安全加社区

公益翻译项目

2016

提升关键基础设施网络安全框架

V1.0 版本

美国国家标准与技术研究院

2014 年 2 月 12 日

文档信息			
原文名称	Framework for Improving Critical Infrastructure Cybersecurity		
原文作者	Costin Raiu, Igor Soumenkov	原文发布日期	2014 年 2 月 12 日
作者简介			
原文发布单位	National Institute of Standards and Technology		
原文出处	www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf		
译者	小蜜蜂公益翻译组	校对者	小蜜蜂公益翻译组

小蜜蜂公益翻译组

执行摘要

美国的国家与经济安全取决于关键基础设施是否可靠运行。越来越多的关键基础设施系统接入网络，日益复杂，成为网络安全威胁的利用因素，置国家安全、经济以及公共安全与健康于风险之中。与金融和信誉风险类似，网络安全风险会使公司成本上升，收入下降，最终影响公司的运营结果。它还会损害组织的创新能力，妨碍其争取并留住客户。

为了更好地应对这些风险，奥巴马总统于 2013 年 2 月 12 日颁布了 13636 号行政命令《提升关键基础设施网络安全》。命令规定，“美国采取（这个）政策，以提升国家关键基础设施的安全与弹性，建立一个有助于提高效率、激发创新、促进经济繁荣的网络环境，同时保障安全、商业机密、隐私与公民自由。”为实施该政策，此行政命令要求制订一个针对此种风险的自愿实施的网络安全框架，以确定行业标准与最佳实践，帮助组织管理网络安全风险。在政府与私有部门的共同努力下，本框架出台，采用通用语言阐述了如何基于业务需求高效地应对并管理网络安全风险，但并未对企业提出额外的合规要求。

该框架强调用业务驱动引导网络安全活动，将网络安全风险作为组织风险管理流程的一部分。框架包括三个部分：框架核心（Framework Core）、框架对齐结果（Framework Profile）及框架执行层级（Framework Implementation Tiers）。框架核心包括网络安全活动、结果以及关键基础设施领域内常见的参考文献，为各组织拟定对齐结果提供具体指导。通过使用对齐结果，组织可协调网络安全活动，使之与业务需求、风险容忍度及资源相匹配。框架执行层级是一种机制。利用这种机制，组织可审视并了解自身的网络安全风险管理特点。

行政命令还要求框架提供恰当方法，保证个人隐私与公民自由不受关键基础设施相关组织进行的网络安全活动的影响。流程与现实需求总会有分歧，因此，组织可根据框架制定综合网络安全计划，将隐私与公民自由包含其中。

对于各种规模的组织、不同程度的网络安全风险以及网络安全形势，该框架都能提供风险管理原则和最佳实践，使其提升关键基础设施的安全与弹性。框架整合了当今业界普遍有效的标准、指南以及实践，为当今各种网络安全方法提供了大纲与架构。此外，框架引用了国际认可的网络安全标准，对海外组织也适用，国际合作亦可以此为指导增强关键基础设施的网络安全。

然而，框架并未提供一成不变的方法来管理关键基础设施的网络安全风险。各组织面临的风险各异（威胁不同、漏洞不同、风险容忍度也不同），因而应采取不同方式来实施框架提供的方法。它们应确定哪些活动对于关键服务交付意义重大，并对投资进行排序，把钱用在刀刃上。框架的终极目标是降低网络安全风险，对其进行更有效的管理。

框架作为动态文件会根据业界使用反馈进行持续更新并优化。在实际操作中，框架会不断合入之前的应用经验，形成新的版本。这样，对于动态环境中不断出现的新威胁、新风险与新解决方案，它可以轻松面对挑战，满足关键基础设施业主与经营者的防护需求。

使用本自愿框架可加强我国关键基础设施的网络安全，它一方面可从整体上改善国家关键基础设施网络安全的形势，另一方面可为各个组织提供指导。

目录

1. 框架介绍

美国的国家与经济安全取决于关键基础设施是否可靠运行。为加强基础设施的弹性，奥巴马总统于 2013 年 2 月 12 日颁布了 13636 号行政命令《提升关键基础设施网络安全》[1]。该命令要求制订一个自愿实施的网络安全框架（简称“框架”），为关键基础设施服务交付中直接涉及的流程、信息及系统提供基于性能的灵活、高效、可复用、具有优先级的网络安全风险管理方法。基于此要求，我们与安全行业共同制订了框架，为组织提供网络安全风险管理方面的指导。

行政命令中将关键基础设施定义为对美国至关重要的物理与虚拟系统和资产，该等系统和资产的缺陷或损坏将会削弱安全、国民经济安全和/或国民公共健康及安全。由于内外威胁造成的压力不断增大，关键基础设施相关组织需要一个持续、迭代的方法用以识别、评估和管理网络安全风险。任何规模的组织，不管其面临的威胁有多大或多复杂，都需要这样一个方法。

关键基础设施人群包括公有及私有业主与经营者及保障国家基础设施安全的实体。每个关键基础设施部门的组成部分在运行时都基于信息技术（IT）与工业控制系统（ICS）[2]，这种对于技术、通信及 IT 和 ICS 互通性的依赖改变并扩大了潜在的脆弱性，增加了潜在的运营风险。例如，ICS 及其运行中产生的数据越来越多地用于交付关键服务，支撑业务决策，这种情况下，须考虑网络安全事件对于组织的业务、资产、个人健康与安全、环境造成的潜在影响。管理网络安全风险需明了组织的业务驱动和针对 IT 与 ICS 的安全考虑。不同组织风险各异，再加上 IT 与 ICS 的使用，因而需要灵活运用本框架，采取不同的工具和方法达到防护目的。

行政命令认为保护隐私与公民自由可获得更多的公众信任，因而要求框架提供相关方法，在关键基础设施组织从事网络安全活动时保护个人隐私与公民自由。许多组织已采用针对隐私与公民自由的流程。框架提供的方法是对此种流程的补充与指导，使组织的隐私风险管理与网络安全风险管理方法相协调。将隐私与网络安全结合起来可提升客户信任度，规范信息共享，简化法务操作，因而对组织大有裨益。

框架保持技术中立，确保了可扩展性并有利于技术创新。框架基于现有标准、指南与实践，帮助关键基础设施提供商增强网络弹性。这些国际性的标准、指南与实践由业界制订、管理并更新。框架基于此提供的实现工具和方法考虑到网络安全风险的全球特性，适用各国情况，并根据技术发展与业务需求不断演进。使用现有及新兴标准具有规模经济效应，可促进开发高效的产品、服务与实践，满足市场需求。市场竞争也会促进这些技术与实践的快速传播，使相关产业的利益主体受益良多。

基于这些标准、指南与实践，框架为组织提供了通用的分类方法与机制以：

1) 描述网络安全现状；
2) 描述网络安全目标状态；
3) 识别可持续复用的各种改善机会，并为其制定优先级；
4) 评估目标状态的进展；
5) 与内外利益主体讨论网络安全风险。

框架对于组织的风险管理流程与网络安全计划来说是一个补充，而非替换。组织可使用其现有流程并利用框架来识别机会，以加强并沟通自己的网络安全风险管理，同时与业界实践对齐。若组织没有网络安全计划，则可以框架为参考制订相关计划。

框架并不囿于某一特定行业，它对于标准、指南与实践的通用分类方法也并非针对某一特定国家。海外组织可使用框架加强自己的网络安全管理，相关国际合作亦可参考框架制定统一标准。

1.1 框架概况

框架提出了基于风险的网络安全风险管理方法，由以下三部分构成：框架核心、框架执行层级及框架对齐结果，每部分都强调业务驱动与网络安全活动的联系。各部分含义解释如下：

[1] 13636 号行政命令《提升关键基础设施网络安全》，DCPD-201300091，2013 年 2 月 12 日. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

[2] DHS 关键基础设施计划列举了各相关部门及其功能与价值链：http://www.dhs.gov/critical-infrastructure-sectors

- 框架核心包括各关键基础设施部门的网络安全活动、期望结果与适用参考。这个部分描述了业界标准、指南与实践，各组织可基于此对网络安全活动与结果在组织内部（管理层至执行层）上传下达。框架核心有 5 个可持续进行的并发功能：识别、防护、检测、响应、恢复。这些功能作为一个整体，可从战略高度展示组织的网络安全风险管理活动。每个功能由关键类别与子类别构成，一一对应示例的参考资料，如现有标准、指南与实践。
- 框架执行层级（简称“层级”）为组织提供了评估网络安全风险的背景以及针对此种风险的现有管理流程。层级描述了组织的网络安全风险管理活动与框架所定义特点（如有风险与威胁意识、可复用、自适应）的符合程度。组织的网络安全风险管理活动被定义为“局部”（1 级）至“自适应”（4 级）等多个层级。这些层级反映了由偶发的被动回应到虑及风险的敏捷方法的递进转变。在确定层级过程中，组织应考虑现有的风险管理实践、威胁环境、法规要求、业务/任务目标及组织局限性。
- 框架对齐结果（简称“对齐结果”）描述了与业务需求相匹配的结果，这些业务需求由组织根据框架定义的类别与子类别进行选择。Profile 的目的是将标准、指南与实践按照实际场景与框架核心对齐。通过将“当前”对齐结果（即“现状”）与“目标”对齐结果（即“未来”状况）进行比较，组织可识别机会，改善网络安全状况。建立 Profile 时，组织可检视所有的类别、子类别，然后基于业务驱动及风险评估来确定重要的类别、子类别。此外，组织可根据风险管理需要添加类别、子类别。当前对齐结果支撑优先级排序，衡量目标对齐结果的进展，同时涵盖其他的业务需求如成本效率与创新。对齐结果适用于自我评估以及组织内或组织间的沟通。

1.2 风险管理与网络安全框架

风险管理是风险识别、评估与响应的动态过程。组织在管理风险时应了解事件发生的可能性及其影响。利用这些信息，组织能确定交付服务时可接受的风险级别，用风险容忍度表示。

组织根据风险容忍度确定网络安全活动的优先级，并对网络安全支出进行明智地决策。组织可通过执行风险管理计划来量化并沟通自己的网络安全计划变动，并可根据对于关键服务交付的潜在影响采用不同方法处理风险，如降低、转移、规避或接受风险。

组织可利用框架提供的风险管理流程传达与网络安全相关的决策并确定其优先级。框架支持连续风险评估及业务驱动认定，帮助组织确定网络安全活动期望达成的目标状态。这样，框架就赋予了组织为 IT 和 ICS 环境动态选择网络安全风险管理及提升方法的能力。

框架提供了灵活的基于风险的实施策略，可适用于各种网络安全风险管理流程，如 ISO 31000:2009[3]、ISO/IEC 27005:2011[4]、NIST 特别刊物（SP）800-39[5]、《电力行业网络安全风险管理流程指南》[6]。

1.3 文档构成

本文档其他部分还包括：

- 第 2 节介绍了框架构成：框架核心、框架执行层级及框架对齐结果；
- 第 3 节举例说明如何使用框架；
- 附录 A 用表格形式介绍了框架核心：功能、类别、子类别、参考资料；
- 附录 B 为术语表；
- 附录 C 列举了本文出现的缩略语。

[3] 国际标准化组织，《风险管理—原则与指南》，ISO 31000:2009，2009 年。
http://www.iso.org/iso/home/standards/iso31000.htm

[4] 国际标准化组织/国际电工委员会，《信息技术—安全技术—信息安全管理》，ISO/IEC 27005:2011，2011 年。
http://www.iso.org/iso/catalogue_detail?csnumber=56742

[5] 联合特别工作组变革项目，《管理信息安全风险：组织、使命与信息系统概念，NIST 特别刊物 800-39,2011 年 3 月。
http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

[6] 美国能源部，《电力行业网络安全风险管理流程》，DOE/OE-0003,2012 年 5 月。
http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20%20Final%20-%20May%202012.pdf

2. 框架基本信息

框架提供通用语言，方便组织内外理解、管理、描述网络安全风险。它可帮助识别降低网络安全风险的活动并定义其优先级，还可协调风险管理的策略、业务及技术方法。它既可管理组织部门间的网络安全风险，也可集中处理组织内部的关键服务交付。不同类型的单位（包括部门协调体系、合营企业及组织）可将框架用于不同目的，包括创建通用对齐结果。

2.1 框架核心

框架核心提供一系列为实现特定网络安全目标而进行的活动及指导示例作为参考。它并非行动列表，而是展示了业界确认的、可促进网络安全风险管理的关键网络安全成果。框架核心包含四个元素：功能、类别、子类别及参考资料，如图 1 所示。

图 1：框架核心结构

框架核心元素工作原理如下：

- **功能**处于最高级别，用于组织基本的网络安全活动。具体来说，功能包括识别、防护、检测、响应与恢复。组织可利用这些功能管理网络安全风险，包括组织信息、启动风险管理决策、解决威胁问题以及根据之前活动经验进行优化。功能在根据现有方法调整后可用于事件管理，展示网络安全投资的效果，例如，规划与演练方面的投资可促进及时响应与恢复，降低对服务交付的影响。
- **类别**是将功能细分为网络安全结果组，与计划需求和实际活动密切相关，比如，“资产管理”、“访问控制”和“检测流程”类别。
- 类别可进一步细分为**子类别**，描述具体的技术及/或管理活动结果。子类别列举了部分可辅助实现各类别目标的结果，“已编目外部信息系统”、“已保护休眠数据”及“已调查检测系统的通知”均为子类别。
- **参考资料**列举了关键基础设施部门常用的标准、指南及实践中的具体章节，描述了达到子类别要求的具体方法。本框架核心并未列举所有的参考资料，仅列举部分作说明之用。这些参考资料均为框架制订过程中最常引用的跨部门指导手册。

下文解释了框架核心功能，这些功能并不需要一步步顺序执行，也不会促使实现最终的静态目标。实际上，它们可以同时持续进行，形成有效的机制以应对动态的网络安全风险。完整的框架核心列表，参见附录 A。

- **识别：**针对系统、资产、数据和能力相关的网络安全风险，组织内部形成共识。
- 识别功能涉及的活动是有效利用框架的基础。组织须了解业务环境、关键功能的辅助资源及相关网络安全风险，这样才能根据风险管理策略及业务需求确定事情的轻重缓急，重点突破。本功能涉及的结果类别包括资产管理、业务环境、治理、风险评估及风险管理策略。
- **防护：**制订实施恰当的防护措施，确保关键基础设施服务的交付。
- 防护功能对于限制或遏制潜在网络安全事件的影响起支撑作用。本功能涉及的结果类别包括访问控制、安全意识与培训、数据安全、信息防护流程及工序、维护和防护技术。
- **检测：**规划并实施恰当的活动，识别网络安全事件。

检测功能可及时发现网络安全事件。本功能涉及的结果类别包括异常与事件、安全持续监控和检测流程。

- **响应：**规划并实施恰当的活动，在检测到网络安全事件时采取相应措施。
- 响应功能对于遏制潜在网络安全事件的影响起支撑作用。本功能涉及的结果类别包括响应规划、沟通、分析、缓解和优化。
- **恢复：**规划并实施恰当的活动来维护网络弹性计划，恢复网络安全事件中受损的功能或服务。
- 恢复功能可及时恢复正常运行，降低网络安全事件的影响。本功能涉及的结果类别包括恢复规划、优化和沟通。

2.2 框架执行层级

框架执行层级（简称“层级”）为组织提供了评估网络安全风险的背景以及针对此种风险的现有管理流程。框架执行层级从低到高分为四级，1 级为“局部”，4 级为“自适应”，描述了网络安全风险管理实践的严格与复杂程度，以及网络风险管理受业务需求的影响程度及其与组织的总体风险管理实践的结合度。风险管理考虑的因素包括网络安全的各个方面，如隐私和公民自由与组织的网络安全风险管理的结合度、对于潜在风险的响应。

在选择层级时，组织应考虑现有的风险管理实践、威胁环境、法规要求、业务/任务目标及组织局限性。组织应确定目标层级，保证所选择的层级符合组织目标，具有可行性，并能将关键资产与资源的网络安全风险降低至可接受级别。组织在确定目标层级时，应考虑从联邦政府部门与机构、信息共享与分析中心、现有的成熟模型或其他来源获取外部指导。

鼓励 1 级（局部）组织向 2 级或更高层级努力，但层级本身并不代表成熟度。若此等晋级可降低网络安全风险及成本，则予以鼓励。框架是否成功执行取决于目标对齐结果中描述的结果是否达成，而非所定的级别。

各层级定义如下：

1 级：局部（Partial）

- *风险管理流程：*组织的网络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。网络安全活动的优先级与组织风险目标、威胁环境或业务/任务需求并无直接联系。
- *综合风险管理计划：*组织层面的网络安全风险意识有限，没有建立组织范围内的网络安全风险管理方法。因经验或从外部获取的信息不同，组织的网络安全风险管理没有规律，总是就事论事。组织缺少流程，无法保证网络安全信息在内部共享。
- *外部参与：*组织缺少现成的流程，无法与其他单位配合协作。

2 级：具有风险意识（Risk Informed）

- *风险管理流程：*管理层允许进行风险管理活动，但是并未确立为组织策略。网络安全活动的优先级与组织风险目标、威胁环境或业务/任务需求有直接联系。
- *综合风险管理计划：*组织层面有网络安全风险意识，但没有建立适用于整个组织的网络安全风险管理方法。虑及风险的流程与工序获得管理层批准并实施，员工有充分资源履行自己的网络安全职责。网络安全信息在组织内部非正式地共享。
- *外部参与：*组织明了自己在更大范围的生态系统中的角色，但是没有将能力固化与外部互动及共享信息。

3 级：可复用（Repeatable）

- *风险管理流程：*组织的风险管理活动获得正式批准，固化为策略。组织的网络安全实践根据风险管理流程在业务/任务需求更改中的应用程度和不断改变的威胁与技术环境而定期更新。
- *综合风险管理计划：*具有适用于整个组织的网络安全风险管理方法，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，员工具有履行指定角色与职责的知识与技能。
- *外部参与：*组织了解附属机构与合作伙伴，并从这些合作伙伴获取信息，以进行协作并在事件发生后作出内部风险管理决策。

4 级：自适应（Adaptive）

- *风险管理流程：*组织根据之前与当前网络安全活动中获得的实践经验与预测指标调整其网络安全实践。组织通过合入先进的网络安全技术与实践进行持续优化，积极调整以适应不断变化的网络安全环境，及时应对不断演进、日益复杂的安全威胁。
- *综合风险管理计划：*具有适用于整个组织的网络安全管理方法，这个方法使用基于风险的策略、流程与工序处理潜在的网络安全事件。网络安全风险管理作为组织文化的一部分，由了解历史活动开始，发展到从其他来源获取信息，再持续监控其系统与网络中的活动。
- *外部参与：*组织管理风险，积极与合作伙伴共享信息，确保所分发及使用的信息准确、实时，以便提高网络安全，防止网络安全事件的发生。

2.3 框架对齐结果

对齐结果将功能、类别和子类别与组织的业务需求、风险承受能力和资源情况相匹配。

组织可利用对齐结果制作一份路线图来降低网络安全风险。该路线图需与组织和部门的目标一致，符合法律和监管要求和行业最佳实践，并反映出风险管理优先级。鉴于自身的复杂性，很多组织可能会选用多个对齐结果，与组织的某些部门相匹配，并识别其个性化需求。

框架对齐结果可显示特定网络安全活动的当前状态或所期望的状态。当前对齐结果呈现当前的网络安全结果。Target Profile 显示期望达到的网络安全风险管理目标。这些对齐结果支持业务/任务需求，并协助实现组织内部或组织间的风险沟通。考虑到实现上的灵活性，该框架文档不规定使用某些对齐结果模板。

通过对比对齐结果（例如当前对齐结果和目标对齐结果），组织可了解其当前网络安全结果与网络安全风险管理目标之间的差距。制定能够消除这些差距的行动计划，有助于实现上述路线图。可根据组织的业务需求和风险管理流程，确定差距缩小的优先顺序。采用这种基于风险的方法，组织可衡量资源评估情况（例如人员配备和融资），并按照优先顺序，以经济有效的方式实现网络安全目标。

2.4 协调框架实施

图 2 为组织内以下层级通用的信息和决策流程：

- 管理层
- 业务/流程层
- 实现/运营层

管理层与业务/流程层就任务优先级、可用资源、以及总体风险承受能力进行沟通。业务/流程层将沟通结果作为风险管理流程的输入，然后与实现/运营层沟通业务需求并创建对齐结果。之后，实现/运营层就对齐结果实现进度与业务/流程层进行沟通。业务/流程层基于这些信息进行影响评估。随后，业务/流程层管理人员将影响评估结果上报管理层，从而将组织内的整体风险管理流程传达给实现/运营层，让其了解风险对业务的影响。

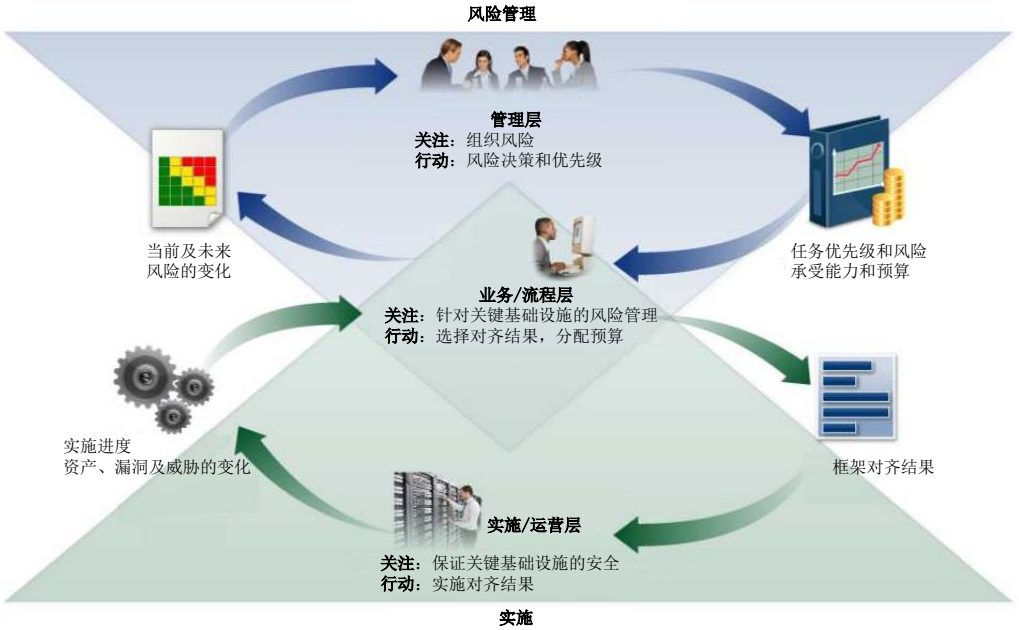

图 2 理论上的组织的信息与决策流程

3. 如何使用该框架

组织可将该框架作为网络安全风险识别、评估和管理这一系统流程的关键部分。该框架并非要取代现有流程。组织仍可使用当前流程，将其覆盖至框架中，以确定当前网络安全风险方案与风险管理目标之前的差距，并制定路线图缩小差距。组织可将框架用作网络安全风险管理工具，以确定对关键服务交付而言最重要的活动，然后对开支进行优先级排序，确保投资影响最大化。

该框架是对现有业务和网络安全运营的补充。组织可基于该框架构建新的网络安全计划或建立当前计划提升机制。该框架提供了一种将网络安全需求传达给业务合作伙伴和客户的方法，并协助组织确定网络安全实践与安全目标之间的差距。并且，该框架提供与网络安全计划可能涉及的隐私和公民自由相关的注意事项和流程。

下面列举了目前的几种框架使用方法。

3.1 对网络安全实践进行基础性评估

该框架可用于将组织当前的网络安全活动与框架核心展现的内容进行比较。通过创建当前对齐结果，组织可确定其对于核心类别和子类别中所展现的结果的实现程度。这些结果对应于框架的五个高层次的功能： 识别、防护、检测、响应与恢复。有的组织可能会发现其既定目标已实现，因此网络安全管理只针对已知风险。而有的组织可能认为还有提升的余地（或需要提升）。这些组织可利用此类信息执行行动计划，加强现有的网络安全实践，降低网络安全风险。还有的组织可能认为针对某些目标的投资是过度的。这些组织可基于此类信息重新确定资源优先级，以加强其他网络安全实践。

尽管这些组织仍采用原有的风险管理流程，但该框架的五个高层次的功能可使高层管理人员和其他人员很容易地提取网络安全风险的基本概念，这样他们就能够评估组织是如何管理已识别的风险的以及组织的网络安全标准、指导方针和实践比现有标准的高明之处。此外，该框架可协助组织回答诸如“我们的工作进行得怎样了？”之类的基本问题。这样，必要的时候，组织可在充分知情的情况下提升其网络安全实践。

3.2 制定或改进网络安全计划

以下步骤说明了组织如何利用该框架创建新的网络安全计划或改进现有计划。为实现网络安全的持续提升，可视需要重复执行以下步骤：

步骤 1 确定优先级和范围。组织确定其业务/任务目标以及整体上的组织优先级。基于这些信息，组织制定与网络安全实施相关的战略决策，并确定哪些系统和资产需支持所选业务线或流程。该框架需支持组织内的各业务线或流程。这些业务线或流程可能会有不同的业务需求和风险承受能力。

步骤 2 定位。组织在明确了需纳入网络安全计划的业务线和流程之后，需确定相关系统和资产，监管要求和整体风险管理方案。此外，组织还需识别这些系统和资产面临的威胁及存在的漏洞。

步骤 3 创建当前对齐结果。组织可创建当前对齐结果来展现框架核心中的类别和子类别的执行结果。

步骤 4 评估风险。组织可依据整体风险管理流程或之前的风险管理活动进行风险评估。评估时，组织需分析运营环境，判断是否有网络安全事件发生，并评估事件对组织的影响。很重要的一点是，组织需基于新型风险、威胁和漏洞数据，识别网络安全事件及其影响。

步骤 5 创建目标对齐结果。组织创建一个目标对齐结果，用于评估展现其期望的网络安全结果的框架类别和子类别。并且，组织还可以开发自己的类别和子类别，以查明其独特的组织风险。此外，组织还需考虑外部利益主体（如部门实体、客户和业务伙伴）的影响和需求。

步骤 6 确定当前的风险管理结果与期望目标之间的差距，分析这些差距，并对其进行优先级排序。组织对当前对齐结果和目标对齐结果的分析结果进行比较，找出差距。接下来，制定一份优先执行的行动计划消除这些差距。该计划依据任务驱动、成本/收益分析，对风险的理解，从而实现目标对齐结果中规划的目标。然后，组织确定消除这些差距所需的资源。通过利用这些对齐结果，组织可针对网络安全活动作出明智的抉择，进行风险管理，并实现高效的、有针对性的。

步骤 7 执行行动计划。组织决定应执行哪些行动以消除差距（如果步骤 6 说明了差距）。之后，组织基于目标对齐结果监控当前的网络安全实践。为提供进一步指导，该框架识别出有关类别和子类别的参考资料实例，而组织应确定哪些标准、指导方针、实践以及部门标准能够最为有效地满足自身的需求。

组织可能会视需要重复执行以上步骤，持续评估和提升其网络安全。例如，组织可能会发现多次执行步骤 2 提升了风险评估质量。此外，组织可通过当前对齐结果的迭代更新监控风险评估进度，随后将当前对齐结果与目标对齐结果提供的结果进行比较。使用这一流程，组织的网络安全计划将更加贴近框架实施层级。

3.3 与利益主体沟通网络安全需求

该框架提供通用语言，方便负责关键基础设施服务交付的相关利益主体进行需求沟通。例如：

- 组织可通过目标对齐结果向外部服务提供商（例如数据上传的云提供商）传达网络安全风险管理需求。
- 组织可通过当前对齐结果传达其网络安全状态，上报结果数据或将其与采集需求进行比较。
- 关键基础设施的负责人或运营商在发现基础设施所依赖的某个外部合作伙伴后，可使用目标对齐结果传达所需的类别和子类别。
- 关键基础设施部门可创建一个目标对齐结果，作为初始的基线对齐结果供员工使用，并在此基础上定制自身的目标对齐结果。

3.4 寻求机会识别新的或修订的参考资料

该框架可用于寻求机会识别新的或修订的标准、指导方针或实践，这些额外的参考资料将有助于组织满足新需求。组织在实现特定子类别或开发新子类别时，可能会发现手头仅有少量参考资料（如果有关于某一活动的此类数据的话）。为解决此问题，组织可与技术领导者和/或标准相关的机构起草、构建或协调某些标准、指导方针或实践。

3.5 保护隐私和公民自由

这一节介绍了行政命令所要求的一种用于解决网络安全操作可能导致的个人隐私和公民自由问题的方法。鉴于个人隐私和公民自由因部门和时间的推移而异，该方法应包含一套通用的注意事项和流程。组织可通过一系列的技术实现来充分考虑这些注意事项和流程。然而，并非安全计划中所涉及的所有活动均需考虑那些注意事项。组织需根据 3.4 节，制定技术方面涉及的隐私标准、指导方针以及其他最佳实践，为技术实现改进提供支撑。

当组织的网络安全活动需使用、收集、处理、维护和披露个人信息时，可能会引起隐私和公民自由问题。以下活动可能会涉及隐私或公民自由问题： 导致个人信息过度收集或保留的网络安全活动；使用或披露与网络安全活动无关的个人信息；造成拒绝服务或其他类似的潜在恶劣影响的网络安全风险缓解活动，包括诸如可能影响言论或结社自由的某些类型的事件检测或监控。

政府及其代理人针对网络安全活动导致的公民自由问题负有直接责任。如下列方法中所述，政府或拥有或运营关键基础设施的政府代理人应出台合理的流程使其网络活动符合适用的隐私权法律、法规和相关的宪法要求。

为解决隐私问题，组织应考虑如何（在采取了合理措施的情况下）使其网络安全计划遵循隐私原则，如： 网络安全活动涉及个人信息收集、披露和保留时确保数据最小化；针对专门用于网络安全活动收集的任意信息，使用网络安全活动之外规定的限制；某些网络安全活动的透明度；网络安全活动中使用个人信息前需得到个人同意，如造成负面影响，应对相关个人进行赔偿；数据质量、完整性和安全性以及问责和审计。

鉴于附录 A 将介绍组织对框架核心的评估，以下流程和活动可以看作是解决上述隐私和公民自由问题的一种方法：

网络安全风险治理

- 组织对网络安全风险和潜在风险响应的评估考虑了其网络安全计划中涉及的隐私问题。
- 负责网络安全隐私问题的员工训练有素，能够及时将发现的问题上报给管理人员。
- 已制定相关流程，确保网络安全活动符合适用的隐私权法律、法规和宪法要求。
- 已制定相关流程，对上述组织措施和控制措施的实施进行评估。
- 对访问组织财产和系统的个人进行识别和认证的方法
- 已采取措施识别和解决访问控制措施所导致的隐私问题。这些访问控制措施针对个人信息的采集、披露或使用。

- 安全意识和培训措施
- 已将组织的隐私策略中的适用信息纳入了网络安全人员的培训和安全意识提升活动。
- 已将组织适用的隐私策略传达给为其提供网络安全相关服务的服务供应商。
- 异常活动检测以及系统和资产监控
- 已制定相关流程，对组织的异常活动检测和网络安全监控进行了隐私审查。
- 响应活动，如信息共享或其他缓解措施
- 已制定流程，评估并解决以下问题：个人信息是否作为网络安全信息共享活动的一部分在组织外进行共享、何时共享、如何共享以及共享程度。
- 已制定流程，对组织的网络安全风险缓解措施进行隐私审查。

附录 A：框架核心

该附录介绍框架核心， 列举了功能、类别、子类别和参考资料，即列出了所有关键基础设施部门通用的网络安全活动。这里介绍的框架核心相当于一个通用网络安全风险管理活动的集合。并且，框架核心的呈现格式并非意在说明特定的实施顺序或表明类别、子类别或参考资料的重要性。该框架虽非详尽无遗，但具备扩展性，提供了子类别和参考资料，可使组织、部门和其他实体高效地管理其网络安全风险。在对齐结果创建过程中，组织可从框架核心中选择活动，并将类别、子类别和参考资料添加到对齐结果中。对齐结果创建时，活动的选择应符合组织的风险管理流程、法律/法规要求、业务/任务目标以及组织约束。在安全风险评估和防护过程中，个人信息应被视为类别中引用的数据或资产的一部分。

虽然 IT 与 ICS 在功能、类别和子类别方面有相同的期望结果，但二者的运行环境和注意事项有差异。ICS 对物理世界有直接影响，例如为个人健康和安全带来潜在风险以及对环境产生影响。此外，与 IT 相比较，ICS 具有独特的性能和可靠性需求，并且执行网络安全措施时必须考虑安全目标和效率。

为方便使用，框架核心的每个组件均有唯一标识。如表 1 所示，每个功能和类别均有唯一的字母标识（由字母组成）。每个类别中的子类别的标识格式为：所属类别的 ID_数字。见表 2。

如欲了解有关该框架的其他资料，请访问 NIST 网站 http://www.nist.gov/cyberframework/。

表 1 功能和类别的标识

功能标识	功能	类别标识	类别
ID	识别	ID.AM	资产管理
		ID.BE	业务环境
		ID.GV	治理
		ID.RA	风险管理
		ID.RM	风险管理战略
PR	防护	PR.AC	访问控制
		PR.AT	意识与培训
		PR.DS	数据安全
		PR.IP	信息防护流程与程序
		PR.MA	维护
		PR.PT	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	通信
		RS.AN	分析
		RS.MI	缓解
		RS.IM	提升
RC	恢复	RC.RP	恢复计划
		RC.IM	提升
		RC.CO	通信

表 2 框架核心（见下页）

功能	类别	子类别	参考资料
识别（ID）	**资产管理（ID.AM）：**对组织实现其业务目标所需的数据、人员、设备、系统和设施进行识别并依据其对组织的业务目标的重要性以及风险战略进行管理。	**ID.AM-1**：清点组织的物理设备和系统。	• 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 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2：清点组织的软件平台和应用。	• 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 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3：将组织沟通与数据流进行对应。	• CCS CSC 1 • COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.2 3 4 • ISO/IEC 27001:2013 A13 21 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4：列出外部信息系统。	• 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：基于类别、危险程度和商业价值对资源（例如硬件、设备、数据和软件）进行排序。	• 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：确立针对组织的全体员工和第三方利益主体（例如供应商、客户和合作伙伴）的网络安全角色和责任。	• COBIT 5 APO01.02, DSS06.03 • ISA 62443-2-1:2009 4.3.2 3 3 • ISO/IEC 27001:2013 A.6.1.1 • NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
	商业环境（ID.BE）：了解组织的使命、目标、利益主体和活动，并对其进行优先级排序。这些信息用于传达有关网络安全角色、责任和风险管理决策方面的信息。	**ID.BE-1**：确定组织在供应链中的角色并充分传达。	• 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：确定组织在关键基础设施和行业部门之中的地位并充分传达。	• COBIT 5 APO02.06, APO03.01 • NIST SP 800-53 Rev. 4 PM-8
		ID.BE-3：确定组织的使命、目标和活动的优先顺序并充分传达。	• 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：确定关键服务交付相关的依赖关系和关键职责。	• 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：确定弹性要求以支撑关键业务的交付。	• COBIT 5 DSS04.02 • ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 • NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14
	治理（ID.GV）：了解组织管理和	**ID.GV-1**：制定组织的信息安全策略。	• 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

	监控其监管、法律、风险、环境和运营方面的要求所采取的政策、程序和流程，并将网络安全风险告知管理人员。		• 所有族内的 NIST SP 800-53 Rev. 4 -1 安全控制措施
		ID.GV-2：协调信息安全角色和职责，使其与内部角色和外部合作伙伴密切合作。	• 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：了解并管理法律和监管要求，包括隐私和公民自由义务。	• COBIT 5 MEA03.01, MEA03.04 • ISA 62443-2-1:2009 4.4 3 7 • 所有族（不包括 PM-1）内的 NIST SP 800-53 Rev. 4 -1 安全控制措施
		ID.GV-4：通过治理以及风险管理流程实现网络安全风险的管控。	• 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）：组织了解与组织运营（包括任务、职责、形象或声誉）、组织资产和个人相关的网络安全风险。	**ID.RA-1**：识别资产漏洞并记录。	• CCS CSC 4 • COBIT 5 AP012.01, AP012.02, AP012.03, AP012.04 • 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接收威胁和漏洞信息。	• 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：识别内部和外部威胁并记录。	• COBIT 5 AP012.01, AP012.02, AP012.03, AP012.04 • 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：识别潜在业务影响及各种可能出现的情况。	• 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：综合考虑各种威胁、漏洞、可能出现的情况和各种影响，确定网络安全风险。	• COBIT 5 AP012.02 • ISO/IEC 27001:2013 A.12.6.1 • NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16
		识别风险响应并对其进行排序。	• COBIT 5 AP012.05, AP013.02 • NIST SP 800-53 Rev. 4 PM-4, PM-9
	风险管理战略（ID.RM）：确定组织的各种优先顺序、约束、风险承受能力和设想，并将这些信息用于为运营风险决策提供支持。	**ID.RM-1**：制定并管理风险管理流程，并征得组织的利益主体的一致同意。	• 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：确定组织的风险承受能力并对其进行清晰传达。	• 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：组织的关键基础设施的角色或风险分析部门对组织确定的风险承受能力进行传达。	• NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14
防护	访问控制	PR.AC-1：为授权设	• CCS CSC 16

（PR）	（PR.AC）：仅授权用户、流程、设备、活动和交易可访问资产和相关设施。	备和用户提供身份和凭证管理。	• 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.9.2.4, 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, PE- 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 • NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20
		PR.AC-4：管理访问权限，最小特权原则和职责分离原则并用	• 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：保护网络完整性，进行适当的网络隔离	• 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
	安全意识与培训（PR.AT）：为组织人员和合作伙伴提供网络安全教育。在接受足够的培训后可根据相关相关政策、程序和协议，履行信息安全职责。	PR.AT-1：通知用户，并提供培训	• CCS CSC 9 • COBIT 5 AP007.03, BAI05.07 • ISA 62443-2-1:2009 4.3.2 4.2 • ISO/IEC 27001:2013 A.7.2.2 • NIST SP 800-53 Rev. 4 AT-2, PM-13
		PR.AT-2：特权用户了解其角色和职责	• CCS CSC 9 • COBIT 5 AP007.02, 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 • NIST SP 800-53 Rev. 4 AT-3, PM-13

		PR.AT-3：第三方利益主体（如供应商、客户、合作伙伴等）了解其角色和职责	• CCS CSC 9 • COBIT 5 AP007.03, AP010.04, AP010.05 • 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：高级主管了解其角色和职责	• CCS CSC 9 • COBIT 5 AP007.03
			• 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-3, 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, • NIST SP 800-53 Rev. 4 AT-3, PM-13
	数据安全（PR.DS）：依据企业风险战略管理信息和记录（数据），保护信息的保密性、完整性和可用性。	PR.DS-1：保护休眠数据	• 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 • NIST SP 800-53 Rev. 4 SC-28
		PR.DS-2：保护传输数据	• 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, A.14.1.2, A.14.1.3 • NIST SP 800-53 Rev. 4 SC-8
		PR.DS-3：在资产移除、转让和处置过程中，有效管理资产	• 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 • NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16
		PR.DS-4：保持足够容量，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
			• NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5
		PR.DS-5：防止数据	• CCS CSC 17

		泄露	• COBIT 5 AP001.06 • 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.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 • NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6：采用完整性检查机制，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:开发测试环境与生产环境分离	• COBIT 5 BAI07.04 • ISO/IEC 27001:2013 A.12.1.4 • NIST SP 800-53 Rev. 4 CM-2
	信息保护流程与工序（PR.IP）：维护安全策略（涉及目的、范围、角色、职责、管理承诺和组织实体之间的协调）、流程与工序，并应用安全策略对信息系统和资产保护进行管理	PR.IP-1：创建和维护信息技术/工控系统的基线配置	• 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:执行系统开发生命周期管理流程	• COBIT 5 AP013.01 • 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
			• 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：有配置更改控制流程	• 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, SA-10
		PR.IP-4：周期性进行信息备份，并对此种备份进行维护和测试	• 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 A12 31, A.17.1.2A.17.1.3, A.18.1.3 • NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9

		PR.IP-5：符合组织资产物理运营环境的相关政策和规定	• 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-13, PE-14, PE-15, PE-18
		PR.IP-6：根据策略，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.8.3.2, A.11.2.7 • NIST SP 800-53 Rev. 4 MP-6
		PR.IP-7：不断完善防护流程	• COBIT 5 APO11.06, DSS04.05 • ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 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, IR-8, PL-2, PM-6
		PR.IP-8：与适当的各方分享防护技术的有效性	• ISO/IEC 27001:2013 A.16.1.6 • NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4
		PR.IP-9：制订并管理响应计划响应计划（事件响应和业务连续性）和恢复计划（事件恢复和灾难恢复）	• 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.17.13 • NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14
		PR.IP-11：网络安全也存在于人力资源实践中（如撤销供应、人员选拔等）	• COBIT 5 AP007.01, AP007.02, AP007.03, AP007.04, AP007.05 • 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：制订并实施漏洞管理计划	• 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）：遵照策略和程序，	PR.MA-1：使用获准的可控工具，对组织资产进行维护和修	• 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

	对工控系统和信息系统组件进行维护和修理。	理，并及时记录	• NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5
		PR.MA-2：允许对组织资产进行远程维护和记录，并阻止未授权访问	• 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 • NIST SP 800-53 Rev. 4 MA-4
	防护技术（PR.PT）：根据相关的政策、程序和协议，管理技术安全解决方案的，确保系统和资产的安全性和弹性。	PR.PT-1：根据策略，管控、记录、执行和审查审计/日志记录。	• CCS CSC 14 • COBIT 5 AP011.04 • 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 2.10, 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：根据策略，保护和限制使用移动媒体	• COBIT 5 DSS05.02, AP013.01 • 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：对系统和资产进行访问控制，实行最小功能原则	• 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, AP013.01 ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 • ISO/IEC 27001:2013 A.13.1.1, A.13.2.1
检测（DE）	异常和事件（DE.AE）：及时检测异常活	DE.AE-1：建立和管理网络操作和预期数据流基线，供用户和	• COBIT 5 DSS03.01 • ISA 62443-2-1:2009 4.4 3 3

	动，了解事件的潜在影响	系统使用	• NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4
		DE.AE-2：分析被检测事件，了解攻击目标和攻击方法	• 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 • NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI- 4
		DE.AE-3：从各种来源及传感器收集、关联事件数据	• 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：判断事件的影响	• COBIT 5 APO12.06 • NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI - 4
		DE.AE-5：设置事件告警阈值	• 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
	安全连续监测（DE.CM）：在离散的时间间隔内，监测信息系统和资产，识别网络安全事件，验证保护措施的有效性。	DE.CM-1：监测网络，检测潜在的网络安全事件	• 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, CA-7, CM-3, SC-5, SC-7, SI-4 • ISA 62443-2-1:2009 4.3.3 3 8
		DE.CM-2：监测物理环境，检测潜在的网络安全事件	• NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE- 20
		DE.CM-3：监测个人行为，检测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, AU-13, CA-7, CM-10, CM-11
		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 • NIST SP 800-53 Rev. 4 SI-3
		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.12.51 • NIST SP 800-53 Rev. 4 SC-18, SI-4. SC-44
		DE.CM-6：监测外部	• COBIT 5 APO07.06

		服务供应商活动，检测潜在的网络安全事件	• 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：监测未授权人员、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：扫描漏洞	• 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）：维护和测试监测流程与工序，确保及时充分地发现异常事件	DE.DP-1：正确定义检测角色和职责，责任到人	• CCS CSC 5 • COBIT 5 DSS05.01 • ISA 62443-2-1:2009 4.4 3 1 • ISO/IEC 27001:2013 A.6.1.1 • NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14

附录 A 中有关参考资料的内容参考链接如下：

- 信息及相关技术控制目标（COBIT）：http://www.isaca.org/COBIT/Pages/default.aspx
- 网络安全协会（CCS）Top 20 重要安全控制（CSC）：http://www.counciloncybersecurity.org
- ANSI/ISA-62443-2-1 (99.02.01)-2009，《工业自动化和控制系统的安全性：建立工业自动化和控制系统安全性计划》：http://www.isa.org/Template.cfm?Section=Standards8&Template=/Ecommerce/ProductDisplay.cfm&ProductID=10243
- ANSI/ISA-62443-3-3 (99.03.03)-2013，《工业自动化和控制系统的安全性：系统安全要求和安全级别》：http://www.isa.org/Template.cfm?Section=Standards2&template=/Ecommerce/ProductDisplay.cfm&ProductID=13420
- ISO/IEC 27001，《信息技术—信息技巧—信息安全管理系统—需求》：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，《联邦信息系统和组织的安全和隐私控制》，2013 年 4 月版（2014 年 1 月 15 日更新）：http://dx.doi.org/10.6028/NIST.SP.800- 53r4.

框架核心子类别和参考资料的指定意节大体对应，并不一定包含预期的子类别结果。

附录 B：词汇表

本附件列出了文中出现的部分术语的定义。

类别	对功能的细分，体现为一个个的网络安全结果组，与计划性需求和活动密切相关，比如，“资产管理”、“访问控制”和“检测流程”类别。
关键基础设施	对美国至关重要的物理与虚拟系统和资产，该等系统和资产的缺陷或损坏将会削弱安全、国民经济安全和/或国民公共健康及安全。
网络安全	通过预防、检测和响应攻击来保护信息的过程。
网络安全事件	网络安全变化可能会影响组织运营（包括使命、能力或信誉）。
检测（功能）	规划并实施恰当的活动，识别网络安全事件。
框架	基于风险、旨在减少网络安全风险的方法，包括以下三部分：框架核心、框架对齐结果及框架执行层级。也被称之为“网络安全框架”。
框架核心	一系列的网络安全活动和关键基础设施的参考信息，是围绕特定结果进行组织的。 框架核心包括以下四类元素：功能、类别、子类别、参考资料。
框架执行层级	反映组织应对风险的方法特点，了解组织如何看待网络安全风险，以及管理风险的现有流程。
框架对齐结果	反应特定系统或组织从框架类别和子类别中的选择结果。
功能	框架的主要组件之一。这些功能为框架中的最高级别，串起基本的网络安全活动，将其划分为类别和子类别。具体来说，功能包括识别、防护、检测、响应与恢复。
识别（功能）	组织内部就管理系统、资产、数据和能力的网络安全风险形成共识。
参考资料	参考资料是关键基础设施部门常用的标准、指南及实践中的章节，描述了达到子类别要求的具体方法。
移动代码	可原封不动地运送至异构平台集合，并用相同的语义执行的程序（例如脚本、宏或其他便携式指令）。
防护（功能）	规划并实施恰当的防护措施，确保关键基础设施服务的交付。
特权用户	授权用户（因此也是信任用户），可使用普通用户未能授权使用的安全功能。
恢复（功能）	规划并实施恰当的活动，维护恢复能力计划，恢复网络安全事件中受损的功能或服务。
响应（功能）	规划并实施恰当的活动，在检测到网络安全事件时采取相应措施。
风险	实体受潜在环境或事件威胁的程度，通常被以下因素制约：（1）环境或事件发生带来的负面影响；（2）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。
子类别	对于类别的细分，体现为具体的技术及/或管理活动结果。比如，“已编目外部信息系统”、“已保护休眠数据及已调查检测系统的通知“”均为子类别。

附录 C：缩略语

本附件列出了文中出现的部分缩略语的定义。

CCS	Council on CyberSecurity	网络安全理事会
COBIT	Control Objectives for Information and Related Technology	信息及相关技术的控制目标
DCS	Distributed Control System	分布式控制系统
DHS	Department of Homeland Security	国土安全部
EO	Executive Order	行政命令
ICS	Industrial Control Systems	工控系统
IEC	International Electrotechnical Commission	国际电工委员会
IR	Interagency Report	跨部门报告
ISA	International Society of Automation	国际自动化学会
ISAC	Information Sharing and Analysis Center	信息共享与分析中心
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	国家标准和技术研究所
RFI	Request for Information	供应商信息询问表
RMP	Risk Management Process	风险管理流程
SCADA	Supervisory Control and Data Acquisition	数据采集与监控制系统
SP	Special Publication	特别刊物

提升关键基础设施网络安全框架

网络安全公益译文项目旨在分享国外先进网络安全理念，将网络安全战略性文档翻译为中文，促进国内安全组织在相关方面的思考和交流。该项目由安全加社区发起，安全加社区是国内的网络安全社区，社区欢迎网络安全人士的加入，并致力于交付网络安全问题的解决能力。