

NIST 网络安全框架 (CSF)2.0

美国国家标准与技术研究院
本出版物可从以下网址免费获取：https://doi.org/10.6028/NIST.CSWP.29

February 26, 2024

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

摘要

NIST 网络安全框架(CSF)2.0 为行业、政府机构和其他组织管理网络安全风险提供指导。它提供了一套高层级网络安全结果的分类体系，任何组织--无论其规模、行业或成熟度如何--均可使用该分类体系来更好地理解、评估、确定优先级并沟通其网络安全工作。CSF 并不规定应如何实现这些结果。相反，它链接到在线资源，这些资源就可用于实现这些结果的实践和控制措施提供额外指导。本文件描述了 CSF 2.0、其组成部分以及它可以被使用的众多方式中的一些。

关键词

网络安全；网络安全框架(CSF)；网络安全风险治理；网络安全风险管理；企业风险管理；概况；层级。

受众

负责制定和领导网络安全计划的人员是 CSF 的主要受众。CSF 也可供参与风险管理的其他人员使用--包括高管、董事会、采购专业人员、技术专业人员、风险管理人员、律师、人力资源专家以及网络安全和风险管理审计人员--以指导其与网络安全相关的决策。此外，CSF 还可用于制定和影响政策的人员(例如协会、专业组织、监管机构)，这些人员为网络安全风险管理设定并传达优先级。

补充内容

NIST 将继续构建和托管更多资源，以帮助组织落实 CSF，包括快速入门指南和社区概况。所有资源均在NIST CSF 网站上公开发布。有关在 NIST CSF 网站上引用的更多资源的建议，可随时通过 cyberframework@nist.gov与 NIST 分享。

注意致读者

除非另有说明，本出版物中引用、参考或摘录的文件并未全部纳入本出版物。

在 2.0 版之前，网络安全框架被称为“改进关键基础设施网络安全框架”。CSF 2.0 不再使用该标题。

致谢

CSF 是美国及世界各地产业界、学术界和政府多年协作努力的成果。NIST 感谢所有为本修订版 CSF 做出贡献的人士。有关 CSF 制定过程的信息可在NIST CSF 网站上找到。有关 CSF 使用经验的反馈可随时通过cyberframework@nist.gov与 NIST 分享。

目录

1. 网络安全框架(CSF)概述 1
2. 引言至CSF核心 3
3. CSF概况与层级简介 6
3.1. CSF Profiles 6
3.2. CSF Tiers 7
4. 补充CSF的在线资源简介 9
5. 改进网络安全风险沟通与整合 10
5.1. Improving Risk Management Communication 10
5.2. Improving Integration with Other Risk Management Programs 11
附录 A.CSF 核心 15
附录 B.CSF 层级 24
附录 C.术语表 26

图表清单

图1.CSF核心结构 3
图 2. CSF 功能 5
图3.创建和使用CSF组织概况的步骤 6
图4.CSF层级用于网络安全风险治理与管理 8
图5.使用CSF改进风险管理沟通 10
图6.网络安全与隐私风险关系 13

前言

网络安全框架(CSF)2.0 旨在帮助各种规模和行业的组织--包括行业、政府、学术界和非营利组织--管理和降低其网络安全风险。无论组织网络安全计划的成熟度水平和技术复杂性如何，它都适用。然而，CSF 并不采用一刀切的方法。每个组织都有共同的和独特的风险，以及不同的风险偏好和容忍度、特定使命以及实现这些使命的目标。组织必然会有不同的 CSF 实施方式。

理想情况下，CSF 将用于在应对企业其他风险(包括财务、隐私、供应链、声誉、技术或物理性质的风险)的同时应对网络安全风险。

CSF描述了旨在被广泛受众理解的目标结果，包括高管、管理者和从业人员，无论其网络安全专业知识如何。由于这些结果具有行业、国家和技术中立性，它们为组织提供了应对其独特风险、技术和使命考量所需的灵活性。结果直接映射到潜在安全控制列表，以便立即考虑缓解网络安全风险。

尽管CSF并非规定性的，但它帮助用户了解和选择特定结果。关于如何实现特定结果的建议，通过一套不断扩展的在线资源提供，这些资源补充了CSF，包括一系列快速入门指南(QSG)。此外，各种工具提供可下载格式，以帮助选择自动化部分流程的组织。QSG提出了使用CSF的初始方法，并邀请读者更深入地探索CSF及相关资源。通过NIST CSF网站获取的CSF以及来自NIST和其他方面的这些补充资源，应被视为一个“CSF组合”，以帮助管理和降低风险。无论以何种方式应用，CSF都促使用户在上下文中考虑其网络安全态势，然后使CSF适应其特定需求。

在先前版本的基础上，CSF 2.0 包含新特性，突显了治理和供应链的重要性。特别关注 QSGs，以确保 CSF 与小型组织及其较大型同行相关且易于获取。NIST 现在提供实施示例和信息性参考，这些内容可在线获取并定期更新。创建当前和目标状态的组织概况有助于组织比较其现状与期望或需要达到的状态，并使其能够更快速地实施和评估安全控制。

网络安全风险不断扩展，管理这些风险必须是一个持续的过程。无论组织是刚刚开始面对其网络安全挑战，还是已经拥有成熟且资源充足的网络安全团队并活跃多年，情况都是如此。CSF 旨在对任何类型的组织都有价值，并预期在长期内提供适当的指导。

1. 网络安全框架(CSF)概述

本文件是 NIST 网络安全框架(框架或*CSF*)2.0 版。它包括以下组成部分：

- **CSF 核心**，是 CSF 的核心部分，它是一个高层级网络安全结果的分类体系，可帮助任何组织管理其网络安全风险。CSF 核心组件是功能、类别和子类别的层级结构，详细描述每个结果。这些结果可被广泛的受众理解，包括高管、管理者和从业人员，无论其网络安全专业水平如何。由于这些结果具有行业、国家和技术中立性，它们为组织提供了所需的灵活性，以应对其独特的风险、技术和使命考量。

- **CSF 组织概况**，这是一种以 CSF 核心的结果来描述组织当前和/或目标网络安全态势的机制。
- **CSF 层级**，可应用于 CSF 组织概况，以表征组织网络安全风险治理和管理实践的严谨程度。层级还可为组织如何看待网络安全风险以及为管理这些风险而建立的流程提供背景。

本文档描述了组织可以期望实现的哪些理想结果。它既不规定结果，也不规定如何实现这些结果。关于组织如何实现这些结果的描述，提供在一套在线资源中，这些资源是对CSF的补充，可通过NIST CSF网站获取。这些资源就可用于实现结果的实践和控制措施提供了额外指导，旨在帮助组织理解、采用和使用CSF。它们包括：

- 参考信息，指向来自现有来源的关于每项结果的指导
  全球标准、指南、框架、法规、政策等。
- 实施示例，说明实现每项结果的可能方式
- 快速入门指南，提供关于使用 CSF 及其在线资源的可操作指导
  资源，包括从之前的 CSF 版本过渡到 2.0 版
- 社区概况和组织概况模板，帮助组织落实
  将 CSF 付诸实践，并为管理网络安全风险设定优先级

组织可以将 CSF 核心、概况和层级与补充资源一起使用，以理解、评估、确定优先级并沟通网络安全风险。

- **理解与评估：**描述组织部分或全部的当前或目标网络安全态势，确定差距，并评估解决这些差距的进展。

- **优先级排序：**识别、组织并优先排序与组织使命、法律和监管要求以及风险管理和治理期望相一致的管理网络安全风险的行动。

- **沟通：**提供一种通用语言，用于在组织内外沟通网络安全风险、能力、需求和期望。

CSF 设计供所有规模和行业的组织使用，包括工业界、政府、学术界和非营利组织，无论其网络安全计划的成熟度如何。CSF 是一种基础资源，可自愿采用，也可通过政府政策和 mandates 采用。CSF 的分类法及引用的标准、指南和实践并非特定于国家，CSF 的先前版本已被美国境内外的许多政府和其他组织成功利用。

CSF 应与其他资源(例如，框架、标准、指南、领先实践)结合使用，以更好地管理网络安全风险，并在企业层面为信息和通信技术(ICT)风险的整体管理提供信息。CSF 是一个灵活的框架，旨在供所有组织根据其规模进行定制使用。组织将继续拥有独特的风险--包括不同的威胁和漏洞--以及风险容忍度，还有独特的任务目标和要求。因此，组织管理风险的方法及其对 CSF 的实施将各不相同。

本文件其余部分的结构如下：

- 第2节解释了CSF核心的基础知识：功能、类别和子类别。
- 第3节定义了CSF概要和等级的概念。
- 第4节概述了CSF在线资源套件中选定的组成部分：信息参考、实施示例和快速入门指南。
- 第5节讨论了组织如何将CSF与其他风险管理计划相整合。
- 附录A是CSF核心。
- 附录 B 包含 CSF 层级的示例性说明。
- 附录 C 是 CSF 术语表。

2. 引言至CSF核心

附录A是CSF核心--一组按功能、类别和子类别排列的网络安全结果，如图1所示。这些结果不是要执行的操作清单；实现结果所采取的具体行动将因组织和使用场景而异，负责这些行动的人员也会有所不同。此外，核心中功能、类别和子类别的顺序和规模并不意味着实现它们的顺序或重要性。核心的结构旨在最大程度地契合那些负责在组织内将风险管理付诸实践的人员。

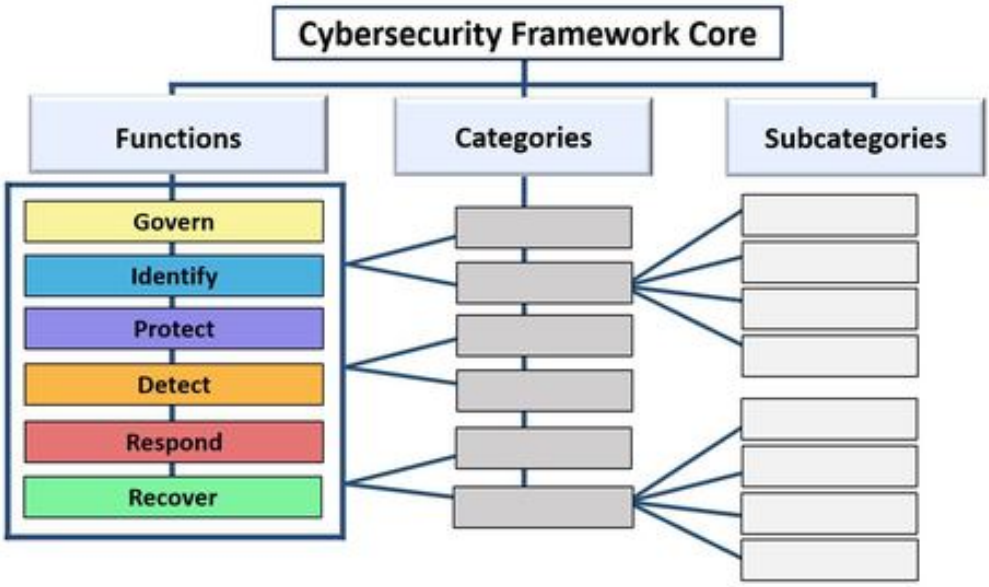


图1.CSF核心结构

CSF核心功能--治理、识别、防护、检测、响应和恢复--在最高层面组织网络安全结果。

- **治理(GV)** - 组织的网络安全风险管理策略、期望和政策得以建立、传达和监控。治理功能提供结果，以告知组织在其使命和利益相关方期望的背景下，可以采取哪些行动来实现并优先考虑其他五个功能的结果。治理活动对于将网络安全纳入组织更广泛的企业风险管理(ERM)策略至关重要。治理涉及对组织背景的理解；网络安全策略和网络安全供应链风险管理的建立；角色、职责与权限；政策；以及对网络安全策略的监督。

- **识别(ID)** - 组织当前的网络安全风险已被理解。理解组织的资产(例如数据、硬件、软件、系统、设施、服务、人员)、供应商及相关网络安全风险，使组织能够按照其风险管理策略和在治理下确定的使命需求来优先排序其工作。该功能还包括识别

组织支持网络安全风险管理的政策、计划、过程、程序和实践的改进机会，以为所有六项功能下的工作提供信息。

- **防护(PR)** - 使用保障措施来管理组织的网络安全风险。一旦资产和风险被识别并确定优先级，防护功能支持保护这些资产的能力，以预防或降低不利网络安全事件的可能性和影响，并增加利用机会的可能性和影响。该功能涵盖的结果包括身份管理、身份验证与访问控制；意识与培训；数据安全；平台安全(即保护物理和虚拟平台的硬件、软件和服务)；以及技术基础设施的韧性。

- **检测(DE)** - 发现并分析可能的网络安全攻击和失陷。检测能够及时发现和分析异常、失陷指标以及其他可能表明网络安全攻击和事件正在发生的不利事件。该功能支持成功的事件响应和恢复活动。

- **响应(RS)** - 针对已检测到的网络安全事件采取行动。响应支持遏制网络安全事件影响的能力。该功能内的结果涵盖事件管理、分析、缓解、报告和沟通。

- **恢复(RC)** - 恢复受网络安全事件影响的资产和运营。恢复支持及时恢复正常运营，以减少网络安全事件的影响，并在恢复工作中实现适当的沟通。

虽然许多网络安全风险管理活动侧重于预防负面事件的发生，但它们也可能支持利用积极机会。降低网络安全风险的行动可能以其他方式使组织受益，例如增加收入(例如，首先向商业托管提供商提供多余的设施空间，用于托管其自身和其他组织的数据中心，然后将主要金融系统从组织的内部数据中心迁移到托管提供商，以降低网络安全风险)。

图2将CSF功能显示为一个轮子，因为所有功能都相互关联。例如，组织将在识别功能下对资产进行分类，并在防护功能下采取措施保护这些资产。在治理和识别功能中规划和测试的投资将支持在检测功能中及时检测意外事件，并支持在响应和恢复功能中对网络安全事件进行事件响应和恢复行动。治理位于轮子的中心，因为它告知组织将如何实施其他五个功能。



图 2. CSF 功能

各项功能应同步推进。支持治理、识别、防护和检测的行动应持续进行，而支持响应和恢复的行动应始终准备就绪，并在网络安全事件发生时执行。所有功能都与网络安全事件密切相关。治理、识别和防护的结果有助于预防和准备应对事件，而治理、检测、响应和恢复的结果有助于发现和管理事件。

每项功能均以一个概括其内容的动词命名。每项功能分为若干类别，这些类别是共同构成该功能的相关网络安全结果。子类别进一步将每个类别划分为技术和管理活动的更具体结果。子类别并非详尽无遗，但它们描述了支持每个类别的详细结果。

功能、类别和子类别适用于组织使用的所有ICT，包括信息技术(IT)、物联网(IoT)和运营技术(OT)。它们也适用于所有类型的技术环境，包括云、移动和人工智能系统。CSF核心具有前瞻性，旨在适用于技术和环境的未来变化。

3.CSF概况和层级简介

本节定义了 CSF 配置文件(Profiles)和层级(Tiers)的概念。

3.1.CSF配置文件

CSF 组织概况从核心的结果角度描述组织当前和/或目标的网络安全态势。组织概况用于通过考虑组织的任务目标、利益相关方期望、威胁态势和要求，来理解、定制、评估、优先排序和沟通核心的结果。组织随后可以优先排序其行动以实现特定结果，并将该信息传达给利益相关方。

每个组织概况都包含以下一项或两项：

1. 当前概况规定了组织当前正在实现(或试图实现)的核心结果，并描述了每个结果的实现方式或实现程度。

2. 目标概况规定了组织为实现其网络安全风险管理目标而选定并优先排序的期望结果。目标概况考虑组织网络安全态势的预期变化，如新要求、新技术采用和威胁情报趋势。

> 社区概况是为解决多个组织之间的共同利益和目标而创建和发布的CSF结果基线。社区概况通常针对特定行业、子行业、技术、威胁类型或其他用例开发。组织可以将社区概况作为其自身目标概况的基础。社区概况的示例可在NIST CSF网站上找到。

图3所示并在下文概述的步骤说明了组织可以使用组织概况来帮助指导其网络安全持续改进的一种方式。



图3.创建和使用CSF组织概况的步骤

1. **界定组织概况的范围。**记录概况所依据的高层级事实和假设，以界定其范围。组织可以根据需要拥有任意数量的组织概况，每个概况具有不同的范围。例如，一个概况可以针对整个组织，也可以限定于组织的财务系统，或限定于应对勒索软件威胁和处理涉及这些财务系统的勒索软件事件。

2. **收集准备组织概况所需的信息。**信息的示例可能包括组织政策、风险管理优先级和资源、企业风险概况、业务影响分析(BIA)登记册、组织遵循的网络安全要求和标准、实践和工具(例如程序和保障措施)以及工作角色。

3. **创建组织概况。**确定概况应针对所选CSF结果包含哪些类型的信息，并记录所需信息。考虑当前概况的风险影响，以为目标概况的规划和优先级排序提供信息。同时，考虑使用社区概况作为目标概况的基础。

4. **分析当前概况与目标概况之间的差距，并制定行动计划。**进行差距分析，以识别和分析当前概况与目标概况之间的差异，并制定优先排序的行动计划(例如风险登记册、风险详细报告、行动计划和里程碑[POA&M])以解决这些差距。

5. **实施行动计划，并更新组织概况。**遵循行动计划以解决差距，并推动组织向目标概况迈进。行动计划可以有总体截止日期，也可以是持续进行的。

鉴于持续改进的重要性，组织可以根据需要多次重复这些步骤。

组织概况还有其他用途。例如，当前概况可用于记录组织当前的网络安全能力及已知的改进机会，并与外部利益相关方(如业务合作伙伴或潜在客户)沟通。此外，目标概况可帮助向供应商、合作伙伴和其他第三方表达组织的网络安全管理要求和期望，作为这些方需达成的目标。

3.2. CSF层级

组织可以选择使用层级来为其当前概况和目标概况提供信息。层级表征组织网络安全风险治理和管理实践的严谨程度，并为组织如何看待网络安全风险以及为管理这些风险而建立的流程提供背景。如图 4 所示并在附录 B 中概念性说明的层级，反映了组织管理网络安全风险的实践，分别为部分(层级 1)、风险知情(层级 2)、可重复(层级 3)和自适应(层级 4)。层级描述了从非正式的、临时的响应到敏捷、风险知情且

持续改进。选择层级有助于为组织如何管理其网络安全风险设定总体基调。

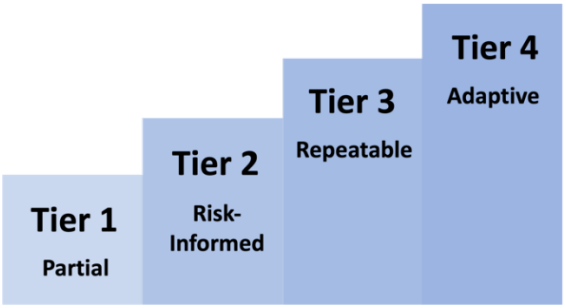


图4.CSF层级用于网络安全风险治理与管理

层级应补充而非取代组织的网络安全风险管理方法。例如，组织可以使用层级在内部沟通，作为组织范围内[1]管理网络安全风险方法的基准。当风险或要求更大，或当成本效益分析表明可可行且具有成本效益地减少负面网络安全风险时，鼓励向更高层级推进。

NIST ~~CSF网站~~提供了~~关于使用概况和层级的更多信息。它包括指向NIST托管的组织概况模板~~的链接，以及以各种机器可读和人类可用格式提供的社区概况存储库。

[1]就本文件而言，“组织范围内”和“企业”这两个术语具有相同含义。

4.补充CSF的在线资源简介

NIST 和其他组织制作了一套在线资源，帮助组织理解、采用和使用 CSF。由于这些资源托管在网上，因此可以比本文件更频繁地更新(本文件为保持对用户的稳定性而很少更新)，并且可以提供机器可读格式。本节概述三类在线资源：信息性参考、实施示例和快速入门指南。

资料性参考是表明核心与各种标准、指南、法规及其他内容之间关系的映射。资料性参考有助于说明组织可如何实现核心的结果。资料性参考可以是特定行业或特定技术的。它们可由 NIST 或其他组织编制。部分资料性参考的范围比子类别更窄。例如，SP 800-53《信息系统和组织的安全与隐私控制》中的某一特定控制，可能只是实现某一子类别所述结果所需的众多参考之一。其他

信息性参考可能层次较高，例如某项政策中的要求，它部分涉及多个子类别。使用 CSF 时，组织可以识别最相关的信息性参考。

实施示例提供了简明、以行动为导向的步骤示例，以帮助实现子类别中的结果。用于表达示例的动词包括共享、记录、开发、执行、监控、分析、评估和演练。这些示例并非组织为实现某一结果可能采取的所有行动的完整清单，也不代表应对网络安全风险所需行动的基线。

快速入门指南(QSGs)是有关特定 CSF 相关主题的简要文档，通常针对特定受众量身定制。QSGs 可以帮助组织落实 CSF，因为它们将 CSF 的特定部分提炼为可操作的“第一步”，组织在改善其网络安全态势和相关风险管理的过程中可以考虑这些步骤。这些指南按各自的时间框架进行修订，并根据需要添加新的指南。

有关 CSF 2.0 新信息性参考的建议可随时通过olir@nist.gov与 NIST 分享。有关在 NIST CSF 网站上引用的其他资源(包括其他 QSG 主题)的建议，应发送至cyberframework@nist.gov。

5.改进网络安全风险沟通与整合

CSF 的使用将因组织独特的使命和风险而异。在了解利益相关方期望以及风险偏好和风险容忍度(如治理中所述)的基础上，组织可以优先安排网络安全活动，从而就网络安全支出和行动做出明智决策。组织可以选择以一种或多种方式处理风险--包括减轻、转移、规避或接受负向风险，以及实现、分担、增强或接受正向风险--具体取决于潜在影响和可能性。重要的是，组织既可以在内部使用 CSF 来管理其网络安全能力，也可以在外部使用 CSF 来监督第三方或与第三方沟通。

无论 CSF 的使用情况如何，组织都可以受益于将 CSF 作为指导，帮助其理解、评估、确定优先级并沟通网络安全风险以及管理这些风险的行动。所选结果可用于聚焦并实施战略决策，以改善网络安全态势并保持关键任务功能的连续性，同时考虑优先事项和可用资源。

5.1.改进风险管理沟通

CSF 为改进有关网络安全期望、规划和资源的沟通提供了基础。CSF 促进了关注组织优先事项和战略方向的高管与负责管理可能影响这些优先事项实现的特定网络安全风险的管理者之间的双向信息流(如图 5 上半部分所示)。CSF 还支持管理者与实施和运营技术的从业人员之间的类似信息流(如图 5 下半部分所示)。该图左侧表明从业人员与管理者和高管分享其最新情况、见解和关切的重要性。



图5.使用CSF改进风险管理沟通

准备创建和使用组织概况涉及从高管处收集有关组织优先事项、资源和风险方向的信息。随后，管理者与从业人员协作，传达业务需求并创建基于风险的组织概况。为弥合当前概况与目标概况之间所识别的任何差距而采取的行动将由管理者和从业人员实施，并将为系统级计划提供关键输入。随着目标状态在整个组织中实现--包括通过系统级应用的控制和监控--更新后的结果可以通过风险登记册和进度报告进行分享。作为持续评估的一部分，管理者获得见解以做出调整，从而进一步减少潜在危害并增加潜在收益。

治理功能支持组织与**高管**之间的风险沟通。高管的讨论涉及战略，特别是网络安全相关不确定性可能如何影响组织目标的实现。这些治理讨论支持就风险管理策略(包括网络安全供应链风险)、角色、职责与权限、政策以及监督进行对话并达成一致。当高管基于这些需求确立网络安全优先事项和目标时，他们会传达有关风险偏好、问责制和资源的期望。高管还负责将网络安全风险管理与 ERM 计划及较低层级的风险管理计划相整合(见第 5.2 节)。图 5 上半部分所反映的沟通可以包括对 ERM 和较低层级计划的考虑，从而为管理者和从业人员提供信息。

高管设定的整体网络安全目标由**管理者**提供信息并逐级传达。在商业实体中，这些目标可能适用于某条业务线或运营部门。对于政府实体，这些可能是部门或分支机构层面的考量。在实施 CSF 时，管理者将侧重于如何通过目标概况中表述的共同服务、控制措施和协作来实现风险目标，并通过行动计划(例如风险登记册、风险详情报告、POA&M)中跟踪的行动加以改进。**从业人员**侧重于实施目标状态并衡量运营风险的变化，以帮助规划、执行和监控特定的网络安全活动。随着控制措施的实施以将风险控制在可接受水平，从业人员为管理者和高管提供所需信息(例如关键绩效指标、关键风险指标)，以了解组织的网络安全态势、做出知情决策并相应地维持或调整风险策略。高管还可以将这些网络安全风险数据与来自组织其他类型的风险信息相结合。随着周期重复，对期望和优先事项的更新将纳入更新后的组织概况。

5.2.改进与其他风险管理计划的整合

每个组织都面临多种类型的 ICT 风险(例如隐私、供应链、人工智能)，并可能使用针对每种风险的框架和管理工具。一些组织通过使用 ERM 在高层整合 ICT 和所有其他风险管理活动，而另一些组织则将各项活动分开，以确保对每项活动给予足够关注。小型

组织因其性质可能在企业层面监控风险，而较大的公司则可能维持独立的风险管理工作并将其整合到 ERM 中。

组织可以采用 ERM 方法来平衡包括网络安全在内的风险考量组合，并做出明智的决策。当高管将治理和风险战略与以往使用 CSF 的结果相结合时，他们会收到关于当前和计划中的风险活动的重要信息。CSF 帮助组织将其网络安全和网络安全风险管理的术语转化为高管能够理解的通用风险管理语言。

描述网络安全风险管理与 ERM 之间相互关系的 NIST 资源包括：

- NIST 网络安全框架 2.0 - 企业风险管理快速入门指南
- NIST 机构间报告(IR) 8286,整合网络安全与企业风险管理(ERM)
- IR 8286A,识别与评估网络安全风险以用于企业风险管理
- IR 8286B,为企业风险管理确定网络安全风险的优先级
- IR 8286C,暂存网络安全风险用于企业风险管理与治理监督
- IR 8286D,使用业务影响分析为风险优先级排序与响应提供依据
- SP 800-221,企业影响的信息与通信技术风险：治理与管理ICT风险项目在企业风险组合中
- SP 800-221A,信息与通信技术(ICT)风险结果：将ICT风险管理计划与企业风险组合整合

组织还可能发现 CSF 有助于将网络安全风险管理与各个 ICT 风险管理计划相整合，例如：

- **网络安全风险管理与评估：** CSF 可与既有的网络安全风险管理与评估计划整合，例如SP 800-37、RiskmanagementFrameworkforInformationSystemsandOrganizations，以及SP 800-30,指南用于开展风险评估，出自 NIST 风险管理框架(RMF)。对于使用NIST RMF 及其系列出版物的组织，CSF 可用于补充 RMF 从SP 800-53Security和PrivacyControlsforInformationSystems和Organizations中选择控制措施并确定其优先级的方法。
- **隐私风险：** 虽然网络安全与隐私是相互独立的学科，但它们的目标在特定情况下存在重叠，如图 6 所示。

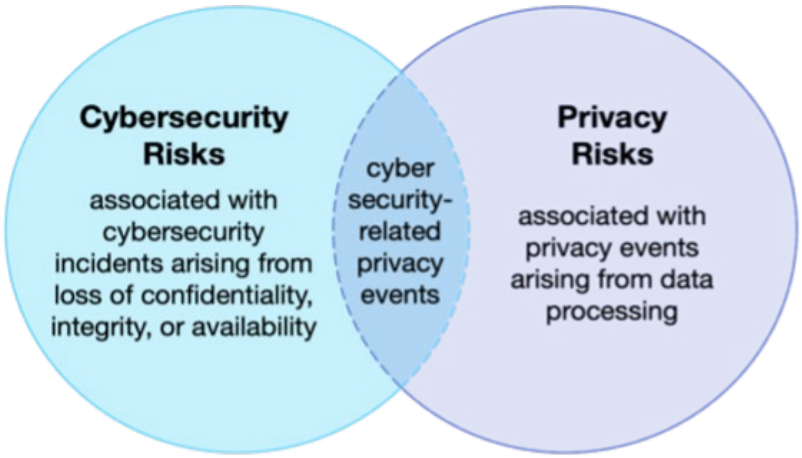


图6.网络安全与隐私风险关系

网络安全风险管理对于应对与个人数据的保密性、完整性和可用性丧失相关的隐私风险至关重要。例如，数据泄露可能导致身份盗用。然而，隐私风险也可能通过与网络安全事件无关的方式产生。

组织处理数据以实现使命或业务目的，这有时可能引发隐私事件，个人可能因数据处理而遭遇问题。这些问题可以多种方式表现，但NIST将其描述为从尊严类影响(例如，尴尬或污名)到更实质性的伤害(例如，歧视、经济损失或身体伤害)。NIST隐私框架和网络安全框架可以一起使用，以应对网络安全和隐私风险的不同方面。此外，NIST的隐私风险评估方法(PRAM)有一个示例问题目录，可用于隐私风险评估。

- **供应链风险：**组织可以使用CSF来促进网络安全风险监督以及与供应链中利益相关方的沟通。所有类型的技术都依赖于一个复杂、全球分布、广泛且互联的供应链生态系统，其具有地理上多样化的路线和多层外包。该生态系统由公共和私营部门实体(例如，采购方、供应商、开发者、系统集成商、外部系统服务提供商以及其他技术相关服务提供商)组成，这些实体相互作用，以研究、开发、设计、制造、采购、交付、集成、运营、维护、处置以及以其他方式利用或管理技术产品和服务。这些相互作用受到技术、法律、政策、程序和实践的塑造和影响。

鉴于该生态系统中复杂且相互关联的关系，供应链风险管理(SCRM)对组织至关重要。网络安全 SCRM(C-SCRM)是一个系统化过程，用于管理整个供应链中网络安全风险的暴露情况，并制定适当的响应策略、政策、过程和程序。CSF C-SCRM 类别[GV.SC]中的子类别提供了纯粹关注网络安全的成果与关注

SP 800-161r1《系统与组织的网络安全供应链风险管理实践》提供C-SCRM的深入信息。

- **新兴技术带来的风险：**随着新技术和技术的新应用变得可用，新的风险变得清晰。一个当代的例子是人工智能(AI)，它具有网络安全和隐私风险，以及许多其他类型的风险。NIST人工智能风险管理框架(AI RMF)的制定是为了帮助应对这些风险。将AI风险与其他企业风险(例如，财务、网络安全、声誉和隐私)一起处理将产生更综合的结果和组织效率。网络安全和隐私风险管理的考虑因素和方法适用于AI系统的设计、开发、部署、评估和使用。AI RMF核心使用功能，

类别和子类别，用于描述 AI 成果并帮助管理与人工智能。

附录 A.CSF 核心

本附录描述了 CSF 核心的功能、类别和子类别。表 1 列出了 CSF 2.0 核心功能和类别名称及唯一字母标识符。表中的每个功能名称都链接到附录的相应部分。核心的功能、类别和子类别的顺序不是按字母顺序排列的；它旨在最能引起组织内负责实施风险管理的人员的共鸣。子类别的编号故意不连续；编号中的空缺表示在 CSF 2.0 中重新定位的 CSF 1.1 子类别。

表1.CSF2.0核心功能与类别名称与标识符

功能	类别	类别标识符
治理(GV)	组织背景	GV.OC
	风险管理策略	GV.RM
	角色、职责和权限	GV.RR
	政策	GV.PO
	监督	GV.OV
	网络安全供应链风险管理	GV.SC
识别(ID)	资产管理	ID.AM
	风险评估	ID.RA
	改进	ID.IM
防护(PR)	身份管理、身份验证和访问控制	PR.AA
	意识与培训	PR.AT
	数据安全	PR.DS
	平台安全	PR.PS
	技术基础设施韧性	PR.IR
检测(DE)	持续监控	DE.CM
	不利事件分析	DE.AE
响应(RS)	事件管理	RS.MA
	事件分析	RS.AN
	事件响应报告与沟通	RS.CO
	事件缓解	RS.MI
恢复(RC)	事件恢复计划执行	RC.RP
	事件恢复沟通	RC.CO

CSF 核心、信息参考和实施示例可在CSF 2.0 网站上以及通过CSF 2.0 参考工具获取，用户可以通过该工具浏览这些内容，并以人类可读和机器可读的格式导出。CSF 2.0 核心还提供了一种类似于 CSF 1.1 的旧版格式。

治理(GV):组织的网络安全风险管理策略、期望和政策得到建立、沟通和监控

- **组织背景(GV.OC):**围绕组织网络安全风险管理决策的环境--使命、利益相关者期望、依赖关系以及法律、监管和合同要求--得到理解 o **GV.OC-01:**组织使命得到理解，并为网络安全风险提供依据

  管理提供信息

  o GV.OC-02：内部和外部利益相关者得到理解，其关于网络安全风险管理的需求和期望得到理解和考虑 o GV.OC-03：关于网络安全的法律、监管和合同要求--

  包括隐私和公民自由义务--被理解和管理 o **GV.OC-04:**外部利益相关方依赖或期望组织具备的关键目标、能力和服务

  被理解并沟通 o **GV.OC-05:**组织所依赖的成果、能力和服务

  理解并传达

- **风险管理策略(GV.RM):**组织的优先级、约束、风险容忍度和偏好声明以及假设被确立、沟通并用于支持运营风险决策

  o **GV.RM-01:**风险管理目标被确立并经组织利益相关方同意

  o **GV.RM-02:**风险偏好和风险容忍度声明被确立、沟通、并维护

  o **GV.RM-03:**网络安全风险管理活动和成果被纳入企业风险管理流程

  o **GV.RM-04:**描述适当风险应对选项的战略方向被已建立并传达

  o GV.RM-05：为网络安全风险(包括来自供应商和其他第三方的风险)建立跨组织的沟通渠道 o GV.RM-06：建立并沟通用于计算、记录、分类和

  优先排序网络安全风险的标准化方法 o **GV.RM-07:**战略机遇(即正向风险)被描述并

  纳入组织网络安全风险讨论

• **角色、职责与权限(GV.RR):**网络安全角色、职责和
促进问责、绩效评估和持续改进的权限已建立并传达

o GV.RR-01：组织领导者对网络安全风险负责并承担责任，并培育风险意识、道德和持续改进的文化 o GV.RR-02：与网络安全风险

管理相关的角色、职责和权限被确立、沟通、理解并执行 o **GV.RR-03:**分配与网络安全风险

策略、角色、职责和政策相称的充足资源 o **GV.RR-04:**网络安全被纳入人力资源实践

• **政策(GV.PO):**组织网络安全政策被确立、沟通并
执行

o GV.PO-01：基于组织背景、网络安全策略和优先级建立管理网络安全风险的政策，并予以沟通和执行 o GV.PO-02：管理网络安全风险的政策被审查、更新、沟通、

并执行，以反映需求、威胁、技术和组织使命的变化

• **监督(GV.OV):**组织范围内网络安全风险管理活动和
绩效的结果被用于为风险管理策略提供信息、改进和调整 o **GV.OV-01:**网络安全风险管理策略成果被审查以为

并调整战略和方向

o GV.OV-02：网络安全风险管理策略被审查和调整，以确保覆盖组织需求和风险 o GV.OV-03：组织网络安全风险管理绩效被评估并

已审查是否需要调整

• **网络安全供应链风险管理(GV.SC):**网络供应链风险
管理流程由组织利益相关方识别、确立、管理、监控和改进

o GV.SC-01：网络安全供应链风险管理计划、策略、目标、政策和流程被确立并经组织利益相关方同意 o GV.SC-02：针对供应商、客户和合作伙伴的网络安全角色和职责

被确立、沟通并在内部和外部协调 o **GV.SC-03:**网络安全供应链风险管理被整合到网络安全

和企业风险管理、风险评估和改进流程中 o **GV.SC-04:**供应商被知晓并按关键性优先排序

o **GV.SC-05:**应对供应链中网络安全风险的要求被确立、
优先排序，并整合到与供应商和其他相关第三方的合同及其他类型的协议中

o **GV.SC-06:**在建立正式供应商或其他第三方关系之前，执行规划与尽职调查以降低风险
o **GV.SC-07:**在关系存续期间，对供应商及其产品和服务以及其他第三方

所带来的风险进行理解、记录、优先级排序、评估、响应和监控

o **GV.SC-08:**相关供应商和其他第三方被纳入事件规划、
响应和恢复活动

o **GV.SC-09:**供应链安全实践被整合到网络安全和企业风险管理计划中，
并在技术产品和服务生命周期内对其绩效进行监控 o **GV.SC-10:**网络安全供应链风险管理计划包含以下条款：

在合作伙伴关系或服务协议结束后发生的活动

识别(ID):理解组织当前的网络安全风险

• **资产管理(ID.AM):**使组织能够实现业务目标的资产(例如数据、硬件、软件、系统、设施、服务、人员)被识别，并按照其对组织目标的重要性和组织的风险策略进行管理

o **ID.AM-01:**维护组织管理的硬件清单 o **ID.AM-02:**维护组织管理的软件、服务和系统清单

得到维护

o ID.AM-03： 维护组织授权网络通信以及内部和外部网络数据流的表示 o ID.AM-04： 维护供应商提供的服务清单 o ID.AM-05： 基于分类、关键性、资源和.....对资产进行优先级排序

对任务的影响

o **ID.AM-07:**维护指定数据类型的
数据和相应元数据的清单 o ID.AM-08： 系统、硬件、软件、服务和数据在整个.....过程中得到管理

它们的生命周期

• **风险评估(ID.RA):**对组织、资产和个人面临的网络安全风险
组织已理解

o **ID.RA-01:**识别、验证并记录资产中的脆弱性

o **ID.RA-02:**从信息共享论坛和
来源接收网络威胁

o **ID.RA-03:**识别并记录组织面临的内部和外部威胁 o **ID.RA-04:**威胁利用脆弱性的潜在影响和可能性

已识别并记录

o **ID.RA-05:**使用威胁、脆弱性、可能性和影响来理解

固有风险并为风险响应优先级排序提供依据 o **ID.RA-06:**选择、优先级排序、规划、跟踪并沟通风险响应 o **ID.RA-07:**管理变更和例外，评估其风险影响，记录并

跟踪

o **ID.RA-08:**接收、分析并响应脆弱性披露的流程
已建立

o **ID.RA-09:**在.....之前评估硬件和软件的真实性和完整性
获取和使用

ID.RA-10:在采购前对关键供应商进行评估

• **改进(ID.IM):**在所有 CSF 功能中识别对组织网络安全风险管理

流程、程序和活动的改进 o **ID.IM-01:**从评估中识别改进 o **ID.IM-02:**从安全测试和演练中识别改进，包括与供应商和相关第三方

协调完成的测试和演练 o **ID.IM-03:**从运营流程的执行中识别改进，

程序、活动和流程

o **ID.IM-04:**事件响应计划和其他影响运营的c网络安全计划
已建立、传达、维护并改进

防护(PR):使用保障措施来管理组织的网络安全风险

• **身份管理、身份验证与访问控制(PR.AA):**对物理和逻辑资产的访问仅限于授权用户、服务和硬件，并按照评估的未授权访问风险进行管理 o **PR.AA-01:**授权用户、服务和硬件的身份和凭证

由组织管理

o **PR.AA-02:**根据交互的上下文对身份进行验证并绑定到凭证
交互

o **PR.AA-03:**用户、服务和硬件均经过身份验证 o **PR.AA-04:**身份断言受到保护、传递和验证

o **PR.AA-05:**访问权限、权利和授权在策略中定义、管理、执行和审查，并纳入最小权限和职责分离原则

o **PR.AA-06:**对资产的物理访问进行管理、监控和执行与风险相称

• **意识与培训(PR.AT):**为组织人员提供网络安全意识与培训，使其能够执行与网络安全相关的任务

o PR.AT-01：为人员提供意识与培训，使其具备在考虑网络安全风险的情况下执行一般任务的知识和技能 o PR.AT-02：为担任专业角色的人员提供意识与培训，使其具备在考虑网络安全风险的情况下执行相关任务的知识和技能

• **数据安全(PR.DS):**数据按照组织的风险策略进行管理，以保护信息的保密性、完整性和可用性 o **PR.DS-01:**静态数据的保密性、完整性和可用性受到保护 o **PR.DS-02:**传输中数据的保密性、完整性和可用性受到保护 o **PR.DS-10:**使用中数据的保密性、完整性和可用性受到保护 o **PR.DS-11:**数据备份被创建、保护、维护和测试

• **平台安全(PR.PS):**硬件、软件(例如固件、操作系统、应用程序)以及物理和虚拟平台的服务按照组织的风险策略进行管理，以保护其保密性、完整性和可用性 o **PR.PS-01:**配置管理实践已建立并应用 o **PR.PS-02:**软件根据风险进行维护、更换和移除 o **PR.PS-03:**硬件根据风险进行维护、更换和移除 o **PR.PS-04:**生成日志记录并使其可用于持续监控 o **PR.PS-05:**防止未经授权软件的安装和执行 o **PR.PS-06:**集成安全软件开发实践，并对其性能在整个软件开发生命周期中受到监控

• **技术基础设施韧性(PR.IR):**安全架构按照组织的风险策略进行管理，以保护资产的保密性、完整性和可用性以及组织韧性

o **PR.IR-01:**网络和环境受到保护，免遭未经授权的逻辑访问和使用

o **PR.IR-02:**组织的技术资产受到保护，免遭环境
威胁

o **PR.IR-03:**实施机制以在正常
以及不利情况

o **PR.IR-04:**维持充足的资源容量以确保可用性

检测(DE):发现并分析可能的网络安全攻击和失陷

• **持续监控(DE.CM):**对资产进行监控，以发现异常、失陷指标和其他潜在不利事件 o **DE.CM-01:**
对网络和网络服务进行监控，以发现潜在不利

事件

o **DE.CM-02:**对物理环境进行监控，以发现潜在不利事件 o **DE.CM-03:**对人员活动和技术使用
进行监控，以发现潜在

不良事件

o **DE.CM-06:**对外部服务提供商的活动和服务进行监控，以发现
潜在不利事件 o DE.CM-09：计算硬件和软件、运行时环境及其数据

受到监控以发现潜在的不良事件

• **不利事件分析(DE.AE):**对异常、失陷指标和其他
潜在不利事件进行分析，以描述事件特征并检测网络安全事件

o **DE.AE-02:**对潜在不利事件进行分析，以更好地理解相关
活动

o **DE.AE-03:**关联来自多个来源的信息 o **DE.AE-04:**理解不利事件的估计影响和范围 o **DE.AE-06:**
向授权人员和工具提供不利事件信息 o **DE.AE-07:**将网络威胁情报和其他上下文信息整合到

分析

o **DE.AE-08:**当不利事件满足所定义的事件
准则

响应(RS):针对已检测到的网络安全事件采取行动

- **事件管理(RS.MA):**对已检测到的网络安全事件的响应进行管理

  - **RS.MA-01:**事件响应计划在与相关第三方的协调下执行
    一旦宣布发生事件，各方

  - **RS.MA-02:**事件报告经过分类和验证 o **RS.MA-03:**事件经过分类和优先级排序 o **RS.MA-04:**事件按需升级或提升 o **RS.MA-05:**启动事件恢复的准则得到应用

- **事件分析(RS.AN):**开展调查以确保有效响应和
  支持取证和恢复活动

  - **RS.AN-03:**执行分析以确定事件期间发生的情况
    以及事件的根本原因

  - **RS.AN-06:**调查期间执行的操作被记录，且记录的
    完整性和来源得以保留

  - **RS.AN-07:**收集事件数据和元数据，并确保其完整性和来源
    得到保留

  RS.AN-08:估计并验证事件的影响程度

- **事件响应报告与沟通(RS.CO):**响应活动
  按法律、法规或政策要求与内部和外部利益相关方协调

  - **RS.CO-02:**将事件通知内部和外部利益相关方 o **RS.CO-03:**与指定的内部和外部利益相关方共享信息

- **事件缓解(RS.MI):**执行活动以防止事件扩大和
  减轻其影响

  - **RS.MI-01:**事件得到遏制

  - **RS.MI-02:**事件已被根除

恢复(RC):受网络安全事件影响的资产和运营得到恢复

- **事件恢复计划执行(RC.RP):**执行恢复活动以确保受网络安全事件影响的系统和服务的运营可用性 o **RC.RP-01:**事件响应计划的恢复部分在启动后执行

  从事件响应流程中

o **RC.RP-02:**选择、界定范围、确定优先级并执行恢复操作 o **RC.RP-03:**在使用前验证备份和其他恢复资产的完整性

用于恢复

o **RC.RP-04:**关键任务功能和网络安全风险管理得到考虑

以建立事件后运营规范 o **RC.RP-05:**恢复资产的完整性得到验证，系统和服务得到恢复，

并确认正常运行状态 o **RC.RP-06:**事件恢复的结束基于标准予以宣布，且事件-

相关文档已完成

• **事件恢复沟通(RC.CO):**恢复活动与以下各方协调

内部和外部各方

o **RC.CO-03:**恢复活动及恢复运营能力的进展

传达给指定的内部和外部利益相关方 o **RC.CO-04:**关于事件恢复的公开更新使用经批准的方法和

信息传达

附录 B.CSF 层级

表2包含第3节所讨论的CSF层级的概念性说明。层级描述组织网络安全风险治理实践(治理)和网络安全风险管理实践(识别、防护、检测、响应和恢复)的严谨程度。

表2.CSF层级的概念性说明

层级	网络安全风险治理	网络安全管理
层级1： 部分	组织的应用 网络安全风险战略得到管理 以临时方式。 优先级排序是临时的，而非 正式基于目标或威胁 环境。	对网络安全风险的认知有限，在 组织层面。 组织以不规则的、逐案的方式实施网络安全风险管理。 组织可能没有能够在内部共享网络安全信息的流程 组织。 组织普遍不了解与其供应商以及其获取和使用的产品和服务相关的网络安全风险。
层级 2：风险 知情	风险管理实践 经管理层批准，但可能 不应将其确立为组织范围内的政策。 网络安全活动的优先级排序 活动和保护需求 直接由组织 风险目标、威胁 环境，或业务/任务 要求。	在组织层面存在对网络安全风险的意识，但尚未建立全组织范围的网络安全风险管理方法 已建立。 在组织目标和计划中对网络安全的考虑可能发生在组织的某些层面，但并非所有层面。对组织和外部资产的网络风险评估会发生，但通常不可重复或不再发生。 网络安全信息在组织内部以非正式方式共享。 组织了解与其供应商以及其获取和使用的产品和服务相关的网络安全风险，但并未针对这些风险采取一致或正式的应对措施。
层级 3： 可重复	组织的风险管理 实践得到正式批准并 表述为政策。 风险知情政策、流程和 程序已定义、按预期实施 并经过审查。 组织网络安全实践 定期更新，基于 风险管理流程的应用 以应对 业务/任务要求、 威胁和技术格局的变化。	存在组织范围内管理网络安全风险的方法。网络安全信息在整个组织内定期共享。 已建立一致的方法来有效应对风险变化。人员具备履行其指定角色所需的知识和技能 职责。 组织一致且准确地监控资产的网络安全风险。高级网络安全和非网络安全高管定期就网络安全风险进行沟通。高管确保在组织的所有运营环节中考虑网络安全。

层级	网络安全风险治理	网络安全管理
		组织的风险战略参考了与其供应商以及其获取和使用的产品和服务相关的网络安全风险。人员通过书面协议等机制正式应对这些风险，以传达基线要求、治理结构(例如风险委员会)以及政策实施和监控。这些行动按预期一致实施，并持续受到监控和审查。
第 4 级：存在组织范围的 采用基于风险信息的政策、流程和程序来应对潜在网络安全事件的适应性方法管理网络安全风险。网络安全风险与组织目标之间的关系被清晰理解并在决策时予以考虑。高管在与财务及其他组织风险相同的背景下监控网络安全风险。组织预算基于对当前和预测风险环境及风险容忍度的理解。业务单元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。	网络安全风险管理是组织文化的一部分。它源于对以往活动的认识以及对组织系统和网络活动的持续认识。组织能够快速高效地说明业务/任务目标的变化如何影响风险的处理和沟通方式。	组织根据以往和当前网络安全活动(包括经验教训和预测性指标)调整其网络安全实践。通过纳入先进网络安全技术和实践的持续改进过程，组织主动适应不断变化的技术格局，并及时有效地应对不断演变的复杂威胁。组织利用实时或近实时信息来理解并持续应对与其供应商以及其获取和使用的产品和服务相关的网络安全风险。网络安全信息在整个组织内部以及与授权第三方之间持续共享。

附录 C.术语表

CSF类别
一组相关的网络安全结果，共同构成一个CSF功能。

CSF社区概况
为满足多个组织之间的共同利益和目标而创建并发布的CSF结果基线。社区概况通常针对特定行业、子行业、技术、威胁类型或其他用例开发。组织可以将社区概况作为其自身目标概况的基础。

CSF核心
高层级网络安全结果的分类体系，可帮助任何组织管理其网络安全风险。其组成部分是功能、类别和子类别的层级结构，详细说明每个结果。

CSF当前配置文件
组织概况的一部分，规定组织当前正在实现(或试图实现)的核心结果，并描述每个结果的实现方式或实现程度。

CSF功能
网络安全结果的最高组织层级。共有六个CSF功能：治理、识别、防护、检测、响应和恢复。

CSF实施示例
一种简洁、以行动为导向的概念性说明，用于帮助实现CSF核心结果。

CSF资料性参考
一种映射，指示CSF核心结果与现有标准、指南、法规或其他内容之间的关系。

CSF组织概况
一种根据CSF核心结果描述组织当前和/或目标网络安全态势的机制。

CSF快速入门指南
一种补充资源，就与CSF相关的特定主题提供简要、可操作的指导。

CSF子类别
一组更具体的技术和管理网络安全活动结果，构成一个CSF类别。

CSF目标概况
组织概况的一部分，规定组织为实现其网络安全风险管理目标而选择和优先排序的期望核心结果。

CSF层级
对组织网络安全风险治理和管理实践严谨程度的表征。共有四个层级：部分(层级1)、风险知情(层级2)、可重复(层级3)和自适应(层级4)。

本文中标识了某些商业设备、仪器、软件或材料(商业或非商业)，以便充分说明实验程序。此类标识并不意味着 NIST 对任何产品或服务的推荐或认可，也不意味着所标识的材料或设备必然是用于该目的的最佳可用选择。

NIST技术系列政策
版权、使用和许可声明
NIST 技术系列出版物标识符语法

如何引用本NIST技术系列出版物：
美国国家标准与技术研究院(2024)NIST 网络安全框架(CSF)2.0。(美国国家标准与技术研究院，马里兰州盖瑟斯堡),NIST 网络安全白皮书(CSWP)NIST CSWP 29。https://doi.org/10.6028/NIST.CSWP.29

联系方式信息
cyberframework@nist.gov

美国国家标准与技术研究院
收件人：应用网络安全部，信息技术实验室 100 Bureau Drive(Mail Stop 2000) Gaithersburg, MD 20899-2000

所有评论均须依据《信息自由法》予以公开(FOIA)。

这份文件是怎么做出来的

本译本是《网络安全框架（CSF）2.0》的中文全译本，共 32 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-csf-2-0-zh

支持私有化部署（需按贵方模型与合规要求评估）

扫码关注服务号
咨询定制交付

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。