增强关键基础设施

网络安全的框架

版本 1.0

美国国家标准与技术研究所

2014 年 2 月 12 日

增强关键基础设施网络安全的框架

非官方中文译文·安天技术公益翻译组 译注

文 档 信 息			
原 文 名 称	Framework for Improving Critical Infrastructure Cybersecurity		
原 文 作 者	美国国家标准与技术研究所	**原 文 发 布 日 期**	2014 年 2 月 12 日
作 者 简 介	美国国家标准与技术研究所前身为国家标准局，是一家测量标准实验室，属于美国商务部的非监管机。 http://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology		
原 文 发 布 单 位	美国国家标准与技术研究所		
原 文 出 处	http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf		
译 者	安天技术公益翻译组	**校 对 者**	安天技术公益翻译组
免 责 声 明	本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本		

	译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。

目录

图形目录

表目录

执行摘要

美国的国家安全和经济安全取决于关键基础设施的可靠运作。网络安全威胁利用了关键基础设施系统的日益复杂性和连接性，将国家的安全、经济、公众安全和健康置于风险之中。与金融和声誉风险类似，网络安全风险影响到公司的底线。这会导致损失并影响收入，可能会损害公司的创新、获得并保持客户的能力。

为了更好地应对这些风险，总统于 2013 年 2 月 12 日签发了行政命令 13636《增强关键基础设施的网络安全》，其中规定："提高国家关键基础设施的安全和恢复能力，保持安全的网络环境，促进高效、创新、经济繁荣、安全、商业机密，隐私和公民自由；这是美国的一项政策"。为了执行该政策，行政命令 13636 呼吁创建一个自愿的基于风险的网络安全框架，该框架是一系列帮助企业管理网络安全风险的行业标准和最佳方法。该框架由政府和私营部门合作创建，根据业务需要用具有成本效益的方式处理和管理企业网络安全风险，而且不会对企业提出额外的监管要求。

该框架着重于使用业务驱动因素来指导网络安全活动，并将网络安全风险作为企业风险管理流程的一部分。该框架由 3 部分组成：框架核心、框架档案和框架实施层级。框架核心是关键基础设施行业的一系列网络安全活动、成果，和翔实的参考资料，为创建企业档案提供详细指导。通过使用档案，该框架将帮助企业根据业务需求、风险承受能力和资源来调整其网络安全活动。框架实施层级向企业提供了审查和了解网络安全风险管理方法的机制。

行政命令 13636 还要求该框架包括保护个人隐私和公民自由的方法（即在开展网络安全活动时需要保护个人隐私和公民自由）。虽然具体流程和现有需求会有所不同，但该框架能够帮助企业整合隐私和公民自由问题，并将其作为全面网络安全计划的一部分。

该框架使企业（无论大小、网络安全风险程度、或网络安全的复杂性）采用原则和最佳方法进行风险管理并改善关键基础设施的安全性和恢复能力。该框架向组织和机构提供了各种网络安全方法，包括有效的标准、准则和惯例。此外，因为它采用了全球公认的网络安全标准，所以美国境外的企业也可以将该框架作为加强关键基础设施网络安全的国际合作模型。

该框架并不是管理关键基础设施网络安全的通用方法。企业将继续面临独特的风险（不同的威胁、不同的漏洞、不同的风险承受能力），而且他们实施该框架的方式会有所不同。企业可以决定重要的关键服务活动，并可以优先考虑投资，以最大限度地获得成本效益。最后，该框架旨在减少和更好地管理网络安全风险。

该框架将会不断更新，会根据业界的反馈不断完善。随着该框架付诸实践，经验教训将被整合到未来版本中。这将确保它满足关键基础设施所有者和运营者在不断变化和充满挑战的环境中（新的威胁、风险和解决方案）的需求。

使用该自愿框架能够提高国家关键基础设施的网络安全，能够为企业提供指导，并能够改善国家关键基础设施的整体网络安全态势。

1. 框架简介

美国的国家安全和经济安全取决于关键基础设施的可靠运作。为了加强关键基础设施的恢复能力，奥巴马总统于 2013 年 2 月 12 日签发了行政命令 13636（EO）[1]《增强关键基础设施的网络安全》。 该行政命令呼吁创建自愿的网络安全框架（“框架”），这一框架提供了“优化、灵活、可重复、基于绩效和成本效益的方法”来管理关键基础设施服务涉及的程序、信息和系统的网络安全风险。该框架与业界合作开发，指导企业管理网络安全风险。

在该行政命令中，关键基础设施被定义为“对美国至关重要的物理或虚拟的系统和资产，这些系统和资产的无法运作或破坏将会对安全、国家经济安全、国家公共健康或安全等造成不利影响”。由于来自外部和内部的威胁压力越来越大，负责关键基础设施的企业需要有一致和迭代的方法来识别、评估和管理网络安全风险。无论企业规模、威胁曝光程度或网络安全的复杂性如何，这种做法是必要的。

关键基础设施机构包括公共和私营的所有者和运营者，以及其他负责保护国家基础设施的机构。每个关键基础设施行业的成员的职能执行受到信息技术（IT）和工业控制系统（ICS）的支持。[2] 这种对于 IT 和 ICS 的技术、通信和互联性的依赖已经改变或扩展了潜在的漏洞和风险。例如，ICS 和 ICS 数据越来越多地用于提供关键服务和支持业务决策，所以我们应该考虑网络安全事件对企业业务、资产、个人健康和安全及环境的潜在影响。为了管理网络安全风险，我们需要清楚地了解涉及 IT 和 ICS 的业务驱动因素和安全问题。因为每个企业的风险都是与众不同的，随着企业使用 IT 和 ICS，其使用的工具和方法也会有所不同。

认识到隐私和公民自由的保护对于提高公众信任的重要性，该行政命令要求框架包括保护个人隐私和公民自由的方法（即在开展网络安全活动时需要保护个人隐私和公民自由）。许多企业已经具备了解决隐私和公民自由问题的程序。该方法旨在补充这些程序，并指导隐私风险管理。隐私和网络安全的结合可以增加客户信心、促进更标准化的信息共享、简化操作，从而使企业获益。

为确保可扩展性和技术创新，该框架是技术中立的。该框架依赖于各种现有的标准、准

[1] Executive Order no. 13636, Improving Critical Infrastructure Cybersecurity, DCPD-201300091, February 12, 2013. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

[2] The DHS Critical Infrastructure program provides a listing of the sectors and their associated critical functions and value chains. http://www.dhs.gov/critical-infrastructure-sectors

则和惯例，使关键基础设施供应商能够具备恢复能力。依靠业界开发、管理和更新的全球性标准、准则和惯例，该框架提出的工具和方法将跨越国界、认识到网络安全风险的全球性、并随着技术进步和业务要求不断发展。利用现有的和新兴的标准能够推动经济规模的扩大，以及符合市场需求的有效产品、服务和方法的发展。市场竞争也促进了技术和方法的传播，为这些行业的利益相关者带来利益。

根据这些标准、准则和惯例，该框架为企业提供了常用的分类方法和机制：

1) 说明目前的网络安全态势；

2) 说明网络安全的目标状态；

3) 连续和重复的过程中，确定并优先处理改善机会；

4) 评估向目标状态的进展；

5) 与网络安全风险的内外部利益相关者沟通。

该框架补充（而非取代）企业的风险管理流程和网络安全方案。企业可以利用其现有流程，并充分利用该框架来寻找改善网络安全风险管理的机会，同时遵守行业惯例。另外，不具备网络安全方案的企业可以将框架作为基准来创建自己的方案。

正如该框架不是针对特定行业的，其提供的标准、准则和惯例的也不是针对特定国家的。美国境外的企业也可以使用该框架来加强自身的网络安全。该框架有助于关键基础设施网络安全方面的国家合作。

1.1 框架概述

该框架是一个基于风险的方法，用于管理网络安全风险，并且由 3 部分组成：核心框架、框架实施层级和框架档案。每个组成部分都加强了业务驱动因素和网络安全活动之间的联系。这些组成部分的介绍如下。

- *框架核心*是关键基础设施行业通用的一系列网络安全活动、期望的结果以及适用的参考文献。框架核心呈现了行业标准、准则和惯例，并考虑到网络安全活动的沟通以及企业预期结果（从管理层到实施/运营层）。框架核心是由 5 个功能组成：识别、保护、检测、响应、恢复。这些功能组成了企业网络安全风险管理的生命周期。该框架核心确定了每

个功能的主要类别和子类别，并将其与实例参考性文献匹配，如每个子类别的现有标准、准则和惯例。

- *框架实施层级*（“层级”）向企业提供审查网络安全风险和管理流程的环境。层级描述了企业的网络安全风险管理方法符合该框架定义的特征（例如，风险和威胁感知、可重复和自适应）的程度。这些层级在一定范围内表征了企业的方法，从部分（第 1 级）到自适应（第 4 级）。这些层级反映了非正式的响应到灵活、基于风险的响应的进展。在层级选择过程中，企业应考虑其目前的风险管理措施、威胁环境、法律和监管规定、业务/任务目标和企业规定。

- 框架档案（“档案”）代表企业基于业务需要从框架类别和子类别中选择的结果。在特殊的实施场景中，档案可以被定性为符合框架核心提出的标准、准则和惯例。可以将“当前”档案（当前状态）与“目标”档案（将来状态）进行比较，从而确定改进网络安全状态的机会。要创建档案，企业可以审查所有类别和子类别，并根据业务驱动因素和风险评估来确定哪些是最重要的；他们可以根据需要增加类别和子类别来解决企业风险。当前档案可以支持面实现目标档案的方法，其他业务需求包括成本效益和创新。档案可用于进行自我评估，并在企业内部或企业之间进行沟通。

1.2 风险管理和网络安全框架

风险管理是识别、评估和应对风险的持续过程。为了管理风险，企业应该了解事件发生的可能性以及其产生的影响。有了这些信息，企业可以确定可接受的风险水平，并将其作为“风险承受能力”。

随着对风险承受能力的了解，企业可以优先考虑网络安全活动，使企业能够做出关于网络安全支出的明智决定。风险管理计划的实施向企业提供了量化和调整网络安全计划的能力。企业可以选择以不同的方法来处理风险，包括缓解风险、转移风险、避免风险或接受风险，这取决于对关键服务的潜在影响。

该框架使用风险管理流程，使企业了解并优先处理网络安全问题。它支持风险评估和业务驱动因素验证，能够帮助企业选择网络安全活动的目标状态，并获得期望的结果。因此，该框架使企业能够在 IT 和 ICS 环境中动态选择并指导网络安全风险管理。

该框架是自适应的，能够提供用于各种网络安全风险管理流程的灵活、基于风险的方法。网络安全风险管理流程的例子包括国际标准化组织（ISO）31000:2009、[3] ISO / IEC27005:2011、[4]国家标准与技术研究所（NIST）的特别刊物（SP）800-39、[5]风险管理流程（RMP）准则。[6]

1.3 文档概述

本文档的其余章节和附录如下：

- 第 2 章描述了框架的组成部分：框架核心、框架实施层级、框架档案。
- 第 3 章给出了使用该框架的例子。
- 附录 A 以表格形式展示了框架核心：功能、类别、子类别、参考性文献。
- 附录 B 是术语表。
- 附录 C 列出了本文中用到的缩写词。

[3] International Organization for Standardization, Risk management – Principles and guidelines, ISO 31000:2009, 2009. http://www.iso.org/iso/home/standards/iso31000.htm

[4] International Organization for Standardization/International Electrotechnical Commission, Information technology – Security techniques – Information security risk management, ISO/IEC 27005:2011, 2011.http://www.iso.org/iso/catalogue_detail?csnumber=56742

[5] Joint Task Force Transformation Initiative, Managing Information Security Risk: Organization, Mission, and Information System View, NIST Special Publication 800-39, March 2011. http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

[6] U.S. Department of Energy, Electricity Subsector Cybersecurity Risk Management Process, DOE/OE-0003, May 2012. http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf

2. 框架基础

该框架提供了一种理解、管理以及表达内外部网络安全风险的共同语言。它有助于确定和降低网络安全风险；可以用来调整管理风险的政策、业务和技术方法。它可用于所有企业的网络安全风险管理，也可以专注于一个企业的关键服务供应。不同类型的机构（包括行业协调机构、协会和企业）可以将该框架用于不同的目的，包括建立共同档案。

2.1 框架核心

框架核心提供了一系列实现网络安全结果的活动，并给出了若干案例。该框架核心并不是要执行的操作清单。它给出了业界确定的网络安全结果，有助于进行风险管理。该框架核心包括 4 个要素：功能、类别、子类别、参考性文献，如图 1 所示：

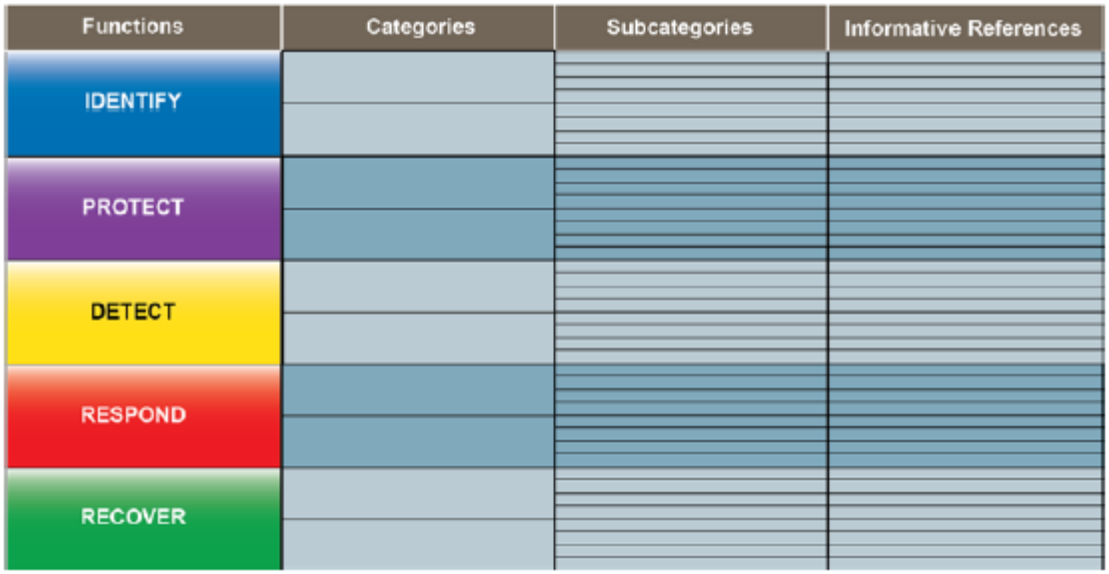

图 1：框架核心结构

该框架的核心元素共同运作，如下所示：

- **功能**：最高水平的基本网络安全活动，包括识别、保护、检测、响应和恢复。它们组织信息、制定风险管理决策、，应对威胁、从之前的活动中吸取教训，从而帮助企业进行网络安全风险管理。这些功能还符合现有的事件管理方法，有助于展示网络安全投资带来的影响。例如，对规划和演习的投资有助于及时响应和恢复，降低对服务供应的影响。

- **类别：**将功能细分为一系列网络安全结果，这些结果与纲领性需求和特定活动紧密相

关。类别的例子包括“资产管理”、“访问控制”和“检测流程”。

- **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。子类别提供了一个结果库，虽然并不详尽，但有助于每个类别的结果的实现。子类别的例子包括：“编目外部信息系统”、“保护静止的数据”和“调查检测系统的通知”。

- **参考性文献：**指关键基础设施行业的标准、准则和惯例，这些文献展示了实现每个子类别结果的方法。核心框架中提出的参考性文献是说明性的，并非详尽无遗。他们基于框架开发过程中最经常使用的跨行业指导。[7]

五个框架核心功能定义如下。这些功能不是为了形成一个串行路径，或实现最终的理想静态。相反，这些功能可以同时和连续地进行，以形成解决动态网络安全风险的方法。完整的框架核心参见附录 A。

- **识别**：企业了解管理系统、资产、数据和功能的网络安全风险。

识别对于框架的有效使用是最基本的。了解业务环境、支持关键功能的资源以及相关的网络安全风险能够使企业专注于其管理活动，同时与风险管理策略和业务需求保持一致。此功能的结果类别的例子包括：资产管理、业务环境、治理、风险评估、风险管理策略。

- **保护**：制定并实施相应的保障措施，以确保关键基础设施服务的供应。

保护功能支持限制网络安全事件影响的能力。此功能的结果类别的例子包括 :访问控制、意识和培训、数据安全、信息保护流程和程序、维护、保护技术。

- **检测**：制定并实施适当的活动，以识别网络安全事件的发生。

检测能够及时发现网络安全事件。此功能的结果类别的例子包括：异常和事件、安全性连续监测、检测流程。

- **响应**：制定并实施适当的活动，对检测到的网络安全事件采取行动。

[7] NIST developed a Compendium of informative references gathered from the Request for Information (RFI) input, Cybersecurity Framework workshops, and stakeholder engagement during the Framework development process. The Compendium includes standards, guidelines, and practices to assist with implementation. The Compendium is not intended to be an exhaustive list, but rather a starting point based on initial stakeholder input. The Compendium and other supporting material can be found at http://www.nist.gov/cyberframework/.

该响应功能支持限制网络安全事件影响的能力。此功能在结果类别的例子包括：响应计划、通信、分析、减灾、改善。

- **恢复**：制定并实施适当的活动，以增强恢复能力，恢复由于网络安全事件受损的任何功能或服务。

该恢复功能支持正常操作的及时恢复，减少网络安全事件的影响。此功能的结果类别的例子包括：恢复计划、改善、通信。

2.2 框架实施层级

该框架的实施层级（“层级”）向企业提供审查网络安全风险和管理流程的环境。层级的范围从部分（第 1 级）到自适应（第 4 级），并描述了网络安全风险管理措施的严谨和复杂程度，以及网络安全风险管理符合业务需求的程度。风险管理的考虑因素包括网络安全的许多方面，例如隐私和公民自由。

层级选择过程考虑到企业当前的风险管理方法、威胁环境、法律和监管要求、业务/任务目标和企业规定。企业应确定所需的层级，以确保所选择的级别符合企业的目标、可行、并能够将重要资产和资源的网络安全风险降低到可接受的水平。企业应考虑利用来自联邦政府部门和机构、信息共享和分析中心（ISACS）、现有的成熟度模型、或其他来源的指导，以帮助确定所需的层级。

虽然我们鼓励被认定为第 1 级（部分）的企业发展到第 2 层或更高层级，但是层级并不代表成熟度。我们鼓励发展到更高层级，是因为这样的改变会降低网络安全风险且符合成本效益。该框架的成功实施取决于企业目标档案中描述的结果，而不是层级的确定。

层级的定义如下：

第 1 级：部分

- *风险管理程序*：企业的网络安全风险管理措施并不拘泥于形式，而且风险管理以点对点方式进行。网络安全活动的优先顺序可能并非由企业风险目标、威胁环境或业务/任务需求直接确定。
- *集成的风险管理计划*： 目前企业层面的网络安全风险认知是有限的，管理网络安全风险的企业范围的方法也尚未确定。由于丰富的经验或从外部获得的大量信息，企业的风险管理措施并不规则，而是针对具体案例。企业可能没有设立在内部共享网络安全信息的流程。
- *外部参与*：企业可能不具备与其他机构协调或协作的流程。

第 2 级：风险知情

- *风险管理流程：*风险管理措施由管理层批准，但可能不被确立为企业范围的策略。网络安全活动的优先顺序由企业风险目标、威胁环境或业务/任务需求直接确定。
- *集成的风险管理计划*：目前企业层面的网络安全风险认知是存在的，但是管理网络安全风险的企业范围的方法尚未确定。风险认知、管理层批准的流程和程序都被制定和实施，具备足够资源的工作人员能够履行其网络安全职责。网络安全信息在企业内部以非正式的方式共享。
- *外部参与*：企业知道它在更大的生态系统中的角色，但还没有正式确定对外交流和共享信息的功能。

第 3 级：可重复

- *风险管理程序*：企业的风险管理措施被正式批准，并确定为企业政策。根据业务/任务要求、威胁和技术全景的变化，企业网络安全措施也定期更新。
- *集成的风险管理计划*：有企业范围的方法来管理网络安全风险。风险告知政策、流程和程序被定义、实施和审查。具备到位的方法来有效地应对风险的变化。企业人员具备履行职责的知识和技能。

- *外部参与*：企业了解其依赖关系和合作伙伴，并从这些合作伙伴获取信息，这些信息使企业制定基于风险的管理决策来响应安全事件。

第 4 级：自适应

- *风险管理流程*：基于经验教训和以往/当前网络安全活动的预测信标，企业采取相应的网络安全方法。通过不断完善、结合先进的网络安全技术和方法，企业积极适应不断变化的网络安全全景，并及时响应不断变化和复杂的安全威胁。
- *集成的风险管理计划*：存在企业范围的方法来管理网络安全风险，该方法采用基于风险的政策、流程和程序，以解决潜在的网络安全事件。网络安全风险管理是组织文化的一部分，从以前的活动、其他渠道的共享信息、以及对其系统和网络活动的不断认识中得以演进。
- *外部参与*：企业管理风险，并与合作伙伴积极共享信息，以确保准确及时的信息传播，在网络安全事件发生之前改善网络安全。

2.3 框架档案

该框架档案（“档案”）是功能、类别和子类别与业务需求、风险承受能力及企业资源的对应。档案使企业能够建立降低网络安全风险的路线图，该路线图符合企业和行业目标、法律/法规要求，被认为是行业最佳方法，并体现了风险管理的优先事项。鉴于许多企业的复杂性，他们可以选择有多个档案，并认识各自的需求。

框架档案可以用来形容特定网络安全活动的当前状态或目标状态。当前档案指示正在取得的网络安全成果。目标档案表明实现网络安全风险管理目标所需要的结果。档案支持业务/任务需求，并有助于企业内部和企业之间的风险沟通。此框架没有规定档案模板，使得该框架的实施具备灵活性。

比较档案（例如，当前档案和目标档案）可以发现实现网络安全风险管理目标的差距并加以解决。解决这些差距的行动计划可以促进上文所述路线图的制定。差距减缓的优先次序受企业业务需求和风险管理流程的驱动。这种基于风险的方法使企业能够衡量资源预算（如人员、资金），用具有成本效益的方法实现网络安全目标。

2.4 框架实施的协调

图 2 描述了企业内部常用的信息和决策流程：

• 管理

• 业务/流程

• 实施/运营

管理层向业务/流程层下达任务优先级、可利用的资源以及整体风险承受能力等信息。业务/流程层利用这些信息进行风险管理，然后与实施/运营层沟通业务需求，并创建一个档案。实施/运营层与业务/流程层沟通档案的进展情况。业务/流程层使用这些信息进行影响评估。业务/流程层向管理层报告评估的结果，使管理层了解企业的整体风险管理状况，并使实施/运营层认识到业务影响。

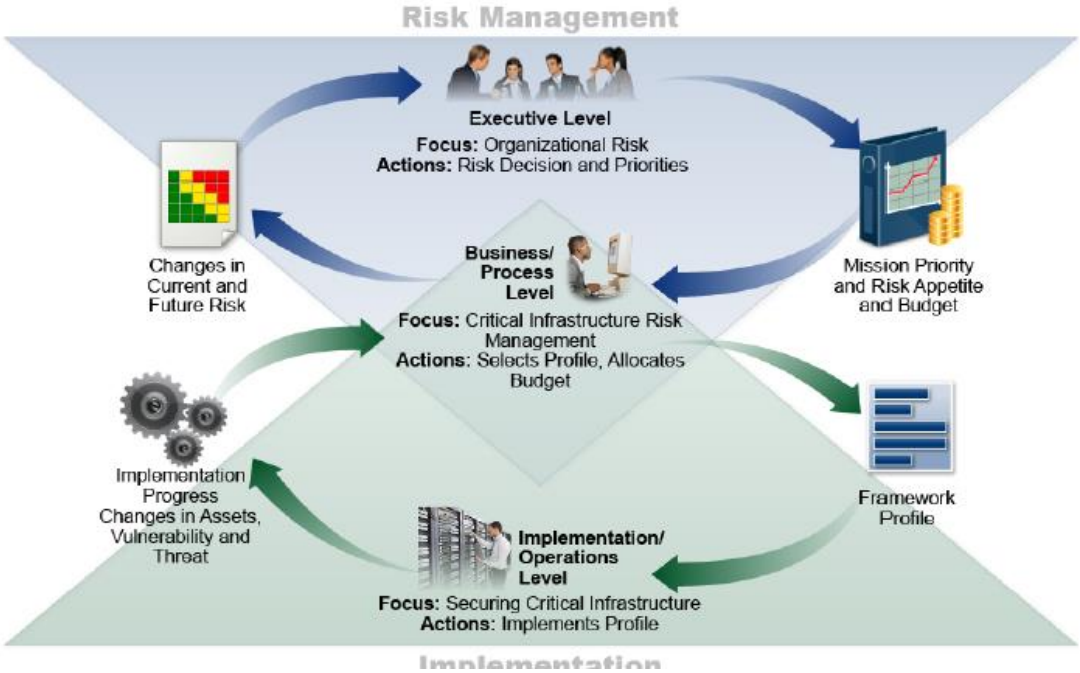

图 2：企业内部的信息和决策流

3. 如何使用该框架

企业可以将该框架作为其系统化过程（识别、评估和管理网络安全风险）的一个关键部分。该框架的目的不是取代现有的流程；企业可以使用其当前流程，并利用该框架弥补现有风险管理方法的漏洞，并制定改进的路线图。利用该框架作为网络安全风险管理工具，企业组织可以判断最重要的关键服务活动和优化支出，以最大限度地提高投资影响。

该框架旨在补充现有业务和网络安全运作。它可以作为新的网络安全方案的基础或改善现有流程的基础。该框架提供了一种向业务伙伴和客户表达网络安全要求的方法，可以帮助确定企业的网络安全方法。它还提供了在网络安全方案中保护隐私和公民自由的注意事项和流程。

以下各章节介绍了企业使用该框架的不同方法。

3.1 网络安全措施的基本评论

该框架可将企业的当前网络安全活动与框架核心提出的活动进行比较。通过创建当前档案，企业可以检查核心类别和子类别中描述的结果的实现程度，并符合 5 个功能：识别、保护、检测、响应和恢复。企业可能会发现它已经达到了理想的结果，因此，网络安全管理与已知风险相称。相反，企业可能会发现还有提高的空间。这样的企业可以利用这些信息来制定行动计划，以加强现有的网络安全措施并降低网络安全风险。企业也可能会发现它过度投资了。这样的企业可以使用此信息来重新优化资源，加强网络安全措施。

虽然这 5 个功能并不能取代风险管理流程，但是它们向高级管理人员和其他人员提供了一个简洁的方式来了解网络安全风险的基本概念，使他们能够评估如何管理识别的风险，以及如何完善现有网络安全标准、准则和惯例。该框架还可以帮助企业回答基本问题，包括“企业情况如何”。然后，企业可以以更明智的方式随时随地加强其网络安全措施。

3.2 建立或完善网络安全方案

下面的步骤说明了企业如何利用该框架来创建新的网络安全方案或改进现有的方案。这些步骤可以根据需要不断重复，以不断提高网络安全。

第 1 步：优先和范围。企业确定其业务/任务目标和高级优先事项。有了这些信息，企业可以制定网络安全决策，确定系统和资产的范围。该框架可适应企业内部的不同业务线或

流程，这些业务线和流程可能有不同的业务需求和风险承受能力。

第 2 步：定位。一旦为业务线或流程确定了网络安全方案的范围，企业应确定相关系统和资产、监管要求和整体风险方法。然后，企业应识别这些系统和资产的威胁和漏洞。

第 3 步：创建当前档案。通过确定实现了那些类别和子类别结果，企业可以创建一个当前档案。

第 4 步：进行风险评估。这项评估可以根据企业的整体风险管理流程或以前的风险评估活动进行。企业分析经营环境，以确定网络安全事件的可能性和事件对企业的影响。重要的是，企业整合新兴风险、威胁和漏洞数据，以便充分理解网络安全事件的可能性和影响。

第 5 步：创建目标档案。企业创建目标档案，该档案侧重于框架类别和子类别（描述企业期望的结果）的评估。企业也可以开发自己额外的类别和子类别，已管理其独特的风险。创建目标档案时，企业也许还要考虑外部利益相关者的影响和要求，如行业机构、客户和业务合作伙伴。

第 6 步：确定、分析和弥补差距。企业通过比较当前档案和目标档案来确定差距。接着，它创建一个优先行动计划，以解决这些差距（通过目标档案中的任务驱动因素、成本/效益分析，以及风险理解确定）。然后，企业确定解决差距所需的资源。以这种方式使用档案使企业能够做出有关网络安全活动的明智决定，支持风险管理，使企业能够进行具有成本效益的、有针对性的改进。

步骤 7：实施行动计划。如果先前步骤确定了差距，企业需要确定要采取的措施。然后，企业监视其目前的网络安全措施。为进一步指导，该框架确定了类别和子类别的示例参考性文献，但是企业需要确定哪些标准、准则和惯例最适合他们的需要。

企业可以根据需要重复这些步骤，以不断评估和改进其网络安全。例如，企业可能会发现，更加频繁地重复定位步骤能够提高风险评估的质量。此外，企业可以通过当前档案的迭代更新监控进展情况，随后将当前档案与目标档案进行比较。企业也可以利用这一流程调整其网络安全计划。

3.3 与利益相关者沟通网络安全要求

该框架为相互依存的利益相关者（负责关键基础设施服务）提供了沟通要求的共同语言，

例如：

- 企业可以利用目标档案向外部服务供应商（例如，企业向其输送数据的云供应商）表达网络安全风险管理要求。
- 企业可以通过当前档案表达其网络安全状态报告，将报告结果或与要求进行比较。
- 关键基础设施所有者/运营者确定其基础设施依赖的外部合作伙伴后，可以使用目标档案来传达所需的类别和子类别。
- 关键基础设施部门可以设立一个目标档案，将其作为定制目标档案的一个初始基线档案。

3.4 为新的/修订的参考信息确定机会

该框架可以为新的或修订的标准、准则或惯例（这些参考信息有助于企业满足新的需求）确定机会。实施给定的子类别、或开发新的子类别的企业可能会发现相关活动的一些参考性信息。为了满足这一需求，企业可能会与技术带头人和/或标准机构合作起草、制定、协调标准、准则或惯例。

3.5 保护隐私和公民自由的方法

本节介绍了行政命令所要求的保护个人隐私和公民自由的方法。由于各行业面临的隐私和公民自由问题不同，所以该方法提出了一系列解决这些问题的注意事项和流程。然而，并非网络安全方案中所有的活动都会引起这些因素引起问题。与第 3.4 节一致，可能需要开发技术保密标准、准则和其他最佳方法来支持技术改进。

当个人信息的使用、收集、处理、保存或泄露与企业的网络安全活动有关时，可能会出现隐私和公民自由问题。涉及隐私或公民自由的例子包括：导致过度收集或过度保存个人信息的网络安全活动；与网络安全活动无关的个人信息泄露或使用；导致拒绝服务或其他类似不利影响的网络安全减灾活动，包括影响言论或结社自由的事件检测或监控活动。

政府和政府代理人有直接的责任来保护网络安全活动中的公民自由。参考下文的方法，拥有或经营关键基础设施的政府和政府代理人应该具备到位的流程，根据适用的隐私法律、法规和宪法要求来支持网络安全活动的合规性。

为了解决隐私问题，企业应该考虑在一定的环境中他们的网络安全流程如何包含隐私原则，例如：尽量减少与网络安全事件相关的个人信息的收集、泄露和保存；将任何个人信息的使用限制于网络安全活动（非网络安全活动不得使用）；某些网络安全活动的透明度；获得个人同意并对不利影响制定补救措施；数据质量、完整性和安全性；问责制和审计。

框架核心参见附录 A，下列流程和活动可被视为解决上文提到的隐私和公民自由的一种手段。

网络安全风险的治理

- 企业对网络安全风险的评估和潜在风险的响应需要考虑到隐私问题；
- 负责网络安全相关隐私问题的人员向适当的管理层报告并接受适当的培训；
- 具备到位的流程，根据适用的隐私法律、法规和宪法要求来支持网络安全活动的合规性；
- 具备到位的流程，以评估企业措施和控制。

确定和授权个人访问企业资产和系统

- 需要采取措施来确定和解决访问控制措施的隐私问题，即涉及个人信息的收集、泄露和使用的问题。

意识和培训措施

- 网络安全工作人员的培训和意识活动应包括企业隐私政策；
- 向企业提供网络安全相关服务的供应商应该了解企业的隐私政策。

异常活动检测以及系统/资产监控

- 具备到位的流程，对企业的异常活动检测和网络安全监控进行隐私审查。

响应活动（包括信息共享或其他减灾工作）

- 具备到位的流程，以评估和应对是否、何时、如何以及在何种程度上将个人信息用于企业之外的网络安全信息共享活动。
- 具备到位的流程，对企业网络安全减灾活动进行隐私审查。

附录 A：框架核心

本附录介绍了核心框架：功能、类别、子类别、以及参考性文献（描述所有关键基础设施行业的通用网络安全活动）。框架核心所选择的呈现形式并不代表具体的实施顺序或暗示类别、子类别、参考性文献的重要性。本附录中的框架核心代表管理网络安全风险的一系列常见活动。虽然该框架并不详尽，但它是可扩展的，允许企业、部门和其他机构使用具有成本效益和效率的子类别和参考性文献，使他们能够管理自己的网络安全风险。在档案创建阶段，可以从框架核心中选取活动，也可以添加额外的类别、子类别和参考性文献。企业的风险管理流程、法律/监管规定、业务/任务目标以及企业规定指导着活动选择。评估安全风险和保护时，个人信息被认为是类别中确定的数据或资产的一部分。

虽然功能、分类和子类别确定的预期结果对 IT 和 ICS 是相同的，但是 IT 和 ICS 的运作环境和注意事项不同。ICS 对现实世界有直接作用，包括对个人健康和安全的潜在风险、对环境的影响。此外，与 IT 相比，ICS 有独特的性能和可靠性要求，当实施网络安全措施时必须考虑到安全和效率目标。

为便于使用，框架核心的每个部分被赋予唯一标识符。功能和类别都有唯一的字母标识符，如表 1 所示。每个类别的子类别用数字表示；每个子类别的唯一标识符参见表 2。

该框架的其他参考资料可在 NIST 网站上找到 http://www.nist.gov/cyberframework/。

功能唯一标识符	功能	类别唯一标识符	类别
ID	识别	ID.AM	资产管理
		ID.BE	业务环境
		ID.GV	治理
		ID.RA	风险评估
		ID.RM	风险管理策略
		PR.AC	访问控制

表 1：功能和类别的唯一标识符

PR	保护	PR.AT	意识和培训
		PR.DS	数据安全
		PR.IP	信息保护流程和程序
		PR.MA	维护
		PR.PT	保护技术
DE	检测	DE.AE	异常和事件
		DE.CM	安全持续性监控
		DE.DP	检测流程
RS	响应	RS.RP	响应计划
		RS.CO	通信
		RS.AN	分析
		RS.MI	减灾
		RS.IM	改善
RC	恢复	RC.RP	恢复计划
		RC.IM	改善
		RC.CO	通信

表 2：框架核心

功能	类别	子类别	参考性文献
识别 (ID)	**资产管理（ID.AM）**：使企业实现其业务目标的数据、人员、设备、系统和设施，根据业务目标和企业战略风险的重要性对这些资产进行管理。	**ID.AM-1**：企业内部的物理设备和系统。	• **CCS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2
		ID.AM-2：企业内部的软件平台和应用程序。	• **CCS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2
		ID.AM-3：映射的企业通信和数据流。	• **CCS CSC** 1 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, CA-3,
		ID.AM-4：编目的外部信息系统。	• **COBIT 5** APO02.02 • **ISO/IEC 27001:2013** A.11.2.6 • **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5：根据分类、重要性和商业价值对资源（例如，硬件、设备、数据和软件）进行优先排序。	• **COBIT 5** APO03.03, APO03.04, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.6 • **ISO/IEC 27001:2013** A.8.2.1 • **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
		ID.AM-6：确定全体员工和第三方利益相关者（如供应商、客户、合作伙伴）的网络安全角色和职责。	• **COBIT 5** APO01.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1

功能	类别	子类别	参考性文献
			• **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11
	业务环境（ID.BE）： 了解和优化企业的使命、目标、利益相关者和活动；此信息有助于确定网络安全角色、职责和风险管理决策。	**ID.BE-1**：确定并传达企业在供应链中的角色。	• **COBIT 5** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 • **ISO/IEC 27001:2013** A.15.1.3, A.15.2.1, A.15.2.2 • **NIST SP 800-53 Rev. 4** CP-2, SA-12
		ID.BE-2：确定并传达企业关键基础设施和行业中的地位。	• **COBIT 5** APO02.06, APO03.01 • **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3：确定并传达企业使命、目标和活动的优先级。	• **COBIT 5** APO02.01, APO02.06, APO03.01 • **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 • **NIST SP 800-53 Rev. 4** PM-11, SA-14
		ID.BE-4：确定对关键服务的依赖性和关键功能。	• **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 • **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5： 确定支持关键服务的恢复力要求。	• **COBIT 5** DSS04.02 • **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1
	治理 (ID.GV)：了解用于监管企业规定、法律、风险、环境和运作要求的政策、程序和流程，并向管理层报告网络安全风险。	**ID.GV-1**：确定企业信息安全策略。	• **COBIT 5** APO01.03, EDM01.01, EDM01.02 • **ISA 62443-2-1:2009** 4.3.2.6 • **ISO/IEC 27001:2013** A.5.1.1 • **NIST SP 800-53 Rev. 4** -1 controls
		ID.GV-2：根据企业内部职责和外部合作伙伴协调信息安全角色和责任。	• **COBIT 5** APO13.12 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1 • **NIST SP 800-53 Rev. 4** PM-1, PS-7
		ID.GV-3：了解和管理关于网络安全的法律及监管规定，包括隐私和公民自由的义务。	• **COBIT 5** MEA03.01, MEA03.04 • **ISA 62443-2-1:2009** 4.4.3.7

功能	类别	子类别	参考性文献
			• **ISO/IEC 27001:2013** A.18.1 • **NIST SP 800-53 Rev. 4** -1 controls from all families (except PM-1)
		ID.GV-4： 应对网络安全风险的治理和风险管理流程。	• **COBIT 5** DSS04.02 • **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 • **NIST SP 800-53 Rev. 4** PM-9, PM-11
	风险评估 (ID.RA)：企业了解运作中的网络安全风险（包括任务、功能、图像或声誉）、企业资产和人员。	**ID.RA-1**：识别和记录漏洞	• **CCS CSC** 4 • **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 • **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2：从信息共享论坛和来源获取威胁和漏洞信息。	• **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 • **ISO/IEC 27001:2013** A.6.1.4 • **NIST SP 800-53 Rev. 4** PM-15, PM-16, SI-5
		ID.RA-3：识别和记录内外部威胁	• **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 • **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
		ID.RA-4 :确定潜在的业务影响和可能性	• **COBIT 5** DSS04.02 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 • **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-9, PM-11, SA-14
		ID.RA-5：通过威胁、漏洞、可能性和影响来确定风险	• **COBIT 5** APO12.02 • **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16
		ID.RA-6：确定并优化风险响应	• **COBIT 5** APO12.05, APO13.02

功能	类别	子类别	参考性文献
		prioritized	• **NIST SP 800-53 Rev. 4** PM-4, PM-9
	风险管理策略(ID.RM)：确定企业的工作重点、规则、风险承受能力，并用于支持风险决策的制定。	**ID.RM-1：**建立、管理、并与企业的利益相关方协商风险管理流程。	• **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 • **ISA 62443-2-1:2009** 4.3.4.2 • **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-2：确定并明确表示企业的风险承受能力	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.3.2.6.5 • **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-3：企业的风险承受能力由它在关键基础设施及特定行业的风险分析中的角色确定。	• **NIST SP 800-53 Rev. 4** PM-8, PM-9, PM-11, SA-14
保护(PR)	**访问控制（PR.AC）：**对资产及相关设施的访问仅限于授权用户、程序、设备、活动和交易。	**PR.AC-1：**授权设备和用户的身份和证书	• **CCS CSC** 16 • **COBIT 5** DSS05.04, DSS06.03 • **ISA 62443-2-1:2009** 4.3.3.5.1 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 • **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.3.1, A.9.4.2, A.9.4.3 • **NIST SP 800-53 Rev. 4** AC-2, IA Family
		PR.AC-2：管理和保护对资产的物理访问	• **COBIT 5** DSS01.04, DSS05.05 • **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 • **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 • **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, 5, PE-6, PE-9
		PR.AC-3：管理远程访问	• **COBIT 5** APO13.01, DSS01.04, DSS05.03 • **ISA 62443-2-1:2009** 4.3.3.6.6 • **ISA 62443-3-3:2013** SR 1.13, SR 2.6 • **ISO/IEC 27001:2013** A.6.2.2, A.13.1.1, A.13.2.1

功能	类别	子类别	参考性文献
			• **NIST SP 800-53 Rev. 4** AC-17, AC-19,
		PR.AC-4：管理访问权限，将最低权限和职责分离原则结合起来。	• **CCS CSC** 12, 15 • **ISA 62443-2-1:2009** 4.3.3.7.3 • **ISA 62443-3-3:2013** SR 2.1 • **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 • **NIST SP 800-53 Rev. 4** AC-2, AC-3, AC-5, AC-6, AC-16
		PR.AC-5：保护网络的完整性，适当地结合网络隔离。	• **ISA 62443-2-1:2009** 4.3.3.4 • **ISA 62443-3-3:2013** SR 3.1, SR 3.8 • **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, SC-7
	意识和培训（PR.AT）：向企业员工和合作伙伴提供网络安全意识培训，使其具备适当的知识来履行自己的信息安全有关的职务，并遵守相关的政策、程序和协议。	**PR.AT-1**：所有的用户经过培训。	• **CCS CSC** 9 • **COBIT 5** APO07.03, BAI05.07 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.7.2.2
		PR.AT-2：授权用户了解其角色和职责。	• **CCS CSC** 9 • **COBIT 5** APO07.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2
		PR.AT-3：第三方利益相关者（如供应商、客户、合作伙伴）了解其角色和职责。	• **CCS CSC** 9 • **COBIT 5** APO07.03, APO10.04, APO10.05 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 • **NIST SP 800-53 Rev. 4** PS-7, SA-9
		PR.AT-4：高级管理人员了解其角色和职责。	• **CCS CSC** 9 • **COBIT 5** APO07.03

功能	类别	子类别	参考性文献
			• **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, • **NIST SP 800-53 Rev. 4** AT-2, PM-13
		PR.AT-5：物理和信息安全人员了解其角色和职责。	• **CCS CSC** 9 • **COBIT 5** APO07.03 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2,
	数据安全（PR.DS）：根据企业的风险策略来管理信息和记录（数据），以保护其机密性、完整性和可用性。	**PR.DS-1**：保护静止的数据。	• **CCS CSC** 17 • **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS06.06 • **ISA 62443-3-3:2013** SR 3.4, SR 4.1 • **ISO/IEC 27001:2013** A.8.2.3
		PR.DS-2：保护传输中的数据。	• **CCS CSC** 17 • **COBIT 5** APO01.06, DSS06.06 • **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3
		PR.DS-3：正式管理资产的移除、转移和处置。	• **COBIT 5** BAI09.03 • **ISA 62443-2-1:2009** 4. 4.3.3.3.9, 4.3.4.4.1 • **ISA 62443-3-3:2013** SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7
		PR.DS-4：有足够的能力确保可用性。	• **COBIT 5** APO13.01 • **ISA 62443-3-3:2013** SR 7.1, SR 7.2 • **ISO/IEC 27001:2013** A.12.3.1

功能	类别	子类别	参考性文献
			• **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
		PR.DS-5：防止数据泄露。	• **CCS CSC** 17 • **COBIT 5** APO01.06 • **ISA 62443-3-3:2013** SR 5.2 • **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, • **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SI-4
		PR.DS-6 :采用完整性检查机制来验证软件、固件和信息的完整性。	• **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 • **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 • **NIST SP 800-53 Rev. 4** SI-7
		PR.DS-7 :开发和测试环境独立于生产环境。	• **COBIT 5** BAI07.04 • **ISO/IEC 27001:2013** A.12.1.4 • **NIST SP 800-53 Rev. 4** CM-2
	信息保护流程和程序（PR.IP）： 采用安全策略（解决企业目的、范围、角色、职责、管理承诺、与其他企业的协调）、流程和程序来保护信息系统和资产。	**PR.IP-1**：建立和维护信息技术/工业控制系统的基本配置。	• **CCS CSC** 3, 10 • **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 • **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 • **ISA 62443-3-3:2013** SR 7.6 • **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4,CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2：实施系统开发生命周期来管理系统。	• **COBIT 5** APO13.01 • **ISA 62443-2-1:2009** 4.3.4.3.3 • **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5

功能	类别	子类别	参考性文献
			• **NIST SP 800-53 Rev. 4** SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8
		PR.IP-3：配置变更控制流程已到位。	• **COBIT 5** BAI06.01, BAI01.06 • **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 • **ISA 62443-3-3:2013** SR 7.6 • **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • **NIST SP 800-53 Rev. 4** CM-3, CM-4,
		PR.IP-4：定期进行、维护和测试信息备份。	• **COBIT 5** APO13.01 • **ISA 62443-2-1:2009** 4.3.4.3.9 • **ISA 62443-3-3:2013** SR 7.3, SR 7.4 • **ISO/IEC 27001:2013** • **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9
		PR.IP-5：符合企业资产物理运行环境的政策和法规要求。	• **COBIT 5** DSS01.04, DSS05.05 • **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 • **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 • **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-14, PE-15, PE-18
		PR.IP-6：根据政策销毁数据。	• **COBIT 5** BAI09.03 • **ISA 62443-2-1:2009** 4.3.4.4.4 • **ISA 62443-3-3:2013** SR 4.2 • **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.11.2.7 • **NIST SP 800-53 Rev. 4** MP-6
		PR.IP-7：不断改善保护流程。	• **COBIT 5** APO11.06, DSS04.05 • **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2,

功能	类别	子类别	参考性文献
			8, PL-2, PM-6
		PR.IP-8：与相关方共享保护技术的有效性。	• **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
		PR.IP-9：具备到位的响应计划（事件响应和业务连续性）和恢复计划（事件恢复和灾难恢复）并进行管理。	• **COBIT 5** DSS04.03 • **ISA 62443-2-1:2009** 4.3.2.5.3. 4.3.4.5.1 • **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2 • **NIST SP 800-53 Rev. 4** CP-2, IR-8
		PR.IP-10：测试响应和恢复计划。	• **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 • **ISA 62443-3-3:2013** SR 3.3 • **ISO/IEC 27001:2013** A.17.1.3 • **NIST SP 800-53 Rev.4** CP-4, IR-3, PM-14
		PR.IP-11：在人力资源措施中增加网络安全方法（例如，取消供应、人员筛选）。	• **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 • **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 • **ISO/IEC 27001:2013** A.7.1.1, A.7.3.1, A.8.1.4 • **NIST SP 800-53 Rev. 4** PS Family
		PR.IP-12：制定和实施漏洞管理方案。	• **ISO/IEC 27001:2013** A.12.6.1, A.18.2.2 • **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
	维护（PR.MA）：根据政策及程序对工业控制和信息系统组件进行维护与修理。	**PR.MA-1**：用批准和受控的工具及时维护企业资产并进行记录。	• **COBIT 5** BAI09.03 • **ISA 62443-2-1:2009** 4.3.3.3.7 • **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5 • **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5
		PR.MA-2：批准和记录企业资产的远程维护，并防止未经授权的访问。	• **COBIT 5** DSS05.04 • **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 • **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1

功能	类别	子类别	参考性文献
			• **NIST SP 800-53 Rev. 4** MA-4
	保护技术（PR.PT）： 根据政策，程序和协议管理技术安全解决方案，以确保系统和资产的安全性和恢复能力。	**PR.PT-1：**按照企业政策确定、记录、实施、审查审计/日志记录。	• **CCS CSC** 14 • **COBIT 5** APO11.04 • **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 • **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR SR 2.11, SR 2.12 • **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 • **NIST SP 800-53 Rev. 4** AU Family
		PR.PT-2:按照企业政策保护和限制可移动媒体的使用。	• **COBIT 5** DSS05.02, APO13.01 • **ISA 62443-3-3:2013** SR 2.3 • **ISO/IEC 27001:2013** A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 • **NIST SP 800-53 Rev. 4** MP-2, MP-4, MP-5, MP-7
		PR.PT-3：控制系统和资产的访问，结合最低功能原则。	• **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 • **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 • **ISO/IEC 27001:2013** A.9.1.2 • **NIST SP 800-53 Rev. 4** AC-3, CM-7
		PR.PT-4：保护通信和控制网络。	• **CCS CSC** 7 • **COBIT 5** DSS05.02, APO13.01 • **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8,

功能	类别	子类别	参考性文献
			SR 7.6 • **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, AC-17,
检测(DE)	**异常和事件（DE.AE）：**及时发现异常活动，了解事件的潜在影响。	**DE.AE-1：**为用户和系统建立网络运营及预期数据流的基线并进行管理。	• **COBIT 5** DSS03.01 • **ISA 62443-2-1:2009** 4.4.3.3 • **NIST SP 800-53 Rev. 4** AC-4, CA-3,
		DE.AE-2：对检测到的事件进行分析，以了解攻击目标和方法。	• **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 **ISO/IEC 27001:2013** A.16.1.1, A.16.1.4
		DE.AE-3：从多个来源和传感器收集事件数据并进行关联。	• **ISA 62443-3-3:2013** SR 6.1 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR- 5, IR-8, SI-4
		DE.AE-4：确定事件的影响。	• **COBIT 5** APO12.06 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI - 4
		DE.AE-5：确定事件警报阈值。	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.2.3.10 • **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
	安全持续性监控（DE.CM）：对信息系统和资产以离散的时间间隔进行监控，以确定网络安全事件并验证防护措施的有效性。	**DE.CM-1：**监控网络，检测潜在的网络安全活动。	• **CCS CSC** 14, 16 • **COBIT 5** DSS05.07 • **ISA 62443-3-3:2013** SR 6.2 • **NIST SP 800-53 Rev. 4** AC-2, AU-12,
		DE.CM-2：对物理环境进行监控，以发现潜在的网络安全事件。	• **ISA 62443-2-1:2009** 4.3.3.3.8

功能	类别	子类别	参考性文献
			• **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE- 20
		DE.CM-3：对人员进行监控，以发现潜在的网络安全事件。	• **ISA 62443-3-3:2013** SR 6.2 • **ISO/IEC 27001:2013** A.12.4.1 • **NIST SP 800-53 Rev. 4** AC-2, AU-12,
		DE.CM-4：检测恶意代码。	• **CCS CSC** 5 • **COBIT 5** DSS05.01 • **ISA 62443-2-1:2009** 4.3.4.3.8 • **ISA 62443-3-3:2013** SR 3.2 • **ISO/IEC 27001:2013** A.12.2.1
		DE.CM-5：检测未授权的移动代码。	• **ISA 62443-3-3:2013** SR 2.4 • **ISO/IEC 27001:2013** A.12.5.1 • **NIST SP 800-53 Rev. 4** SC-18, SI-4. SC-44
		DE.CM-6：对外部服务供应商的活动进行监控，以发现潜在的网络安全事件。	• **COBIT 5** APO07.06 • **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 • **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA- 9, SI-4
		DE.CM-7：监控未经授权的人员、连接、设备和软件。	• **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8：进行漏洞检测。	• **COBIT 5** BAI03.10 • **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 • **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** RA-5
	检测流程（DE.DP）：维护和测试检测流程和程序，以确保及时和充分的认识到异常事件。	**DE.DP-1**：明确界定检测角色和职责，以确保问责制。	• **CCS CSC** 5 • **COBIT 5** DSS05.01 • **ISA 62443-2-1:2009** 4.4.3.1 • **ISO/IEC 27001:2013** A.6.1.1

功能	类别	子类别	参考性文献
			• **NIST SP 800-53 Rev. 4** CA-2, CA-7,
		DE.DP-2：检测行为需遵守所有的要求。	• **ISA 62443-2-1:2009** 4.4.3.2 • **ISO/IEC 27001:2013** A.18.1.4 • **NIST SP 800-53 Rev. 4** CA-2, CA-7,
		DE.DP-3：测试检测流程。	• **COBIT 5** APO13.02 • **ISA 62443-2-1:2009** 4.4.3.2 • **ISA 62443-3-3:2013** SR 3.3 • **ISO/IEC 27001:2013** A.14.2.8 • **NIST SP 800-53 Rev. 4** CA-2, CA-7,
		DE.DP-4：向相关方传达事件检测信息。	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.3.4.5.9 • **ISA 62443-3-3:2013** SR 6.1 • **ISO/IEC 27001:2013** A.16.1.2 • **NIST SP 800-53 Rev. 4** AU-6, CA-2,
		DE.DP-5：不断完善事件检测流程。	• **COBIT 5** APO11.06, DSS04.05 • **ISA 62443-2-1:2009** 4.4.3.4 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4**, CA-2, CA-7,

功能	类别	子类别	参考性文献
响应 (RS)	**响应计划（RS.RP）**：执行和维护响应过程和程序，以确保及时应对网络安全活动。	**RS.RP-1**：事件中或事件后执行响应活动。	• **COBIT 5** BAI01.10 • **CCS CSC** 18 • **ISA 62443-2-1:2009** 4.3.4.5.1 • **ISO/IEC 27001:2013** A.16.1.5 • **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR- 8
	通信（RS.CO）： 与内部和外部利益相关者协调响应活动，包括来自执法部门的外部支持。	**RS.CO-1**：当需要进行响应时，工作人员知道自己的角色和运作顺序。	• **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 • **ISO/IEC 27001:2013** A.6.1.1, A.16.1.1 • **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2：根据确定的标准对事件进行报告。	• **ISA 62443-2-1:2009** 4.3.4.5.5 • **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 • **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
		RS.CO-3：根据响应计划共享信息。	• **ISA 62443-2-1:2009** 4.3.4.5.2 • **ISO/IEC 27001:2013** A.16.1.2 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4：根据响应计划与利益相关者进行协调。	• **ISA 62443-2-1:2009** 4.3.4.5.5 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.CO-5：如果外部利益相关者希望实现更广泛的网络安全态势感知，则可以自愿性地共享信息。	• **NIST SP 800-53 Rev. 4** PM-15, SI-5
	分析(RS.AN)：进行分析，以充分响应并支持恢复活动。	**RS.AN-1**：调查检测系统的通知。	• **COBIT 5** DSS02.07 • **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISA 62443-3-3:2013** SR 6.1 A.16.1.5 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-

功能	类别	子类别	参考性文献
			5, PE-6, SI-4
		RS.AN-2：了解事件的影响。	• **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISO/IEC 27001:2013** A.16.1.6
		RS.AN-3：进行取证。	• **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 • **ISO/IEC 27001:2013** A.16.1.7 • **NIST SP 800-53 Rev. 4** AU-7, IR-4
		RS.AN-4：根据响应计划对事件进行分类。	• **ISA 62443-2-1:2009** 4.3.4.5.6 • **ISO/IEC 27001:2013** A.16.1.4 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
	减灾（RS.MI）：执行活动，以防止事件扩张，减轻其影响，并消除事件。	**RS.MI-1**：对事件进行限制。	• **ISA 62443-2-1:2009** 4.3.4.5.6 • **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 • **ISO/IEC 27001:2013** A.16.1.5 • **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-2：缓解事件。	• **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 • **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 • **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-3：缓解新发现的漏洞或将其记录为风险。	• **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
	改善（RS.IM）：企业应根据当前和以前的检测/响应活动的经验教训改善其响应活动。	**RS.IM-1**：响应计划结合经验教训。	• **COBIT 5** BAI01.13 • **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.IM-2：更新响应活动。	• **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
恢复 (RC)	**恢复计划（RC.RP）**：执行和维护恢复流程和程序，以确保及时恢复受网络安全事件影响的系统和资产。	**RC.RP-1**：事件中或事件后执行恢复计划。	• **CCS CSC** 8 • **COBIT 5** DSS02.05, DSS03.04 • **ISO/IEC 27001:2013** A.16.1.5

功能	类别	子类别	参考性文献
			• **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
	改善（RC.IM）：结合经验教训，改善恢复计划和过程。	**RC.IM-1：**恢复计划结合经验教训。	• **COBIT 5** BAI05.07 • **ISA 62443-2-1:2009** 4.4.3.4 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.IM-2：更新恢复策略。	• **COBIT 5** BAI07.08 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
	通信（RC.CO）：与内外部各方协调恢复活动，如协调中心、互联网服务供应商、受攻击系统的所有者、被害人、其他 CSIR 以及供应商。	**RC.CO-1：**管理公共关系。	• **COBIT 5** EDM03.02
		RC.CO-2：事件后恢复声誉。	• **COBIT 5** MEA03.02
		RC.CO-3：与内部利益相关者和管理团队沟通恢复活动。	• **NIST SP 800-53 Rev. 4** CP-2, IR-4

附录 A 中提到的参考性文献可以参见以下资源：

- Control Objectives for Information and Related Technology (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx
- Council on CyberSecurity (CCS) Top 20 Critical Security Controls (CSC): http://www.counciloncybersecurity.org
- ANSI/ISA-62443-2-1 (99.02.01)-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program: http://www.isa.org/Template.cfm?Section=Standards8&Template=/Ecommerce/ProductDisplay.cfm&ProductID=10243
- ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels: http://www.isa.org/Template.cfm?Section=Standards2&template=/Ecommerce/ProductDisplay.cfm&ProductID=13420
- ISO/IEC 27001, Information technology -- Security techniques -- Information security management systems -Requirements: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534

- NIST SP 800-53 Rev. 4: NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 (including updates as of January 15, 2014). http://dx.doi.org/10.6028/NIST.SP.800- 53r4.

框架核心的子类别和参考性文献之间的映射代表了一致性，并非旨在确定参考性文献是否提供了期望的子目录结果。

附录 B：名词解释

本附录定义了本文中出现的术语。

类别：将一个功能细分为一系列网络安全结果，与纲领性需要和特定活动紧密相关。类别的例子包括“资产管理”、“访问控制”和“检测流程”。

关键基础设施：对美国至关重要的物理或虚拟的系统和资产，这些系统和资产的无法运作或破坏将会对安全、国家经济安全、国家公共健康或安全等造成不利影响。

网络安全：通过防止、检测和应对攻击来保护信息的过程。

网络安全事件：可能对企业运作带来影响的网络安全变化（包括任务、功能或声誉）。

检测（功能）：制定和实施适当的活动，以识别网络安全事件的发生。

框架：一种基于风险来降低网络安全风险的方法，由 3 部分组成：核心框架、框架档案和框架实施层级。也被称为“网络安全框架”。

框架核心：关键基础设施部门通用的网络安全活动和参考文献，并围绕具体结果组织而成。框架核心包括 4 种类型的元素：功能、类别、子类别、参考性文献。

框架实施层级：用来审查企业管理风险的结构，即企业如何看待网络安全风险、是否具备到位的流程来管理这种风险。

框架档案：一个特定的系统或企业从框架类别和子类别中选择的结果的一种表示。

功能：该框架的一个主要组成部分。功能提供了将网络安全活动纳入类别和子类别的最高水平结构。这 5 个功能是识别、保护、检测、响应和恢复。

识别（功能）: 了解并管理系统、资产、数据和能力的网络安全风险。

参考性文献：关键基础设施行业的标准、准则和惯例的特定部分，显示了实现子类别相关的结果的方法。

移动代码：可以原封不动地用于异构平台并以相同的语义执行的程序（例如，脚本、宏或其它便携式指令）。

保护（功能）：制定并实施相应的保障措施，以确保关键基础设施服务的供应。

授权用户：被授权（因此，是受信的）执行普通用户无权执行的、与安全性相关功能的用户。

恢复（功能）：制定和实施适当的活动，以保持计划的弹性，并恢复受网络安全事件影响的任何功能或服务。

响应（功能）：制定和实施适当的活动，针对检测到的网络安全事件采取行动。

风险：机构受潜在情况或事件威胁的程度，通常是（i）情况或事件发生时可能导致的不利影响；以及（ii）情况或事件发生的可能性。

风险管理：识别、评估和响应风险的过程。

子类别：将类别细分为技术和/或管理活动的具体结果。子类别的例子包括："编目外部信息系统"、"保护静止的数据"和"调查检测系统的通知"。

附录 C：缩写词

本附录定义了本文中出现的首字母缩写词。

CCS：网络安全理事会

COBIT：信息及相关技术的控制目标

DCS：分布式控制系统

DHS：美国国土安全部

EO：行政命令

ICS：工业控制系统

IEC：国际电工委员会

IR：跨机构报告

ISA：国际自动化协会

ISAC：信息共享和分析中心

ISO：国际标准化组织

IT：信息技术

NIST：美国国家标准和技术研究所

RFI：索取资料

RMP：风险管理流程

SCADA：监控和数据采集

SP：特刊