关键基础设施安全框架

美国的国家和经济安全离不开关键基础设施的可靠性。伴随着关键基础设施的复杂性和关联性的增加，信息安全威胁使得国家的安全、经济和公众的安全以及人民的健康面临着风险。如同信誉和金融风险一样，信息安全风险对企业造成了影响，它不仅增加了消耗、影响了企业效益，而且还伤害了企业的创新能力，流失了固定的顾客。

为了更好的应对这些风险，总统于 2013 年 2 月 12 日签署了 13636 号执行指令 “提高关键基础设施安信息安全”。该文件是“美国政府为提高国家关键基础设施的安全与可靠性，保障安全的网络环境；并在提高生产效率、创新能力与经济繁荣的同时，保证生产的安全稳定，保护企业商业机密、隐私、以及公民自由的政策文件”，该执行指令要求自发的形成一种基于风险的信息安全框架----以一系列的标准和最佳实践来帮助企业管理信息安全风险。这版由政府和私人组织合作创建的框架，用一种最普通的语言、在基于商业需求的前提下、用最经济有效的方法来描述和管理信息安全风险，该框架并不会增加另外的商业监管要求。

该框架利用商业驱动的方式来指导信息安全操作并且将信息安全风险作为企业风险管理过程的一部分。该框架由三部分组成：框架核心（core）、框架剖面图(profiles)、框架实施层次。框架核心是一系列的信息安全操作、实现效果以及关键基础设施邻域常见的信息参考文献的集合，它能提供详细的指导用来建立个人组织剖面。通过使用框架剖面图，使得企业能将其信息安全操作与商业需求、风险容忍和资源结合起来。实施层次能帮助企业认识和理解其管理信息安全风险的方法的特点。

该执行指令也要求框架包含相应的方法，使得关键基础设施组织者在设计信息安全操作时能保护个人隐私和公民自由。尽管生产过程和需求不同，该框架仍然能将个人隐私和公众自由融合到综合信息安全规划中。

该框架适用于任何企业，不论其大小规模、信息安全风险程度和信息安全复杂度，企业都可以采用风险管理机制和最佳实践来提升关键基础设施的安全和恢复力。该框架为企业和组织提供了最新的多种安全策略，汇总了在工业上有效的标准、指导和实践。另外，由于其参考了全球的信息安全认知标准，所以该框架可以为国外公司提供一个国际合作模型用来加强关键基础设施的信息安全。

该框架并不是万能的用以管理关键基础设施信息安全的方法，企业会继续面临一些特殊的风险----不同的威胁、不同的薄弱点、不同的风险容忍度，从而导致其在实现框架时会存在着差异。企业可以由关键服务的分布不同来决定其操作，也可以对投资进行优先分级以最

大化投资产生的效益，最后，该框架的目的是降低和更好的管理信息安全风险。

该框架并不是一成不变的，当接收到工业应用中的反馈之后，它将会继续进行更新和提高。伴随着该框架的投放使用，未来的版本中会提供相应的学习课程。该策施满足关键基础设施所有者和操作者的需求，当他们处于动态和挑战性的环境中面临着新的威胁、风险和解决方案时。

使用该自愿性质的框架的下一步工作是提高我们国家关键基础设施的信息安全----向私人组织提供指导，从而增加国家关键基础设施一体化的信息安全情况。

1.0 框架介绍

在执行指令中，对关键基础设施的定义为："那些对国家至关重要的系统和资产，不论是物理的还是虚拟的，所谓至关重要是指一旦该系统或资产的能力丧失或遭到破坏，就会削弱国防安全、国家经济安全、公众健康或安全或者这些重要方面的任意组合"。

关键基础设施的团体分成公共和私有的业主和操作员，以及那些保障国家设施安全的组织。关键基础设施的功能部分的实现必须由信息技术（IT）和工业控制系统来支持（ICS）。由于 IT 和 ICS 的技术、彼此间的交流以及互联导致了潜在的脆弱点的改变和扩大以及增加了操作的潜在风险。

该框架提供了一种通用的分类和机制，具体如下：

1）描述当前的信息安全情形。

2）描述了信息安全的目标状态。

3）确定连续和可重复的过程的范围内并对其进行优先提升。

4）在向目标状态进行过程中评估其进展。

5）与内部和外部的利益相关者进行有关信息安全风险的沟通。

1.1 框架的概述

该框架采用了基于风险的方法来进行信息安全风险的管理，其由三部分组成，每部分都用来加固商业驱动和信息安全操作的联系。这三部分的介绍如下：

1）框架核心：其由信息安全操作、期望的结果、关键基础设施领域内常见的应用参考文献组成。该核心提供了工业标准、指导方针和实践的方式，该方式能使得企业内部的行政层到执行\操作层都能进行信息安全的操作和输出结果的交流。该框架核心包含五个并行和连续的功能------识别、保护、检测、反应、恢复。当一起考虑这些功能时，它能提供基于

管理信息安全风险生命周期的高层的、战略性的视角。该核心不仅为各种功能提供了不同的分类和子分类，并且匹配了相应的参考信息案例文献，如现有的标准、指导方针和实践。

2）框架实施层级：该层级提供了一个环境，使得企业认识到信息安全风险和处理过程，从而管理信息安全风险。层级描述了企业在安全风险管理实践过程表现出来基于框架特征的分级（风险和威胁感知、重复性、自适应）。层次将企业的实践进行了分级，从局部的（层次 1）到自适应的（层级 4）。这些层级反映了从非正式、被动反应到快速的、风险感知的处理这个连续的过程。在层级选择过程中，企业应当考虑到其当前的风险管理实践、威胁环境、法律法规、管理需求、业务/任务客体以及组织约束。

3）框架剖面：剖面体现了企业从框架里选择了分类和子分类后产生的结果。剖面可以理解成将框架核心中的标准、指导方针、实践应用到特定的场景后产生的结果的特征。通过对比“当前的”剖面（“目前”状态）和“目标”剖面（“将要到达”的状态），它可以用来识别出能提高信息安全情形（Posture）的机会。为了建立一个剖面，企业应当检阅所有的分类和子分类，考虑到业务驱动和风险评估，最后选择哪些分类是最重要的。企业可以在面临着组织风险时增加分类和子分类。当前的剖面可以用来支持优先次序和测量对比以便向目标剖面进行转换过程中，会面临着其它的业务需求包含成本效益和创新需求。剖面可以用来自我评估和在组织内部或组织之间进行交流。

1.2 风险管理和信息安全框架

风险管理是指由对风险进行识别、评估和应对组成的一个持续的过程。为了实现风险管理，企业应当了解事故发生的可能性以及造成的后果。有了这些信息，企业可以决定它们的风险接受水平以便提供相应的服务，并且将其表达成它们的风险容忍能力。

了解了其风险容忍能力之后，企业可以优先考虑信息安全操作，从而使得企业能对信息安全开支做出明确的确定。

风险管理计划的实施给企业提供了量化和沟通调整自身网络安全计划的能力。企业可以采用不同的方式来处理风险，如减轻风险、转移风险、避免风险或者接受风险，方式的采用取决于风险对关键服务造成的潜在的影响程度。

框架通过使用风险管理流程使得企业能获取信息安全信息和对其进行优先的处理选择。框架支持循环的风险评估和业务驱动的验证，从而帮助企业选择信息安全操作的最终目标状态，并通过期望输出来体现最终目标状态。因此，框架能使企业动态选择和直接提升信息安全风险管理计划，以用于 IT 和 ICS 环境。

2.0 基本框架

略

2.1 框架核心

该框架核心提供了一系列的操作和指导方针的参考案例以便获取特殊的信息安全输出结果。该核心不是需要执行的操作清单。它提供了行业中关键的信息安全输出结果以便对管理信息安全风险有所帮助。该核心由四部分组成：功能定义、分类、子分类、信息参考文献，如图 1 所示：

图 1 框架核心结构

框架核心元素定义如下：

1）功能定义：功能是指将基本的网络安全操作以最高层次体现出来，这些功能为识别、保护、检测、反应和恢复。它通过组织信息的方式帮助企业来表现其网络安全风险的管理，使能风险管理决策、应对威胁，以及通过学习以往的操作来提升性能。该功能还能配合已有的事件管理方法以及将应用在网络安全的投资产生影响显现出来。例如，对实时反应和恢复操作的计算和执行支持上的投资，会导致降低了服务的投送的影响。

2）分类：分类是指将功能细分成与纲领性需求和特殊操作密切关联的网络安全结果的分组。例如分类包含“资产评估”，“接入控制”和“检测过程”。

3）子分类：子分类是将分类再细分成基于技术和管理操作的特殊的输出结果。它提供了一个不够详尽的结果用来支持每个分类都能达到其期望的结果。例如子分类包含“对外部信息系统进行编目”，“静止数据需要保护”，“来自于检测系统的通知需要研究”。

4）参考文献：这些文献由关键基础设施领域内常用的标准、指导方针、实践组成，其

描述了与每个子分类相关输出结果相关的实现方案。这些文献是说明性的，并非是详细无遗的。它们在框架开发过程中的跨职能的指导方案中经常被引用。

框架核心的五个功能并不是串行的或者是为了产生一个静态的期望结果，它们可以并行和连续的产生操作方法，以便能应对动态的网络安全风险。以下对这五种功能进行定义：

1）识别：使得企业能了解系统、资产、数据和功能所存在的网络安全风险。

在基于识别功能的操作是建立在对框架有效利用的基础之上。了解业务环境、支持关键功能的资源、相关联的网络安全风险，可以使得企业能聚焦和优先化其工作方向，该方向与风险管理策略和业务需求一致。例如这些功能的输出结果分类为：资产管理、业务环境、治理手段、风险评估以及风险管理机制。

2）保护：建立或提升适当的保护机制以保护关键基础设备的服务的传送。

保护功能提供了限制和控制潜在的网络安全事件影响的能力。该功能的输出结果分类包含：接入控制、认知和培训、数据安全、信息保护过程和步骤、维护以及保护技术。

3）检测：建立或提升适当的操作，用来识别网络安全事件的发生。

检测功能可以实时的发现网络安全事件。该功能的输出结果分类包含：异常和事件、连续性的安全监视、检测过程。

4）响应：建立或提升适当的操作，用来应对检测到的网络安全事件。

响应功能能提供控制潜在的网络安全事件影响的能力。该功能的输出结果分类包含：响应计划、交流、分析、缓解以及提升。

5）恢复：建立或提升适当的操作，以便用来保存恢复计划、还原由于网络安全事件所损害的能力或服务。

恢复功能能够提供及时的恢复到正常的操作的能力，以便减少来自于网络安全事件的影响力。该功能的输出结果分类包含：恢复计划、系统提升、交流。

2.2 框架实施层级

框架实施层级提供了相应的对应标准环境，通过对比该标准，企业可以认识到网络安全风险以及处理过程以便能对风险进行管理。该层级从局部（第一层级）到自适应（第四层级），描述了在网络安全风险管理实践中严谨和复杂的逐步增加的度，网络安全风险管理基于了业务需求并将其集成到企业中的全部风险管理实践中。风险管理需要考虑一些网络安全方向，包含了将个人隐私和公众自由集成到网络安全风险管理和潜在的风险响应中所产生的度。

接下来对各个层级进行描述：

层级 1：局部的

1）风险管理过程：组织的网络安全风险管理实践是非正式的，风险管理处于一种时有时无的状态。网络安全操作的优先级没有直接考虑到组织的风险客体、威胁的环境、业务/任务的需求。

2）集成的风险管理计划：目前的网络安全风险在组织层上认知有限，尚未建立整个组织范围内的网络安全风险管理机制。企业在处理网络安全风险时就不规则的、就事论事的，处理方式采用的信息来源于外部资源。企业也许不具有将网络安全信息与别的企业共享的能力或计划。

3）外部参与：企业不具有与其它组织进行协调或合作的过程计划。

层级 2：风险感知

1）风险管理过程：风险管理实践已被管理层批准，但没有被确立为全组织范围的策略。网络安全操作优先级的选择来源于组织的风险客体、威胁的环境、业务/任务需求。

2）集成的风险管理计划：在组织层对网络安全风险有着认知，但尚未建立组织范围内的管理网络安全风险的机制。基于风险告知、管理层批准的过程和规划已经被定义和应用，另外已分配足够的资源去实现网络安全目标。网络安全信息在组织内部非正式的共享。

3）外部参与：企业知道自己在大体系中的地位和角色，但没有与外界进行接触和共享以便确定其具体的功能。

层级 2：可重复性

1）风险管理过程：该组织的风险管理方法被批准并作为一项政策。网络安全方案定期的在风险管理过程的应用结果的基础上进行更新，或者受业务/任务需求、威胁、技术背景的改变而改变。

2）集中式风险管理计划：存在着全组织范围的网络安全风险管理方案。基于风险告知的政策、处理过程、规划已被确定、有目的实现、定期更新。一致性方法有效性的应对风险的变化。具有相应知识和技能的人员被用来实现其指定的任务和职责。

3）外部参与：企业了解了其依赖关系和合作伙伴，并且从这些合作伙伴那接收相应的信息用来进行合作和在企业内部针对安全事件制定基于风险的管理决策。

层级 4：自适应

1）风险管理过程：基于课程学习、从以往和当前的网络安全操作过程中获取的预测指标，企业自适应的建立了网络安全实现方案。通过不断的改善先进的网络安全技术和实践的过程，企业能积极适应经常变化的信息安全背景以及能及时的应对不断发展的和复杂的威胁。

2）集成的风险管理计划：存在着全组织范围的管理信息安全风险的方案，该方案利用风险告知策略、处理流程、规划来应对潜在的信息安全事件。信息安全风险管理是企业文化的一部分，并且通过对以往操作的认知、其它资源共享的信息、对当前系统和网络内连续的操作的认识从而不停的进化。

3）外部参与：企业能管理分险，能主动的与合作者分享信息以保证精确的、最近的信息能被发送和消耗，从而能在信息安全事件发生之前来提升信息安全能力。

2.3 框架剖面

框架剖面是由功能、分类、子分类和业务需求、风险容忍、企业的资源的结合。框架能让企业建立一个降低信息安全风险的路线图，该路线图可以很好的实现企业和各部门之间目标的一致，考虑到法律/法规要求和行业内最佳实现方案，以及能反应出风险管理过程的优先级设置。鉴于一些企业的复杂性，它们可以选择多重剖面，实现不同组件的统一以及认识到其独有的需求。

框架剖面可以描述当前的状态或者特殊的网络安全操作所期望的状态。当前剖面体现了当前获得的信息安全的成果。目标剖面显示了需要实现的信息安全风险管理目标的最终输出结果。剖面支持业务/任务需求并且有助于企业内部和企业之间的进行风险知识的交流。

比较不同的剖面（如当前剖面和目标剖面）可以揭示出差距，企业应对这些差距以实现信息安全风险管理目标。处理这些差距的措施可以对路线图有所帮助。缓解差距的措施的优先级由企业的业务需求和风险管理过程所驱动的。该基于风险的方法使得企业对现有的资源进行评估以成本高效益和优先方式来实现信息安全目标。

2.4 框架实现协调

图 2 描述了在企业内部不同层次间的信息和决策的流动，这些层次分为以下三种：

- 行政层
- 业务/过程层
- 实施/操作层

下面对图 2 进行分析：

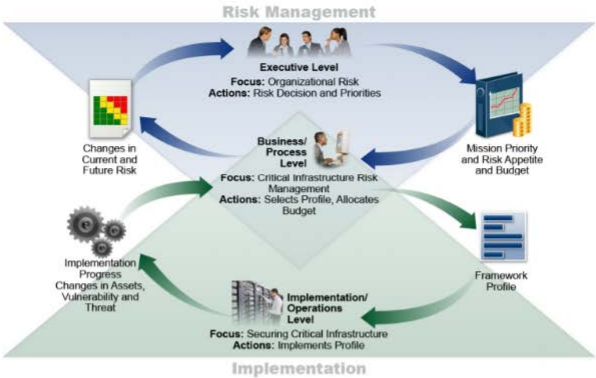

图 2 企业内部抽象的信息和决策流

行政层将任务的优先级别、可提供的资源、总体风险容忍的信息传送给业务层；业务层将这些信息输入到风险管理过程中，然后与实施操作层进行合作进行业务需求的传输以及创建一个剖面；实施操作层将剖面执行进展传送到业务层；业务层利用这些信息进行影响评估；业务层管理人员将影响评估的结果传送给行政层，以便行政层能了解全企业所有的风险管理过程；业务层管理人员将影响评估的结果传送给执行层以便其认知业务影响。

3.0 如何使用框架

一个组织可以使用该框架作为系统过程中一个重要部分，该部分可以用来进行识别、评估、管理信息安全风险。该框架并不是用来取代现有的处理过程；组织可以将当前的处理过程覆盖到框架中去，以便发现当前的信息安全风险处理流程的不足之处和建立一个提升性能的路线图。利用该框架作为信息安全风险管理工具，组织可以决定那些对关键服务传送至关重要的操作和优先处理开支以便最大化投资的影响。

该框架是对现有的业务和信息安全操作的补充，它可以用来创建一个新的信息安全计划或者创建一个可以提升现有计划的策略。该框架将网络安全需求传送给业务伙伴以及顾客，并且有助于识别组织的信息安全方案的差距，它同样提供了一系列的考虑和处理过程，这些过程为个人隐私和公众自由对信息安全计划造成的影响。

接下来的部分将说明组织从不同的方面来应用框架。

3.1 基本审视信息安全实践方案

该框架可以被用来比较组织内当前的信息安全操作与框架核心中的概述条例。通过创建立一个当前的剖面，企业可以检测出它已获得的成果已达到了何种程度，这些成果在核心中的分类和子分类中已描述清楚且与五种高级功能（识别、保护、检测、响应、恢复）一致。组织可能会发现其已经达到它们想要的结果，因此，该信息安全管理与已知的风险相平衡。相反的，组织可能判定其有机会（或者需要）提升其信息安全能力。组织可以使用这些信息来建立一个操作计划以以便加固已有的信息安全实践方案和降低信息安全风险。组织也许会发现它在获取特定的结果时投入过多。组织可以使用这些信息来调整资源的优先级以加强其它信息安全的实践方案。

假如它们不需要取代风险管理过程，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信息安全风险的基本概念，使他们能够评估识别风险的管理方式，和在高层上组织已有的信息安全标准、指导方针、实践方案的方式。该框架同样能帮助一个组织回答基本的问题，如“我们如何做”，然后它们可以在任何时间体任何地方需要的时候，能以一种明确的方式来加强信息安全的实践。

3.2 建立或者提高信息安全计划

接下来就是介绍一个组织如何使用框架来创建一个新的信息安全计划或者改进已有的计划，这些步骤也许会被连续的重复以提高信息安全。

Step 1: 优先级和范围：组织应当识别出其业务/任务目标和高层的组织的优先事项，有了这些信息，组织可以制定有关信息安全实施的战略决策，并确定支持选择的业务线或处理过程的系统和资产的范围。该框架适合于支持组织内部不同的业务线或处理过程，而该组织具有不同的业务需求和相关的风险容忍能力。

Step 2: 确定方向：（orient） 一旦基于业务线和处理流程的信息安全计划的范围被确定了，组织就可以识别出相应的系统和资产、调整相应需求、和全体的风险方法。然后组织也能识别出系统和资产面临的威胁和具有的薄弱点。

Step 3: 创建一个当前的剖面： 组织可以建立一个当前的剖面，该剖面根据框架核心中的分类和子分类的输出结果来确定当前的需要获取的结果。

Step 4: 执行风险评估：该项操作可以将组织的整体风险管理过程或以前的风险评估操

作做为指导。组织能操作环境进行分析，以便得到信息安全事件发生的概率以及其对组织造成的影响。对于组织来说，将新出现的风险、威胁和脆弱的数据变成易于理解的安全事件发生的概率及影响，这项工作是很重要的。

Step 5: 创建一个目标剖面：组织创建的目标剖面，聚焦于利用框架的分类和子分类对组织需要得到的信息安全输出结果进行评估和描述。组织也许会建立额外的分类或子分类来应对特殊的组织风险。组织也许会考虑组织以外的利益相关者的需求和影响来创建目标剖面，如部门实体、顾客、业务伙伴。

Step 6: 确定、分析以及对差距进行优先分类：组织将当前的剖面与目标剖面进行对比以确定差距，接下来，组织根据业务驱动、成本/效益分析、对目标剖面中的输出结果的理解来建立一个优先操作表。然后组织确定应对这些差距所必需的资源。采用这种方式来使用剖面可以使得组织能制定有关信息安全操作的明智决定，支持风险管理以及使得组织能进行具有成本效益的、有针对目标的改进。

Step 7: 实施行动计划：组织需在决定哪些操作被用来应对差距，如果这些操作存在的话，那么就需要在先前的步骤进区别开来。接下来依靠目标剖面对当前的信息安全实践操作进行监视。为了进行更加深入的指导，框架应当对有关分类和子分类的例子参考文献进行识别，但是，组织应根据其部门特性、更好的工作需求来决定哪些标准、指导方针、实践方案。

一个组织可以重复这些步骤，如需要连续进行评估和提升它的信息安全能力。例如，组织会发现其通过重复性的确定方向操作来提升风险评估的质量。此外，组织通过迭代更新当前剖面来监视当前的处理过程，随后将当前剖面与目标剖面进行比较。组织也可以利用这些步骤来统一其信息安全计划和期望框架实施层级。

3.3 与利益相关者进行信息安全需求的交流

相关关联的利益相关者可以利用框架提供的简明的方式进行交流，而交流的内容为关键基础设施必不可少的服务的传递。例如：

1）一个组织可以利用目标剖面来表达其信息安全风险管理的需求，并将该需求传递给外界的服务提供商（如一个云计算提供商所导出的数据）。

2）一个组织可以通过当前剖面来表达其信息安全状态，以便记录下结果或与收集的需求进行对比。

3）一个关键基础设施的业主/操作员可以利用目标剖面传送需求分类或子分类的方式来确定它需要关联的外界合作伙伴。

4）一个关键基础设施部门可以设立一个目标剖面，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剖面。

3.4 在重新建立或修改参考文献时抓住机会

新的或修改的标准、指导方针、实践方案有助于组织能寻找出机遇，而附加的信息参考文献可以帮助组织面对新出现的需求。组织在实施已有的分类或者建立新的分类时，也许会发现只有极少数与相应操作有关的信息参考文献。为了解决这一问题，组织应当与技术带人人合作，参与标准的起草、制定与协调，整合标准、指导方针与实践方案。

3.5 保护个人隐私和公众自由的方法

这部分主要描述了由行政层要求的由于信息安全操作而导致对个人隐私和公众自由造成的影响的处理方法。

当个人信息被使用、收集、处理、维护或者在信息安全操作时被泄露时就会产生个人隐私与公众自由的问题。以下是一些可能需要考虑到人个隐私和公众自由的操作：导致个人信息被过度采集或过度保留的信息安全操作；与信息安全操作无关的个人信息的泄露和使用；导致拒绝服务或类似潜在不利影响的信息安全缓解操作，包括一些对表达和关联自由造成影响的事件检测或监视操作。

企业和政府部门应当直接负责由信息安全操作导致的公众自由的保护。参考下文方法，拥有或操作关键基础设施的企业和政府部门应当具有服从隐私法律、法规和宪法要求的操作以支持的信息安全活动。

为了应对隐私影响，组织应当考虑它们在这种情况下，哪些措施是适当的。它的的信息安全计划应当包含隐私原则，包括：在信息安全事件中，有关个人信息材料的数据应当减少收集、泄露和保留；限制基于信息收集的外部信息安全操作活动；对某些特定的信息安全操作透明；在对个人信息进行操作时应当获取当事人的同意或对当事人进行补偿；数据质量、完整性、机密性；责任与审查。

下面就是对一些方法：

信息安全的风险管理

- 组织在对信息安全风险和潜在的风险回应进行评估时应当考虑到其信息安全计划对隐私造成的影响。
- 具有信息安全相关的隐私负责人应当接受适当的管理和培训。
- 支持信息安全操作的过程应当考虑到隐私法律、法规和宪法需求。
- 过程中间应当评估上述的组织措施和控制方法造成的影响。

个体接入系统或资产之前进行识别认证

- 采取措施以识别和解决访问控制措施的隐私问题，它们涉及个人信息的收集，泄露和使用

认知和培训措施

- 来源于组织隐私策略的有用信息包括信息安全工作人员的培训和认知活动。
- 为组织提供信息安全服务的服务提供商都会被告知组织的适用的隐私策略。

异常动作检测和系统资产监视

- 在组织异常检测和信息安全监视过程中进行隐私审查

响应操作，包含信息共享和其它缓解措施

- 评估和应对是否、什么时间、以何种方式、多大范围内个人信息被组织外界进行共享，该操作为安全信息共享活动的一部分。
- 对组织的信息安全缓解影响进行隐私审查。

附录 A： 框架核心

该附录介绍了核心框架：功能、分类、子分类以及描述了在所有关键基础设施部门中常见的信息安全操作的信息参考文献。当前的框架核心格式并没有提出一种特殊的实施命令或者有关分类、子分类、参考文献的重要的度。该附录中的框架提供了对信息安全风险进行管理动作的通用的代表集合。该框架不是详尽的，它是可以扩展的，允许组织、部门和其它实体来基于成本效益和高效的使用子分类和信息安全参考文献，并使得它们能管理其信息安全风险。可以在剖面创建过程中选择框架核心中的操作，以及将额外的分类、子分类、信息安全参考文献添加到该剖面中。一个组织的风险管理过程、法律/法规需求、业务/任务目标、组织的限制等指导了组织在创建剖面时选择了哪些操作。在进行信息安全风险评估和保护操过程中，个人隐私被当作分类中引用的数据和资产的一部分进行考虑。

尽管在功能、分类、子分类方面 IT 和 ICS 的输出结果是相同的，但是操作环境和考虑条件却存在着差异。ICS 对物理世界产生了直接的影响，包含对安全和人体的安全的潜在风险，对环境造成的影响。另外，与 IT 相比，ICS 拥有其独特的性能和可靠性需求，在实施信息安全措施时安全和有效性的目标必须被考虑。

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。功能和分类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；每个子类别的唯一字母标识符在表 2 中显示。

表 1 功能和分类的特殊标识符

功能标识符	功能	分类标识符	分类
ID	识别	ID.AM	资产管理
		ID.BE	业务环境
		ID.GV	governance
		ID.RA	风险评估
		ID.RM	风险管理策略
PR	保护	PR.AC	接入控制
		PR.AT	认知和培训
		PR.DS	数据加密
		PR.IP	信息保护过程和计划
		PR.MA	维护
		PR.PT	保护机制
DE	检测	DE.AE	异常和事件
		DE.CM	连续安全监视
		DE.DP	检测过程
RS	响应	RS.RP	响应计划
		RS.CO	交流和通信
		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	交流

表 2 框架核心详细定义 （略）