改善关键基础设施的网络安全框架

Version 1.0

国家标准与技术研究院

February 12, 2014

Table of Contents

List of Figures

List of Tables

执行摘要

美国的国家和经济安全依赖于可靠的关键基础设施功能。网络安全威胁利用关键基础设施系统日益增加的复杂性和连通性，把国家的安全，经济，公众安全和公共健康置于风险境地。类似的财务和声誉风险，网络安全风险将影响到公司的底线。它可以驱动多达费用及影响收入。它可能会损害组织的创新能力以及增加和维持客户的能力。

为了更好地处理这些风险，总统于 2013 年 2 月 12 日，颁布 13636 号行政命令：“改善关键基础设施的网络安全”，其中规定“它是美国在提高安保，安全性，商业机密，隐私和公民自由的同时，增强国家关键基础的安全性和可靠性，并维持一个鼓励高效、创新和经济繁荣的网络环境的政策“ 在颁布这项政策时，行政命令需要一个自愿的基于风险的网络安全的发展框架——一系列的工业标准和最佳实践来帮助组织管理网络安全风险项。这个框架通过政府和私营部门的合作创建，基于业务需要、以低成本方式使用通用语言来处理和管理网络安全风险，而无需对企业使用额外的管控要求。该框架着重于使用业务驱动因素，以指导网络安全的活动，并考虑网络安全风险，组织风险管理程序的一部分。该框架由三部分组成：核心框架，该框架配置文件和框架实施层级。该框架的核心是一套网络安全的活动，成果，和翔实的参考资料是通用的重要基础设施行业，为发展个人组织档案的详细指导。通过使用配置文件中，该框架将帮助组织调整其网络安全的活动，其业务需求，风险承受能力和资源。各层提供一个机制，组织查看和了解他们的方法来管理网络安全风险的特性。

该行政命令还要求该框架包括一个方法来保护个人隐私和公民自由时，重要的基础设施组织开展网络安全的活动。虽然流程和现有的需求会有所不同，该框架能够帮助组织整合的隐私和公民自由的全面网络安全计划的一部分。

该框架使组织 - 无论大小，网络安全风险程度，或网络安全的复杂性 - 原则和风险管理的最佳实践应用到改善关键基础设施的安全性和弹性。该框架提供了组织和结构到今天的多种途径，以网络安全组装标准，准则和做法，如今正在有效地业。此外，因为它引用了全球公认的标准，网络安全，该框架还可以用于由位于美国以外的组织，可以作为一个典范加强关键基础设施的网络安全国际合作。

该框架是不是一个尺寸适合所有人的方法来管理网络安全风险的关键基础设施。组织将继

续有独特的风险 - 不同的威胁，不同的弱点，不同的风险承受能力 - 以及他们如何实施该框架的行为会有所不同。组织可以决定是很重要的关键服务活动，并可以优先考虑投资，以最大限度地度过每一美元的影响。最终，该框架旨在减少和更好地管理网络安全风险。

该框架是一个活的文件，并会继续进行更新和改善，产业提供了执行的反馈。在架构上付诸实践，经验教训将被整合到未来版本。这将确保它满足关键基础设施的业主和运营商的需求在新的威胁，风险和解决方案，一个充满活力和挑战性的环境。

使用这种自愿框架是下一步要提高我们国家的关键基础设施的网络安全 - 为个别组织的指导，同时增加了国家的关键基础设施作为一个整体的网络安全态势。

1.0 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的。为了加强这一基础设施的恢复力，奥巴马总统 2 月 12 日颁布行政命令 13636 （ EO ） ， “改善关键基础设施的网络安全， ”，

对于自愿网络安全框架（ “框架” ） ，它提供了“优先，灵活，可重复，基于绩效的，和成本效益的方法”直接管理这些流程，信息和系统网络安全风险的发展这一行政命令要求参与关键基础设施服务的提供。该框架，与业界合作开发，提供指导，在管理网络安全风险的一个组织。

关键基础设施是在 EO 定义为“系统和资产，不论是物理或虚拟的，所以至关重要的美国的无行为能力或破坏这些制度和资产将会对安全，国家经济安全，国家公共健康或使人衰弱的影响安全，或该等事项的任何组合。 “由于来自外部和内部的威胁越来越大的压力，负责关键基础设施的组织需要有一个一致的，迭代的方法来识别，评估和管理网络安全风险。这种做法是必要的，无论一个组织的规模，威胁曝光或网络安全的复杂的今天。

在关键基础设施的社区，包括公共和私营业主和运营商，以及其他实体在确保国家的基础设施的作用。每个关键基础设施部门的执行委员是由信息技术支持的功能（ IT）和工业控制系统（ ICS ） .2 这依赖于技术，通信和 IT 和 ICS 的互联互通已发生变化，扩大了潜在的漏洞和潜在的增长对风险的操作。例如， ICS 和 ICS 的操作产生的数据越来越多地用于提供关键的服务和支持业务决策，一个网络安全事件对组织业务的潜在影响，资产，健康和个人安全和环境，应考虑。要管理网络安全风险，该组织的业务驱动因素和具体到它的使用 IT 和 ICS 安全考虑清楚的认识是必要的。因为每个组织的风险是独一无二的，随着其使用的 IT 和 ICS 的，用于实现由框架所描述的结果的工具和方法会有所不同。

认识到隐私和公民自由的保护，提高公众的信任所扮演的角色，执行命令要求该框架包括一个方法来保护个人隐私和公民自由时，重要的基础设施组织开展网络安全的活动。许多组织已经有了解决隐私和公民自由的过程。该方法的目的是补充这些过程，并提供

指导，以促进隐私风险管理与组织的方法，网络安全风险管理是一致的。集成的隐私和网络安全可以通过增加客户的信心，让更多的标准化的信息共享，并在法律制度简化操作获益的组织。

---

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

为确保可扩展性，使技术创新，架构是技术中立的。该框架依赖于各种现有的标准，准则和措施，使关键基础设施供应商，实现弹性。依靠这些全球性的标准，指南和开发，管理，及行业更新的做法，可实现的成果框架的工具和方法将规模跨越国界，承认网络安全风险的全球性，并发展与技术的进步和业务要求。利用现有的和新兴的标准，使规模经济和推动有效的产品，服务和实践，满足确定市场需求的发展。

市场竞争也促进了这些技术和做法，实现了利益相关者，这些行业很多好处更快的传播。

从这些标准，准则和惯例建立，框架提供了常用的分类和机制组织：

1）形容自己目前网络安全的姿势;

2）描述自己的目标状态，网络安全;

3）确定并优先用于连续和重复的过程的范围内改善的机会;

4）评估向目标状态的进展;

5）沟通有关网络安全风险的内部和外部利益相关者之间。

该框架的补充，而不会取代，一个组织的风险管理流程和网络安全方案。该组织可以利用其现有流程，并充分利用该框架来寻找机会，加强和沟通的网络安全风险的管理，同时与行业惯例调整。可替换地，不具有现有的网络安全方案的组织可以使用框架作为基准，建立 1 。

正如框架不是特定行业，标准，准则和惯例的通用分类法，它也提供了不特定国家。在美国以外的机构也可以使用框架来加强自身的网络安全的努力，以及该框架可以促进发展的共同语言对关键基础设施的网络安全国际合作。

1.1 在视图框架工作

该框架是一个基于风险的方法来管理网络安全风险，并且由三部分组成：核心框架，该框架的实施层级和架构配置文件。每个框架组件强化业务驱动和网络安全的活动之间的联系。下面这些部件进行说明。

- •该框架的核心是一套网络安全的活动，期望的结果，而且是通用的关键基础设施部门适用的参考。核心呈现的方式，允许对网络安全的活动的沟通和跨组织的成果从行政级别来实施/运营层面的行业标准，准则和惯例。该框架的核心是由五个并发和连续函数，确定，保护，检测，响应，恢复的。当一起考虑，这些功能提供了网络安全风险的一个组织的管理生命周期的一个高层次的，战略的眼光。该框架的核心，然后确定相关主要类别和子类别的每个功能，并以实例参考性文献，如现有标准，指南，并为每个子目录的做法符合他们。

- •框架实施层级（“层”）提供上下文对一个组织如何观看网络安全风险，并在适当的程序来管理风险。层描述的程度，一个组织的网络安全风险管理实践中表现出的框架（如，风险和威胁感知，可重复和自适应）所定义的特征。这些层在一定范围内表征一个组织的做法，从部分（第 1 层），以自适应（第 4 层）。这些层级反映非正式的，无响应的进程来是敏捷和风险告知的方法。在第一级选择过程中，组织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/任务目标和组织约束。

- •一个框架配置文件（“档案”）代表需要一个组织已经从框架类别和子类别选择的基于业务的成果。配置文件可以被定性为标准，准则和惯例的对齐方式 Framework 核心在一个特定的实施方案。配置文件可用于通过比较“当前”个人资料以确定改进网络安全姿势的机会（在“按原样”状态）与“目标”个人资料（在“是”的状态）。要开发一个配置文件，一个组织可以查看所有类别和子类别，并根据业务驱动因素和风险评估，确定哪些是最重要的，他们可以根据需要来满足组织的风险增加类别和子类别。当前配置文件可以被用来支持优先级和向着目标配置文件进度测量，而在其他的业务需求，包括成本效益和创新保理。配置文件可以被用来进行自我评估，并在组织内部或组织之间的沟通。

1.2 风险管理换货和网络安全工作框架

风险管理是识别，评估和应对风险的持续过程。管理风险，企业应该明白，将会发生一个事件的可能性和由此产生的影响。有了这些信息，企业可以决定可接受的风险水平提供服务，并可以表达这是他们的风险承受能力。

随着风险承受能力有所了解，企业可以优先考虑网络安全的活动，使企业能够做出关于网络安全支出明智的决定。

风险管理计划的实施提供了组织量化和沟通调整其网络安全计划的能力。组织可以选择处理以不同的方式，包括减轻风险，转移风险，从而避免了风险，或接受的风险，这取决于对关键服务的递送的潜在影响的风险。

该框架使用的风险管理流程，使组织有关网络安全通知和优先决定。它支持经常性的风险评估和业务驱动的验证，以帮助企业选择目标国家网络安全的活动，反映了期望的结果。因此，该框架使企业能够动态地选择和网络安全风险管理为 IT 和 ICS 的环境中直接改善的能力

该框架是自适应，提供一个灵活的，基于风险的实现，它可以与网络安全风险管理过程的一系列广泛使用。网络安全风险管理流程的例子包括国际标准化组织（ ISO ）31000:20093， ISO / IEC 27005:20114，国家标准与技术研究所（ NIST）的特别出版物（SP ） 800-395，以及电力界别分组网络安全风险管理流程（ RMP） guideline6 。

1.3 文档概述

本文档的其余部分包含以下章节和附录：

- •第 2 节描述了框架的组成部分：框架核心的层级，以及配置文件。
- •第 3 节介绍了该框架可以使用的例子。
- •附录 A 给出了核心框架以表格格式：的功能，类别，子类别，并参考性文献。
- •附录 B 中包含选定的术语表。
- •附录 C 列出本文件中用到的缩写词。

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

2.0 基本框架

该框架提供了一种共同语言的理解，管理，以及内部和外部表达网络安全风险。它可以用来帮助识别和优先降低网络安全风险的行动，这是调整政策，业务和技术方法来管理这种风险的工具。它可用于在整个组织管理的网络安全风险，或者它可以集中在一个组织内的输送关键服务。不同类型的实体 - 包括部门的协调机构，协会和组织 - 可以使用框架为不同的目的，包括建立共同的配置文件中。

2.1 框架的核心

该框架核心提供了一组活动，以实现特定的网络安全成果，并指导参考实例来实现这些成果。核心是不是要执行的操作清单。它提出了确定行业管理网络安全风险的有益网络安全的关键成果。核心包括四个要素：功能，类别，子类别，并参考性文献，如图 1 所示：

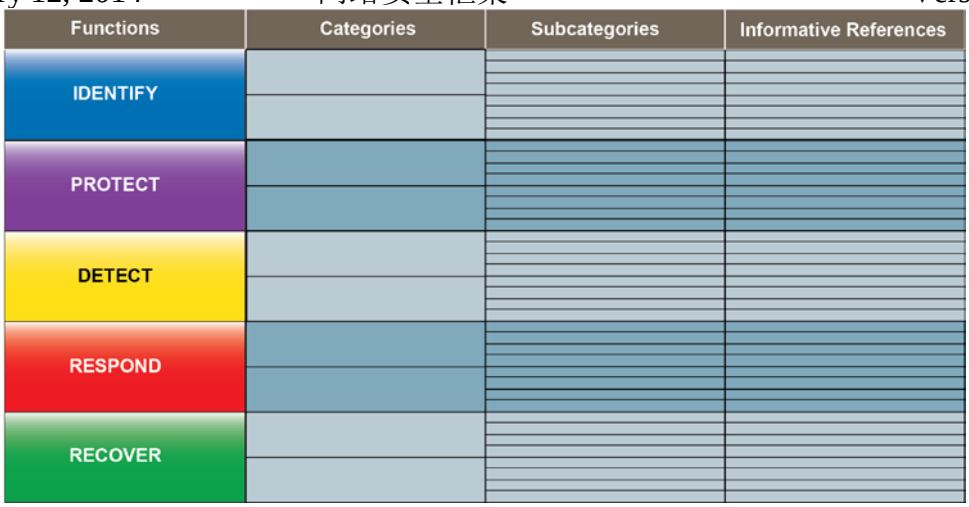

Figure 1: Framework Core Structure

该框架的核心元素结合在一起的工作方式如下：

- •功能组织基本的网络安全活动的最高水平。这些功能是识别，保护，检测，响应和恢复。他们帮助一个组织中表达的网络安全风险及其通过组织信息化管理，使风险管理决策，应对威胁，并从以往的活动学习提高。该功能还配合现有方法的事件管理和帮助表示投资的网络安全带来的影响。例如，在规划和演习的投资支持及时响应和恢复行动，导致对服务的交付减少的影响。
- •分类是一个功能的细分到网络安全的成果紧密联系在一起的纲领性需求和特定活动的团体。类别的例子包括“资产管理”，“访问控制”和“检测过程。 ”
- •子类别进一步划分一个类别为技术和/或管理活动的具体成果。他们提供了一个结果集，虽然并不详尽，帮助支持实现在每个类别的成果。子类别的例子包括：“外部信息系统进行编目”，“数据的静止是被保护的”，和“从检测系统通知进行了研究。 ”
- •参考性文献的标准，准则和关键基础设施部门，说明的方法，以实现与各子类别相关的结果之间的共同做法的具体章节。在核心框架提出的参考性文献是说明性的，并非详尽无遗。他们是基于跨部门的指导框架开发 process.7 过程中最经常被引用的

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，或导致静态理想的

最终状态。相反，该函数可以同时和连续地进行，以形成解决了动态网络安全风险的操作培养。见附录 A 的完整框架核心上市。

- •识别 - 开发组织的理解来管理网络安全风险的系统，资产，数据和功能。
- 在识别功能的活动是基本有效使用框架。了解业务环境，支持关键职能的资源，以及相关的网络安全风险，使组织能够集中和优先努力，凭借其风险管理策略和业务需求保持一致。此功能在结果分类的例子包括：资产管理，商业环境，治理，风险评估，以及风险管理策略。
- •保护 - 制定并实施相应的保障措施，以确保提供重要的基础设施服务。
- 保护功能支持限制或含有潜在的网络安全事件的影响的能力。此功能在结果分类的例子包括：访问控制，意识和培训，数据安全，信息保护流程和程序;维护;和保护技术。
- •检测 - 制定并实施适当的活动，以识别网络安全事件的发生。
- 该检测功能能够及时发现网络安全事件。此功能在结果分类的例子包括：异常和事件;安全连续监测，以及检测过程。
- •响应 - 制定并实施适当的活动，以采取有关检测到的网络安全事件的行动。

[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/.

该响应函数支持包含一个潜在的网络安全事件的影响的能力。此功能在结果分类的例子包括：响应计划;通讯，分析，减灾;和改进。

•恢复 - 制定并实施适当的活动，以保持计划的弹性和还原是由于网络安全事件受损的任何功能或服务。

该恢复功能支持及时恢复到正常的操作，以减少从网络安全事件的影响。此功能在结果分

类的例子包括：恢复规划;改进;和通信。

2.2 框架实现层级

该框架的实施层级（“层”）提供上下文对一个组织如何观看网络安全风险，并在适当的程序来管理风险。该层级的范围从部分（第 1 层），以自适应（第 4 层），并描述了严谨和复杂的程度增加网络安全的风险管理做法，其网络安全风险管理是由业务需求了解并集成到一个组织的整体风险程度管理实践。风险管理的考虑因素包括网络安全的许多方面，包括其隐私和公民自由方面的考虑都融入的网络安全风险和潜在的风险应对组织的管理程度。

第一级选择过程中考虑企业当前的风险管理做法，威胁环境，法律和监管规定，业务/任务目标和组织约束。组织应确定所需的第一级，以确保所选择的级别是否符合组织的目标，是贯彻落实可行的，并降低网络安全风险的重要资产和资源，以接受该组织的水平。组织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，或其他来源获得的，以帮助确定自己想要的层外部指导。

虽然组织认定为一级（部分）鼓励将考虑转向方法 2 或更大，层级并不代表成熟度级别。发展到更高层级的鼓励时，这样的改变会降低网络安全风险，并符合成本效益。成功实施该框架是基于成就组织的目标配置文件（S ），而不是在一线的决心所描述的结果时。

该层定义如下：

第 1 级：部分

•风险管理程序 - 组织网络安全风险管理实践没有正式的，而且风险是在一个特设有时无的方式进行管理。网络安全的活动的优先顺序，不得直接告知组织风险的目标，威胁环境，或业务/任务需求。

•集成的风险管理计划 - 目前的网络安全风险在组织层面认识有限和整个组织的方法来管理网络安全风险尚未确定。组织实施对不规则，逐案基础上，由于丰富的经验，或从外部来源获得的信息网络安全风险管理。该组织可能没有流程，使网络安全信息可在组织内共享。

•外部参与 - 一个组织可能没有到位的过程中参与的协调或协作与其他实体。

第 2 层：风险知情

•风险管理流程 - 风险管理实践均经管理层批准，但可能不被确立为组织范围的策略。网络安全的活动的优先顺序是直接告知组织风险的目标，威胁环境，或业务/任务需求。

•集成的风险管理计划 - 目前的网络安全风险在组织水平，但全组织的方法来管理网络安全风险尚未建立的意识。风险告知，管理层批准的过程和程序都定义和实现，以及工作人员有足够的资源来履行其网络安全的职责。网络安全信息上非正式地在组织内共享。

•外部参与 - 组织知道它在更大的生态系统的作用，但还没有正式确定了其功能，对外交流和共享信息。

第 3 层：可重复

•风险管理程序 - 该组织的风险管理做法被正式批准，并表示为政策。组织网络安全的做法是定期更新的基础上的风险管理程序的应用，以改变业务/任务要求和不断变化的威胁和技术的景观。

•集成的风险管理计划 - 有一个组织范围内的方法来管理网络安全风险。是风险告知政策，流程和程序中定义，实现为目的，并审查。一致的方法已到位，有效地改变应对风险。人员具备的知识和技能，以履行其指定的角色和责任。

•外部参与 - 组织了解其依赖关系和合作伙伴，并从这些合作伙伴，使协作和组织内部基于风险的管理决策响应事件接收信息。

第 4 级：自适应

•风险管理流程 - 基于经验教训，并从以往和当前网络安全的活动所产生的预测指标，该组织适应其网络安全的做法。通过不断完善结合先进的网络安全技术和实践的过程中，组织积极适应不断变化的网络安全景观和响应不断变化，并及时复杂的安全威胁。

•集成的风险管理计划 - 有一个组织范围内的方法来管理使用风险告知政策，流程和程序，以解决潜在的网络安全事件的网络安全风险。网络安全风险管理是组织文化的一部分，从以前的活动，通过其他渠道共享信息，并在他们的系统和网络活动的意识不断的认识演进。

•外部参与 - 组织管理风险，并积极分享信息与合作伙伴，以确保准确，及时的信息的分发和消费的一个网络安全事件发生之前，以改善网络安全。

2.3 框架简介

该框架配置文件（“档案”）是函数，类别和子类别的业务需求，风险承受能力，以及资源组织的对齐方式。一个侧影使组织能够建立一个路线图，降低网络安全风险，是很好用的组织和部门的目标一致，认为法律/法规要求和行业最佳实践，并体现了风险管理的优先事项。鉴于许多组织的复杂性，他们可以选择有多个配置文件，特别组件，并认识他们的个人需求保持一致。

框架配置文件可以用来形容当前的状态或特定的网络安全活动所需的目标状态。当前配置文件的指示，目前正在取得的网络安全成果。目标资料表明以实现所需的网络安全风险管理目标所需要的结果。配置文件支持业务/任务需求，并有助于风险的内部和组织之间的沟通。此框架文件没有规定个人资料模板，允许在实施的灵活性。

配置文件（例如，当前配置和目标配置文件）的比较可发现差距加以解决，以满足网络安全的风险管理目标。一项行动计划，以解决这些差距可以促进上述路线图。减缓差距的优先次序是由组织的业务需求和风险管理流程驱动的。这种基于风险的方法使组织能够衡量资源估算（如人员，资金）来实现具有成本效益的，优先的方式网络安全的目标。

2.4 协调框架的实施

图 2 描述的信息，并决定组织内部的共同流量为以下几个层次：

•执行

•业务/流程

•实施/运营

行政级别通信的任务优先级，可利用的资源，以及整体风险承受能力到业务/流程层面。业务/流程层面使用信息作为输入到风险管理过程，然后与合作的实施/运营级通信业务需求，并创建一个配置文件。实施/运营级通信的个人资料实施进展情况向业务/流程层面。业务/流程层面使用这些信息来进行影响评估。业务/流程层面的管理报告，影响评估的结果，以行政级别来通知该组织的整体风险管理程序，并实施/操作对业务的影响的认识水平。

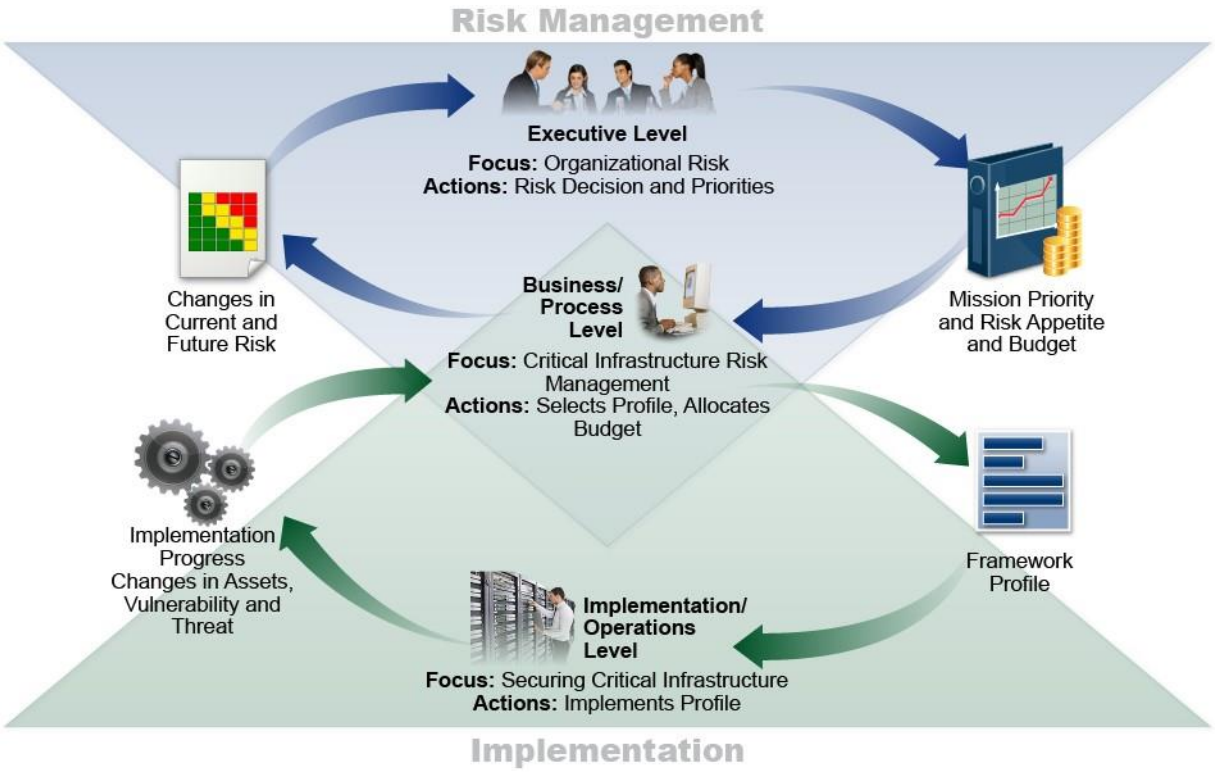

Figure 2: Notional Information and Decision Flows within an Organization

3.0 如何使用框架

一个组织可以使用该框架作为其系统的过程的一个关键部分进行识别，评估和管理网络安全风险。该框架的目的不是要取代现有的流程，组织可以使用其当前进程和覆盖其上的框架，以确定差距，其目前的网络安全风险的方法，并制定路线图的改进。利用该框架作为一个网络安全的风险管理工具，一个组织可以判断是最重要的，关键的服务提供活动和优先支出，以最大限度地提高投资的影响。

该框架的目的是补充现有业务和网络安全业务。它可以作为一个新的网络安全方案或机制以改善现有程序的基础。该框架提供了一种表达网络安全要求与业务合作伙伴和客户的一种手段，可以帮助确定一个组织的网络安全实践的差距。它还提供了一个一般设置注意事项和流程考虑在网络安全程序的上下文隐私和公民自由问题。

以下各节介绍不同的方法，使组织可以使用该框架。

3.1 基本审查网络安全实践

该框架可用于与本框架的核心概括比较组织当前网络安全的活动。通过创建一个当前的配置文件，组织可以检查它们所实现的核心类别和子类别描述的结果，与五高层次的功能一致的程度：识别，保护，检测，响应和恢复。一个组织可能会发现它已经达到理想的结果，因此，网络安全管理与已知的风险相称。相反，一个组织可以判定它有机会（或需要）提高。该组织可以利用这些信息来制定一项行动计划，以加强现有的网络安全实践，并降低网络安全风险。一个组织也可能会发现，它是过度投资达到一定的成果。该组织可以使用此信息来重新确定优先次序资源，加强网络安全的其他行为。

虽然他们并不能取代风险管理程序，这五个高水平的功能将会对高级管理人员和其他人提供了一个简洁的方式来提炼的网络安全风险的基本概念，使他们能够评估如何识别风险的管理，以及如何组织他们的书库在高达针对现有网络安全标准，准则和惯例的高水平。该框架还可以帮助企业回答的基本问题，包括“是怎样的呢？”然后，他们可以在一个更明智的方式来加强其网络安全的做法认为有必要在何时何地移动。

3.2 建立或完善一个网络安全计划

下面的步骤说明如何组织可以使用该框架来创建一个新的网络安全程序或改进现有的程序。应重复这些步骤，要不断提高网络安全。

第 1 步：优先和范围。该组织确定其业务/任务目标和高层次的组织优先事项。有了这些信息，组织公司对于网络安全的实现战略决策，并确定系统和支持选定的业务线或过程资产的范围。该框架可适应以支持组织内的不同业务线或过程，也可以有不同的业务需求和相关的风险承受能力。

第 2 步：东方。一旦网络安全方案的范围已确定为业务线或过程，组织确定了相关制度和资产，监管要求和整体风险的方法。然后，组织识别威胁，而且，这些系统和资产脆弱性。

第 3 步：创建一个当前配置文件。该组织通过指示其分类，并从框架核心子目录成果，目前正在实现开发一个当前配置文件。

第 4 步：进行风险评估。这项评估可能由该组织的整体风险管理过程中或以前的风险评估活动的指导。该组织分析经营环境，以识别一个网络安全事件的可能性和该事件可能对组织的影响。重要的是，组织争取把新的风险和威胁和漏洞数据，以便充分理解的可能性和网络安全事件的影响。

第 5 步：创建目标配置文件。该组织创建目标配置文件，侧重于框架类别和子类别描述了组织的期望的网络安全成果的评估。组织也可以开发自己的额外的类别和子类别占到独特的组织风险。创建目标配置文件时，该组织也可考虑影响和外部利益相关者的要求，如部门实体，客户和业务合作伙伴。

第 6 步：确定，分析和优先差距。该组织比较了当前配置和目标配置文件，以确定差距。接着，它会创建一个优先行动计划，以解决这些差距的借鉴使命的驱动程序，成本/效益分析，以及对风险的理解，以达到在目标配置文件的结果。该组织然后确定需要解决的差距的资源。以这种方式使用配置文件使组织能够做出有关网络安全的活动明智的决定，支持风险管理，使组织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。该组织决定要采取的措施的问候的间隙，如果有的话，在先前步骤中确定的。然后它会监视对目标配置文件目前网络安全的做法。为进一步指导，框架识别有关类别和子类别的例子参考性文献，但组织应确定哪些标准，准

则和做法，包括那些特定行业，最适合他们的需要。

根据需要不断评估和改进其网络安全的组织可能会重复这些步骤。例如，组织可能会发现，东方步骤更加频繁重复提高风险评估的质量。此外，组织可以通过迭代更新到当前的配置文件监测进展情况，随后比较当前配置文件到目标配置文件。组织也可以利用这个过程来自己理想的框架实现层调整其网络安全计划。

3.3 通信网络安全需求与利益相关者

该框架提供了一个共同的语言进行沟通负责必不可少的关键基础设施服务的提供相互依存的利益相关者的要求。实例包括：

•一个组织可能利用目标配置文件来表达网络安全风险管理要求，外部服务提供商（例如，一个云提供商它所导出的数据）。

•一个组织可以通过当前的配置文件表示其网络安全状态报告结果或与收购的要求进行比较。

•一个重要的基础设施所有者/经营者，在确定对其中的基础设施依赖外部合作伙伴，可以使用目标配置文件来传达所需的类别和子类别。

•一个重要的基础设施部门可以设立一个目标配置文件，可以使用它的成分中作为一个初始基线资料，以建立自己的定制目标配置文件。

3.4 确定新的机遇或修订的规范性参考文献

该框架可用于识别新的或修订的标准，准则或惯例在附加参考性文献，将有助于企业满足新的需求机会。实现给定的子类别，或开发新的子类别的组织，可能会发现，有一些参考性文献，如果有的话，对于相关的活动。为了满足这一需求，该组织可能会与技术带头人和/或标准组织起草，制定，协调标准，准则或惯例进行合作。

3.5 方法来保护隐私和公民自由

本节介绍了所要求的行政命令来解决个人隐私和公民自由的影响，可能导致网络安全业务的一种方法。这种方法的目的是因为隐私和公民自由的影响可能会有所不同部门或随着时间的推移和组织可以解决这些方面的考虑和流程，一系列的技术实现一般设置注意事项和流程。然而，在一个网络安全方案并非所有的活动，可能这些

因素引起。符合第 3.4 节，技术保密标准，准则和其他最佳做法可能需要开发支持改进的技术实现。

当个人信息的使用，收集，处理，保存，或与一个组织的网络安全活动有关的披露可能出现的隐私和公民自由问题。那熊隐私或公民自由方面的考虑活动的一些例子可能包括：网络安全的活动，导致过度采集或过度保留的个人信息;披露无关的网络安全活动的个人信息或使用，这导致拒绝网络安全减灾活动服务或其他类似的潜在的不利影响，包括活动，如某些类型的事件检测或监测可能影响言论或结社的自由。

政府的政府和代理商有直接的责任，以保护网络安全的活动所产生的公民自由。参考下文的方法，政府或拥有或经营的关键基础设施，政府的代理人应该有一个过程，以支持遵守适用的隐私法律，法规和宪法要求网络安全的活动。

为了解决隐私问题，企业可以考虑怎么样，而该等措施是适当的，他们的网络安全程序可能包含隐私原则，例如：尽量减少数据的收集，披露和保留相关的网络安全事件的个人信息资料的;使用限制对专门针对网络安全的活动收集的任何信息网络安全的活动外，对某些网络安全的活动的透明度;个人同意和补救措施的使用在网络安全活动的个人信息而产生的不利影响;数据质量，完整性和安全性，以及问责制和审计。

随着组织评估框架核心附录 A 中，下列过程和活动可被视为一种手段，以解决上面提到的隐私和公民自由的含义：

的网络安全风险治理

•网络安全的风险的一个组织的评估和潜在的风险应对措施考虑其网络安全计划的隐私问题

•个人与网络安全相关的隐私责任报告适当的管理和相应培训

•过程是否到位，以支持遵守适用的隐私法律，法规和宪法规定的网络安全活动

•过程是否到位，以评估实施上述组织措施和控制

途径识别和授权的个人访问组织资产和系统

•采取措施以识别和解决访问控制措施的隐私问题的范围内，它们涉及个人信息的收集，披露，使用或意识和培训措施

•从组织的隐私政策适用的信息包含在网络安全工作人员的培训和宣传活动

•服务提供商为组织提供网络安全相关的服务都被告知该组织的适用的隐私政策

异常活动的检测以及系统和资产监控

•过程是否到位进行组织的异常活动的检测和网络安全监控的隐私审查

应对活动，包括信息共享或其他减灾工作

•过程是否到位，评估和应对是否，何时，如何，以及在何种程度上的个人信息在组织外部共享作为网络安全信息共享活动的一部分

•过程是否到位进行组织的网络安全减灾努力的隐私审查

附录 A：核心框架

本附录介绍了核心框架：功能，类别，子类别，以及描述具体的网络安全活动，是通用的所有关键基础设施部门参考性文献的列表。为框架核心所选择的演示文稿格式不提出一个具体的实施顺序或暗示的学位类别，子类别，并参考性文献的重要性。本附录中给出的框架核心代表一组通用的管理网络安全风险的活动。而框架并不详尽，它是可扩展的，允许组织，部门和其他实体使用子类别和参考性文献是成本效益和效率，使他们能够管理自己的网络安全风险。活动可以从核心框架在配置文件创建过程中选择和额外的类别，子类别，并参考性文献可以被添加到配置文件。一个组织的风险管理流程，法律/监管规定，业务/任务目标，并组织约束引导配置文件创建在这些活动的选择。个人信息被认为是评估安全风险和保护时，在分类中引用的数据或资产的一个组成部分。

而在功能方面，分类和子类别确定的预期结果是相同的 IT 和 ICS 的，因为它的作战环境和注意事项和 ICS 不同。 ICS 对现实世界中的直接作用，包括对健康和个人安全的潜在风险，以及对环境的影响。此外， ICS 与它比较独特的性能和可靠性要求，以及安全和效率的目标必须实现网络安全的措施时，必须考虑。

为便于使用，该框架核心的每个组件被赋予一个唯一的标识符。功能和类别都有一个唯一字母标识符，如表 1 所示。每个类别内的子类别进行了数值引用;每个子类别的唯一标识符被包括在表 2 中。

有关框架的其他证明材料可在 NIST 网站上的 http://www.nist.gov/cyberframework/找

到。

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

表 2：框架核心

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	• **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: Software platforms and applications within the organization are inventoried	• **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: Organizational communication and data flows are mapped	• **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, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	• **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: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and	• **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
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers	• **COBIT 5** APO01.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1

Function	Category	Subcategory	Informative References
			• **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-
	The organization's objectives, stakeholders, activities are understood prioritized; this information used to inform roles, responsibilities, and management decisions.	supply chain is identified and communicated	• **COBIT 5** APO08.04, APO08.05, 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: The organization's place in critical infrastructure and its industry sector is identified and	• **COBIT 5** APO02.06, APO03.01 • **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are	• **COBIT 5** APO02.01, APO02.06, APO03.01 • **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	• **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: Resilience requirements to support delivery of critical services are established	• **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,
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of	**ID.GV-1:** Organizational information security policy is established	• **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: Information security roles & responsibilities are coordinated and aligned with	• **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: Legal and regulatory requirements regarding	• **COBIT 5** MEA03.01, MEA03.04 • **ISA 62443-2-1:2009** 4.4.3.7

Function	Category	Subcategory	Informative References
		including privacy and civil liberties obligations, are understood and managed	• **ISO/IEC 27001:2013** A.18.1 • **NIST SP 800-53 Rev. 4** -1 controls from all families (except PM-1)
		ID.GV-4: Governance and risk management processes address	• **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
	organization understands cybersecurity risk to organizational operations (including mission, image, or reputation), organizational assets, and individuals.	identified and documented	• **CCS CSC** 4 • **COBIT 5** APO12.01, APO12.02, APO12.04 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 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, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and	• **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 • **ISO/IEC 27001:2013** A.6.1.4
		ID.RA-3: Threats, both internal and external, are identified and documented	• **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
		ID.RA-4: Potential business impacts and likelihoods are	• **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-
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	• **COBIT 5** APO12.02 • **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** RA-2, RA-3,
		ID.RA-6: Risk responses are	• **COBIT 5** APO12.05, APO13.02

Function	Category	Subcategory	Informative References
		prioritized	• **NIST SP 800-53 Rev. 4** PM-4, PM-9
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational	• **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: Organizational risk tolerance is determined and clearly	• **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: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific	• **NIST SP 800-53 Rev. 4** PM-8, PM-9, PM-11, SA-14
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated is limited to authorized users, processes, or authorized activities and transactions.	managed for authorized devices and users	• **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 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
		managed and protected	• **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-5, PE-6, PE-9
		PR.AC-3: Remote access is managed	• **COBIT 5** APO13.01, DSS01.04, • **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

Function	Category	Subcategory	Informative References
			• **NIST SP 800-53 Rev. 4** AC-17, AC-19,
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	• **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: Network integrity is protected, incorporating network segregation where appropriate	• **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
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies,	**PR.AT-1:** All users are informed and trained	• **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 • **NIST SP 800-53 Rev. 4** AT-2, PM-13
		PR.AT-2: Privileged users understand roles & responsibilities	• **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 • **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles &	• **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
		PR.AT-4: Senior executives understand roles & responsibilities	• **CCS CSC** 9 • **COBIT 5** APO07.03

Function	Category	Subcategory	Informative References
			• **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: Physical and information security personnel understand roles & responsibilities	• **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
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	• **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: Data-in-transit is protected	• **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: Assets are formally managed throughout removal, transfers, and disposition	• **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: Adequate capacity to ensure availability is maintained	• **COBIT 5** APO13.01 • **ISA 62443-3-3:2013** SR 7.1, SR 7.2 • **ISO/IEC 27001:2013** A.12.3.1

Function	Category	Subcategory	Informative References
			• **NIST SP 800-53 Rev. 4** AU-4, CP-2,
		PR.DS-5: Protections against data leaks are implemented	• **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.9.1.2, 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, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SI-4
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and	• **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
		PR.DS-7: The development and testing environment(s) are separate from the production environment	• **COBIT 5** BAI07.04 • **ISO/IEC 27001:2013** A.12.1.4 • **NIST SP 800-53 Rev. 4** CM-2
	Processes and Procedures (PR.IP): Security policies commitment, and among organizational processes, and procedures maintained and used to protection of information and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	• **CCS CSC** 3, 10 • **COBIT 5** BAI10.01, BAI10.02, 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-5, CM-6, CM-7, CM-9, SA-10
		Cycle to manage systems is implemented	• **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

Function	Category	Subcategory	Informative References
			• **NIST SP 800-53 Rev. 4** SA-3, SA-4, SA-8, SA- 10, SA-11, SA-12, SA-15, SA-17,
		processes are in place	• **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: Backups of information are conducted, maintained, and tested periodically	• **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** A.12.3.1. • **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-
		the physical operating environment organizational assets are met	• **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
		policy	• **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
		continuously improved	• **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,

Function	Category	Subcategory	Informative References
			8, PL-2, PM-6
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	• **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
		PR.IP-9: Response plans (Incident Response and Business Continuity) recovery plans (Incident Recovery Disaster Recovery) are in place and managed	• **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: Response and recovery plans are tested	• **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-
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	• **COBIT 5** APO07.01, APO07.02, 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, • **NIST SP 800-53 Rev. 4** PS Family
		PR.IP-12: A vulnerability management plan is developed and	• **ISO/IEC 27001:2013** A.12.6.1, A.18.2.2 • **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-
	Maintenance (PR.MA): industrial control and system components is consistent with policies procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and	• **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,
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	• **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

Function	Category	Subcategory	Informative References
			• **NIST SP 800-53 Rev. 4** MA-4
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	• **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 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
		PR.PT-2: Removable media is protected and its use restricted according to policy	• **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: Access to systems and assets is controlled, incorporating the principle of least functionality	• **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 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR • **ISO/IEC 27001:2013** A.9.1.2 • **NIST SP 800-53 Rev. 4** AC-3, CM-7
		PR.PT-4: Communications and control networks are protected	• **CCS CSC** 7 • **COBIT 5** DSS05.02, APO13.01 • **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8,

Function	Category	Subcategory	Informative References
			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, AC-18, CP-8, SC-7
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	• **COBIT 5** DSS03.01 • **ISA 62443-2-1:2009** 4.4.3.3 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	• **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
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	• **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: Impact of events is determined	• **COBIT 5** APO12.06 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI - 4
		DE.AE-5: Incident alert thresholds are established	• **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
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	• **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
		DE.CM-2: The physical	• **ISA 62443-2-1:2009** 4.3.3.3.8

Function	Category	Subcategory	Informative References
		monitored to detect potential cybersecurity events	• **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20
		DE.CM-3: Personnel activity is monitored to detect potential	• **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: Malicious code is detected	• **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: Unauthorized mobile code is detected	• **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-
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity	• **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: Monitoring for unauthorized personnel, connections, devices, and software	• **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: Vulnerability scans are performed	• **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
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure	• **CCS CSC** 5 • **COBIT 5** DSS05.01 • **ISA 62443-2-1:2009** 4.4.3.1 • **ISO/IEC 27001:2013** A.6.1.1

Function	Category	Subcategory	Informative References
	adequate awareness of anomalous events.		• **NIST SP 800-53 Rev. 4** CA-2, CA-7,
		DE.DP-2: Detection activities comply with all applicable	• **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, PM-14, SI-4
		DE.DP-3: Detection processes are tested	• **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, PE-3, PM-14, SI-3, SI-4
		DE.DP-4: Event detection information is communicated to appropriate parties	• **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, CA-7, RA-5, SI-4
		DE.DP-5: Detection processes are continuously improved	• **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, PL-2, RA-5, SI-4, PM-14

Function	Category	Subcategory	Informative References
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected	**RS.RP-1:** Response plan is executed during or after an event	• **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
	Response activities are coordinated with internal external stakeholders, as appropriate, to include support from law agencies.	**RS.CO-1:** Personnel know their roles and order of operations when	• **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: Events are reported consistent with established criteria	• **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-
		with response plans	• **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, 4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Coordination with occurs consistent with response	• **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: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational	• **NIST SP 800-53 Rev. 4** PM-15, SI-5
	Analysis (RS.AN): Analysis is conducted to activities.	**RS.AN-1:** Notifications from detection systems are investigated	• **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 • **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-

Function	Category	Subcategory	Informative References
			5, PE-6, SI-4
		RS.AN-2: The impact of the incident is understood	• **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 • **NIST SP 800-53 Rev. 4** CP-2, IR-4
		RS.AN-3: Forensics are performed	• **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
		RS.AN-4: Incidents are categorized consistent with response plans	• **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-
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained	• **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
		RS.MI-2: Incidents are mitigated	• **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: Newly identified vulnerabilities are mitigated or documented as accepted risks	• **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response	**RS.IM-1:** Response plans incorporate lessons learned	• **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: Response strategies are	• **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and	**RC.RP-1:** Recovery plan is executed during or after an event	• **CCS CSC** 8 • **COBIT 5** DSS02.05, DSS03.04 • **ISO/IEC 27001:2013** A.16.1.5

Function	Category	Subcategory	Informative References
	restoration of systems or assets affected by		• **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future	**RC.IM-1:** Recovery plans incorporate lessons learned	• **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: Recovery strategies are	• **COBIT 5** BAI07.08 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers,	**RC.CO-1:** Public relations are	• **COBIT 5** EDM03.02
		RC.CO-2: Reputation after an event is repaired	• **COBIT 5** MEA03.02
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and	• **NIST SP 800-53 Rev. 4** CP-2, IR-4

Information regarding Informative References described in Appendix A may be found at the following locations:

- 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.

Mappings between the Framework Core Subcategories and the specified sections in the Informative References represent a general correspondence and are not intended to definitively determine whether the specified sections in the Informative References provide the desired Subcategory outcome.

附录 B：词汇表

This appendix defines selected terms used in the publication.

Category	The subdivision of a Function into groups of cybersecurity outcomes, closely tied to programmatic needs and particular activities. Examples of Categories include "Asset Management," "Access Control," and "Detection Processes."
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters.
Cybersecurity	The process of protecting information by preventing, detecting, and responding to attacks.
Cybersecurity Event	A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).
Detect (function)	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
Framework	A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. Also known as the "Cybersecurity Framework."
Framework Core	A set of cybersecurity activities and references that are common across critical infrastructure sectors and are organized around particular outcomes. The Framework Core comprises four types of elements: Functions, Categories, Subcategories, and Informative References.
Framework Implementation Tier	A lens through which to view the characteristics of an organization's approach to risk—how an organization views cybersecurity risk and the processes in place to manage that risk.
Framework Profile	A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories.
Function	One of the main components of the Framework. Functions provide the highest level of structure for organizing basic cybersecurity activities into Categories and Subcategories. The five functions are Identify,

	Protect, Detect, Respond, and Recover.
Identify (function)	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
Informative Reference	A specific section of standards, guidelines, and practices common among critical infrastructure sectors that illustrates a method to achieve the outcomes associated with each Subcategory.
Mobile Code	A program (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics.
Protect (function)	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
Privileged User	A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
Recover (function)	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.
Respond (function)	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Risk Management	The process of identifying, assessing, and responding to risk.
Subcategory	The subdivision of a Category into specific outcomes of technical and/or management activities. Examples of Subcategories include "External information systems are catalogued," "Data-at-rest is protected," and "Notifications from detection systems are investigated."

附录 C：缩略语

本附录定义在出版物中使用选定的首字母缩写。

CCS 理事会关于网络安全
COBIT 控制目标的信息及相关技术
DCS 集散控制系统
美国国土安全部国土安全部
EO 行政命令
ICS 工业控制系统
IEC 国际电工委员会
红外线的机构间报告
自动化的 ISA 国际协会
ISAC 信息共享和分析中心
ISO 国际标准化组织
IT 信息技术
标准的 NIST 和技术研究所
RFI 索取资料
RMP 风险管理程序
SCADA 监控和数据采集
SP 特刊