识别个人隐私风险，选择更多样的缓解措施。确定参与风险管理沟通的角色时须考虑组织的背景和构成，当然，组织的隐私和网络安全计划之间的协作也很重要。如果为一个人分配多种角色，则应考虑如何管理潜在的利益冲突。

- **企业风险管理战略(GV.RM-P)：**

  组织的企业风险管理战略旨在将组织的使命和价值与组织的风险承受能力、假设、约束和重要事项对齐。在实现任务/业务目标的同时还要管理多种风险，资源受限，这时可能需要权衡取舍。让隐私风险管理人员了解组织的风险承受能力，有助于引导资源分配决策，优化风险响应决策。

- **关键利益相关者（GV.PO-P4，ID.DE-P）**

  隐私利益相关者关注系统/产品/服务的隐私结果或与之有利益瓜葛。例如，对法律方面的关注可能集中在系统/产品/服务的运行方式是否会导致组织违反隐私法律法规或其业务协议上；追求最大化使用率的企业负责人可能会担心隐私保护不足而导致客户对系统/产品/服务失去信任。处理个人数据或个人与系统/产品/服务交互时，个人希望的是避免遇到问题或不良后果。了解利益相关者及其关注的隐私结果类型有助于合理设计系统/产品/服务，满足利益相关者的要求。

- **组织层面的隐私要求（GV.PO-P）**

  组织层面的隐私要求指组织要遵守的法律义务、隐私价值和政策。了解这些要求是确保系统/产品/服务设计符合组织义务的关键。组织层面的隐私要求来自多个方面，包括：

  - 法律环境（如法律法规、合同等）
  - 组织政策或文化价值
  - 相关标准
  - 隐私原则

- **系统/产品/服务设计工件（ID.BE-P3）**

  设计工件多种多样，例如系统设计架构或数据流程图。使用这些工件，组织可了解自己的系统/产品/服务的运作方式。因此，隐私计划中可采用这些工件，促进了解系统/产品/服务的工作机制，方便选择、实施控制方法或措施，辅助缓解隐私风险，在维持功能性的同时保护隐私。

- **数据图（ID.IM-P）**

  数据图用以展示数据处理过程以及个人与系统/产品/服务的交互，不仅包括数据处理环境，还包括数据处理组件或与个人交互的组件、组件的所有者或运营方、不连续数据操作以及处理中的特定数据元素。数据图形式多样，视组织需求提供不同程度的细节信息。它可置于现有系统/产品/服务设计工件之上，方便、简化组织部门之间沟通。如下所述，数据图是隐私风险评估中的重要工具。

选用隐私功能

隐私功能用于描述实现目标隐私结果的系统/产品/服务属性或功能（例如，“该服务可最小化数据”）。为系统/产品/服务设计安全功能时，可同时参考安全目标（机密性、完整性和可用性）和安全要求。表 3 列举了隐私工程目标，为隐私功能选用提供支持。组织可基于这些隐私工程目标对功能进行粗略划分。若系统/产品/服务的可预测性、可管理性或隔离性较低，可能说明隐私风险较高，须进行更全面的隐私风险评估。

选用隐私能力时，组织会考虑哪些隐私工程和安全目标对其任务/业务需求、风险承受能力和组织层面的隐私要求最为重要（见上文的“筹措资源”）。各目标并非同等重要，可能需要取舍。隐私功能支持风险优先级决策，为隐私风险评估提供支撑。另一方面，隐私功能亦可基于风险评估进行相应调整，为特定隐私风险的管理提供支持或应对环境中的变化（包括系统/产品/服务设计更改）。

	目标	定义	《隐私框架》核心 主要相关功能
隐私工程目标	可预测性	支持个人、所有人和运营方对数据以及系统处理数据的可靠假设。	识别-P、治理-P、控制-P、沟通-P、防护-P
	可管理性	提供数据精细管理功能，包括搜集、更改、删除和选择性公开。	识别-P、治理-P、控制-P
	隔离性	保证处理数据或事件时不涉及与系统操作无关的个人或设备。	识别-P、治理-P、控制-P
安全目标	机密性	通过授权，限制信息访问及披露，包括对个人隐私与私有信息的保护。	识别-P、治理-P、防护-P
	完整性	防止不当信息更改或破坏，包括保证信息的抗抵赖性与真实性。	识别-P、治理-P、防护-P
	可用性	确保可及时、可靠地访问并使用信息。	识别-P、治理-P、防护-P

明确隐私要求

隐私要求对系统/产品/服务的功能运作方式作了规定，以满足利益相关者期望的隐私结果（例如，“应用程序应允许用户选择特定数据元素”）。要定义隐私要求，须考虑组织层面的隐私要求（见上文“筹措资源”）和隐私风险评估输出。这一过程可帮助组织回答以下两个问题：系统/产品/服务在数据处理和与个人的交互中（1）能够做什么以及（2）应该做什么。接下来，组织分配资源，按照明确要求，设计系统/产品/服务。最终，基于明智的风险决策进行开发，在系统/产品/服务中加强个人隐私保护。

进行隐私风险评估

进行隐私风险评估有助于组织识别系统/产品/服务中的隐私风险，对隐私进行优先级排序，最终就如何应对风险做出明智决策（ID.RA-P，GV.RM-P ）。隐私风险评估方法纵有不同，组织在选取方法时的考虑因素却大同小异[18]：

- **风险模型（ID.RA-P，GV.MT-P1）**

  风险模型定义了须评估的风险因素以及这些因素之间的关系[19]。若组织没有预定义的风险模型，则应明确定义欲评估的风险因素以及这些因素之间的关系。网络安全有基于威胁、漏洞、可能性和影响等风险因素的风险模型，且这种模型广泛使用，而隐私风险却缺乏这样一种公认的模型。NIST 的隐私风险模型计算风险的公式是：风险 = 可疑数据操作的可能性 X 可疑数据操作的影响。下面逐一介绍这些风险因素。

NIST 隐私风险因素：

可疑数据操作|可能性|影响

  - 可疑数据操作指系统处理数据时可能为个人带来问题的任何操作。组织要考虑与特定人群相关的问题类型。问题形式多样，有些问题可能与个人经历有关[20]。
  - 可能性是一种上下文分析，对象是可能会对特定人群造成问题的数据操作。上下文可包括组织因素（例如公众对相关组织隐私保护方面的看法）、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等）或个人因素（例如人群分布、个人对隐私问题的兴趣或看法、个人的数据敏感性等）[21]。可辅助使用数据图进行上下文分析（见“筹措资源”）。
  - 影响是对问题发生所产生成本的分析。如 1.2 节所述，组织不会直接遭遇这些问题。此外，个人经历可能具有主观性。因此，影响或难以准确评估。在评估对个人的影响时，组织应考虑如何以最优方式进行内化，以便合理确定优先级，应对隐私风险[22]。

18 NIST 所开发的隐私风险评估方法（PRAM）可帮助组织识别、评估、应对隐私风险。该方法由一系列工作表构成。详细信息，请访问相关网站[3]。

19 参见 NIST SP 800-30《风险评估指南》（修订版 1）[12]，第 8 页。

20 NIST 在 PRAM 中加入了可疑数据操作及问题说明[3]，以供参考。有的组织有自己的问题集，有的组织将可疑数据操作及问题称为不良后果或危害。

21 有关上下文因素的更多信息，见 NIST PRAM 的工作表 2。

22 NIST PRAM 的工作表 3（影响页签）将组织成本（包括违规成本、直接业务成本、声誉成本以及内部文化成本）作为驱动因素，评估隐私问题对个人的影响。

- **评估方法**

  评估方法是确定已识别风险优先级的机制。评估方法可分为量化、半量化及定性三种[23][24]。

- **确定风险优先级（ID.RA-P4）**

  鉴于组织资源有限，组织会为风险划分优先级，方便确定应对措施[25]。

- **应对风险（ID.RA-P5）**

  如 1.2.2 节所述，风险应对通常分为缓解、转移/分担、规避和接受[26]。

建立可追溯的隐私要求

在明确哪些风险可以缓解后，组织就可以细化隐私要求，然后选取并实施控制措施（即技术、物理和/或政策保护措施）来满足这些要求[27]。可从各种来源选择控制措施，例如 NIST SP 800-53《信息系统与组织的安全和隐私控制》[28]。实施后，组织会持续评估控制措施是否可有效满足隐私要求并管理隐私风险。这样，就保证了控制措施和隐私要求之间可相互溯源，系统/产品/服务与组织的隐私目标之间责任明确。

监控变化

隐私风险管理是一个动态过程。组织要监控业务环境变化（包括新法律法规、新兴技术）以及系统/产品/服务的相应变化对隐私风险的影响，并依据本附录内容不断调整。（GV.MT-P1）

23 参见 NIST SP 800-30《风险评估指南》（修订版 1）[12]，第 14 页。
24 NIST PRAM 采用 10 分制（1–10），使用半量化方法.
25 NIST PRAM 提供了各种优先级表示方法，包括热图。具体信息，见工作表 3[3]。
26 NIST PRAM 的工作表 4 提供了流程，以应对不同优先级的各种隐私风险。
27 参见 NIST SP 800-37（修订版 2）[7]。
28 参见 NIST SP 800-53[10]更新内容。

附录 E 实现层级定义

本框架对各层级从四个方面进行了定义：

1 级：局部（Partial）

- **隐私风险管理流程：**组织的隐私安全风险管理实践并未固化，风险管理更像是即兴所为，有时甚至是被动反应。无法基于组织的风险管理优先级、隐私风险评估和业务/任务需求直接确定隐私活动的优先级。
- **综合隐私风险管理计划：**组织层级的隐私风险意识有限。因经验或从外部获取的信息不同，组织的隐私风险管理没有规律，总是就事论事。组织缺乏流程，无法在内部共享数据处理及其所产生隐私风险方面的信息。
- **数据处理生态系统关系：**几乎不了解组织与生态系统中其他实体（例如买方、供应商、服务提供商、业务伙伴、合作伙伴等）的关系。组织缺乏流程，无法了解隐私风险在整个生态系统中的扩散方式，也无法将隐私风险/要求传达给生态系统中的其他实体。
- **员工队伍：**部分员工对隐私风险或隐私风险管理流程有一些了解，但不承担具体的隐私责任。偶尔会提供隐私培训，但内容与最佳实践并未同步。

2 级：有风险意识（Risk Informed）

- **隐私风险管理流程：**管理层允许进行风险管理活动，但是并未将隐私管理确立为组织策略。无法基于组织的风险管理优先级、隐私风险评估和业务/任务需求直接确定隐私活动的优先级。
- **综合隐私风险管理计划：**组织层面有隐私风险意识，但没有建立适用于整个组织的隐私风险管理方法。组织内部以非正式的方式共享数据处理及其所产生隐私风险方面的信息。组织的部分层级会在组织目标和计划中考虑隐私风险。有隐私风险评估，但这种评估一般是一次性的，未形成持续机制。
- **数据处理生态系统关系：**对组织与生态系统中其他实体（例如买方、供应商、服务提供商、业务伙伴、合作伙伴等）的关系有些许了解。组织意识到自己所提供和使用的产品/服务存在隐私生态系统风险，但是并未正式采取统一行动。
- **员工队伍：**有专门人员负责隐私管理，但这些人可能同时承担其他责任。定期为隐私人员提供隐私培训，但缺乏统一流程及时获取最新的最佳实践。

3 级：可复用（Repeatable）

- **隐私风险管理流程：**组织的风险管理活动获得正式批准，固化为政策。风险管理流程根据业务/任务目标的变化而不断调整，再加上风险、政策与技术环境的不断变化，组织的隐私风险措施也随之定期更新。
- **综合隐私风险管理计划：**具有适用于整个组织的隐私风险管理方法，定义了基于风险的策略、流程与工序，并按计划实施及评审，有统一方法有效应对风险变化，能持续、精确地监控隐私风险。主管隐私的高管和其他高管就隐私风险定期沟通，确保组织的各项业务均考虑到了隐私。
- **数据处理生态系统关系：**组织明了自己在生态系统中的角色、依存关系和从属者，促进业内更广泛地了解风险，意识到自己所提供和使用的产品/服务存在隐私生态系统风险。此外，针对这些风险，组织通常会采取正式行动，包括通过书面协议传达隐私要求、治理架构及政策实施/监控。

- 员工队伍：隐私人员具有履行指定角色和职责的知识和技能。有针对全员的专业的定期隐私培训，普及最新的隐私做法。

4 级：自适应（Adaptive）

- **隐私风险管理流程：**根据隐私事件中吸取的教训以及所识别的新隐私风险，调整隐私实践。合入先进的隐私技术和实践进行持续优化，积极调整以适应不断变化的政策和技术环境，及时、有效应对不断演进的隐私风险。
- **综合隐私风险管理计划：**具有适用于整个组织的隐私风险管理方法，使用基于风险的政策、流程和程序处理可疑数据操作。决策时，清楚地了解并考虑到了隐私风险与组织目标之间的关系。高管将隐私风险与网络安全风险、财务风险和其他组织风险一视同仁，进行监控。组织在制定预算时，对当前和预测的风险环境以及风险承受能力有充分了解。业务部门在组织的风险承受范围内实现管理愿景，分析系统级风险。隐私风险管理作为组织文化的一部分，根据过往经验教训和对数据处理及其所产生隐私风险的不断深入了解，持续发展演进。组织能够快速高效地把握风险处理、传达方法的变化对于业务/任务目标的影响。
- **数据处理生态系统关系：**组织了解自己在生态系统中的角色、依存关系和从属者，促进业内更广泛地了解风险。通过实时或接近实时的信息，了解所提供和使用的产品/服务的隐私生态系统风险，并采取统一措施应对风险。此外，还会使用正式（例如协议）和非正式机制进行积极沟通，形成并维护牢固的生态系统关系。
- **员工队伍：**具有专业技能的隐私人员分布在组织各个部门；不同员工的视角不同，均能为隐私风险管理做出贡献。有针对全员的专业的定期隐私培训，普及最新的隐私做法。各级人员均了解组织的隐私价值以及自己在维护价值方面的角色。

小蜜蜂翻译公益译文项目，旨在分享国外先进网络安全理念、规划、框架、技术标准与实践，将网络安全战略性文档翻译为中文，为网络安全从业人员提供参考，促进国内安全组织在相关方面的思考和交流。

“安全加”社区

小蜜蜂公益翻译组