CCID 赛迪智库 译丛

2017 年 8 月 7 日　　第 30 期　　总第 315 期

改善关键基础设施网络安全框架（1.1 版）

【译者按】 关键基础设施运行可靠与否决定着世界主要经济体的国家安全与经济安全。为更好地保障关键基础设施网络安全，美国国家标准和技术研究院 2017 年 1 月修订发布了《改善关键基础设施网络安全框架》1.1 版。新版本完善了框架基础三要素（框架核心、框架实施层和框架文件）的内涵和外延，提供了一套框架使用流程，指导各实体组织创建新的网络安全计划或改进已有计划。新版本还突出强调了网络供应链风险管理和网络安全度量的重要性。赛迪智库军民结合研究所对新版本进行了编译，期望对我国相关部门提供参考。

【关键词】 关键基础设施　网络安全　风险管理　框架

新时期，关键基础设施系统日益复杂，互联互通越来越强，使得网络安全威胁有了新的可乘之机，国家安全、经济、公共安全与医疗也因此被置于险境。为应对新的网络安全风险，2014 年 2 月，美国国家标准与技术研究院（NIST）按照总统 13636 号行政命令“改善关键基础设施网络安全”要求，发布了《改善关键基础设施网络安全框架》1.0 正式版本，涉及一系列与标准、准则和惯例相匹配的解决网络安全风险的政策、业务和技术方法。经过近两年政府和私营部门的共同实践，NIST 获取了一系列关于框架改进的反馈意见，通过整理分析形成《改善关键基础设施网络安全框架》1.1 版（以下简称“框架”），1.1 版框架在最大程度保持与 1.0 版本兼容的基础上，对内容进行了完善、澄清和改进。框架将网络安全风险纳入各实体风险管理流程，重点运用业务驱动因素指导网络安全活动，提供了一套关键基础设施安全风险管控的标准化实施指南。框架的实施完全出于自愿，不仅能为各实体提供个别指导，强化网络安全风险管理，又能提高国家关键基础设施的整体网络安全状况。

一、框架介绍

框架由框架核心、框架实施层和框架文件三个基础要素组成。其中，**框架核心**提供了关键基础设施领域常见的各种网络安全活

动、预期结果和适用范围，包括识别、保护、检测、响应和恢复五个功能。**框架实施层**分析了各实体机构应当如何审视网络安全风险以及管理风险的相关流程，包括部分实施到自适应实施四级。**框架文件**代表某实体根据业务需求，选定的框架类别和子类别，通过对比当前文件（当前状态）与目标文件（目标状态），发现提高网络安全状态的机会。此外，框架还提供了一整套使用流程和通用要素，以便于在网络安全计划的范围内考虑保护隐私和公民自由的影响，遵守联邦规定；最后讨论了网络安全与业务目标的相关性，突出和强调了网络安全衡量的重要性。

框架的根本目标是降低和更好地管理网络安全风险。换言之，框架是基于风险的网络安全风险管理方法，给出了了解、管理和表述内外部网络安全风险的通用语言，有助于找出降低网络安全风险的优先措施，同时它也是风险管理工具，从而使政策、业务与技术手段保持一致。

值得注意的是，框架并不是管理关键基础设施网络安全风险的万全之策。不同主体仍将面临特有风险，其威胁、漏洞，对风险的容忍程度也各不相同，因此框架各项措施的具体实施方法也将各不相同。框架仅仅补充而非代替各实体的风险管理流程和网络安全计划，具有较强的适应性，可与各种网络安全风险管理流程配合运用。各实体可利用现有流程，在本框架的帮助下，加强

网络安全风险管理和行业交流，同时与行业惯例保持一致。此外，尚无网络安全计划的各实体也可以参考本框架制定其网络安全计划。同时，本框架并不局限于任何特定行业，其中标准、准则和惯例的通用分类法亦不局限于特定国家。国外实体也可以利用本框架加强自身的网络安全，本框架还将有助于制定关键基础设施网络安全方面进行国际合作的共同语言。

二、框架的基础要素

（一）框架核心

框架核心提供了一系列活动以实现特定的网络安全功能，并提供了实现这些功能的最佳参考实例。框架核心包括功能、类别、子类别和信息参考四个要素，如图 1 所示。

图 1　框架核心结构

框架核心共有如下五个功能，这些功能既不是按部就班的先后顺序，也不是一成不变的预期结束状态，而是可以同时持续执行，形成应对动态网络安全风险的运营文化。

1、识别：帮助组织了解进而管理系统、资产、数据和能力所面临的网络安全风险。识别功能是有效使用框架的基础。了解当前所处的背景，支持关键功能的资源以及相关的网络安全风险，有助于根据风险管理策略和业务需求厘清主次，合理安排工作重点。此功能的结果类别有：资产管理、运营环境、治理模式、风险评估及风险管理策略。

2、保护：制定和实施相应保障措施，确保关键基础设施服务的实现。保护功能有助于限制或降低潜在网络安全事件的影响。此功能的结果分类包括：访问控制、安全意识和培训、数据安全、信息保护流程、维护及保护技术。

3、检测：制定并实施相应措施，发现网络安全事件。检测功能可及时发现网络安全事件。此功能的结果分类包括：异常和事件、持续安全监控及检测流程。

4、响应：制定和实施相应活动，采取措施应对已探明的网络安全事件。响应功能有助于控制潜在网络安全事件的影响。此功能的结果类别包括：响应规划、通信、分析、缓解及改进。

5、恢复：制定并实施相关活动，维护弹性计划，恢复因网络

安全事件而受损的能力或服务。恢复功能有助于及时恢复正常运营，减少网络安全事件的影响。此功能的结果分类包括：恢复计划、改进和通讯。

（二）框架实施层

框架实施层为如何审视网络安全风险提供了一个风险管理相关流程。实施层的范围从部分实施到自适应实施共四个层级，各层级网络安全风险管理实践的严谨度和复杂度逐渐增加。

层级 1：部分实施

风险管理流程：没有正式的网络安全风险管理实践惯例，仅采用临时措施进行风险管理，时常处于被动应对状态。网络安全活动的主次安排，未考虑风险目标、威胁环境或业务/任务需求。

综合风险管理计划：整个实体层面的网络安全风险意识十分有限。由于从外部获得的经验或信息千差万别，采取的网络安全风险管理措施也是千差万别，缺乏规律和统一，也可能根本就没有在内部实现网络安全信息共享的流程。

外部参与：实体没有应对经验和合作伙伴，无法与其他实体进行协调和合作。

网络供应链风险管理：对网络供应链风险影响的了解很不全面，或者没有确定、评估和减轻网络供应链风险的流程。

层级 2：风险提示

风险管理流程：风险管理实践惯例得到管理部门的认可，但并没有将其确立为在整个实体进行贯彻落实的政策，而是根据各部门风险目标、威胁环境或业务/任务要求，确定网络安全活动的轻重缓急。

综合风险管理计划：在实体层面上已经有了网络安全风险意识，但尚未建立在整个实体进行贯彻落实的网络安全风险管理方法，而是对非正式的途径在实体内部共享网络安全信息。仅在部分层面考虑任务/业务目标中的网络安全问题。通常不会对整个实体资产所面临的网络风险进行经常性的反复评估。

外部参与：该实体了解自己在大型生态系统中的作用，但尚未建立外部交流和共享信息的正式部门。

网络供应链风险管理：实体了解产品或服务相关的网络供应链风险，这些产品或服务要么有助于实现其业务任务功能，要么就是正在应用于自己的产品或服务。内部没有建立管理网络供应链风险的正式部门，也没有与供应商及合作伙伴统一应对措施。

层级 3：可重复

风险管理流程：该实体已经有了正式的风险管理政策，并根据业务/任务需求及威胁和技术格局出现的变化，对其网络安全实践进行定期升级。

综合风险管理计划：拥有在整个实体范围内进行贯彻落实的

网络安全风险管理方法，已确立、落实和审查风险提示的政策、流程和程序。拥有应对风险变化的统一有效方法。其人员具有履行其任职和职责的知识和技能，能够持续准确地监控实体资产所面临的网络安全风险。高级网络安全人员与非网络安全管理人员定期沟通网络安全风险的相关情况。高级管理人员确保实体内部所有运营都要考虑网络安全风险。

外部参与：实体了解附属部门和合作伙伴，接收合作伙伴发来的信息，通过合作和基于风险的管理决策来应对其内部的各种情况。

网络供应链风险管理：已经通过企业风险管理政策和流程实行涵盖整个实体的网络供应链风险方案，包括管理网络供应链风险与其他企业风险平衡的治理机构（例如风险委员会）。实体能够主动贯彻政策、流程和程序，并进行持续的监控和审查。其人员具备相应的知识和技能，能够履行各自的网络供应链风险管理职责。该实体已经制定了正式协议，能够向供应商和合作伙伴传达根本要求。

层级 4：自适应

风险管理流程：实体根据以往和目前网络安全活动中学到的经验教训和预测指标，对网络安全实践惯例进行调整，并结合先进的网络安全技术和惯例进行持续不断的改进，从而积极适应不

断变化的网络安全环境，及时应对不断变化、日益复杂的威胁。

综合风险管理计划：实体已经全面落实网络安全风险管理方法，能够运用风险提示、流程和程序来应对潜在的网络安全事件。在决策时，已经了解并考虑网络安全风险与任务/业务目标之间的关系。高级管理人员对网络安全风险的重视程度不亚于财务风险和其他风险。能够分析了解当前的风险环境，预测未来的风险环境和风险倾向，并以此为基础制定预算计划。业务部门能够在实体的风险倾向和容忍能力范围内实施愿景，并分析系统层面的风险。网络安全风险管理已成为企业文化的一部分，并能够在先前活动意识、其他来源共享信息、以及对系统和网络活动时刻保持警惕的基础上持续发展。实体的所有层级对网络安全风险都有着清楚的认识和理解，可以快速有效地应对业务/任务目标以及威胁和技术领域出现的变化，对风险产生与出现的方式了如指掌。

外部参与：实体能够主动管理风险，并积极与合作伙伴共享信息，确保提前传达准确及时的信息，做到防患于未然。

网络供应链风险管理：实体能够运用实时或近实时信息，快速有效地分析新出现的网络供应链风险，并能够促使外部供应商、合作伙伴、以及内部的职能部门和所有层级都能运用结构化的网络供应链风险管理知识。实体能够积极地传达并运用正式（例如协议）和非正式机制，与供应商、合作伙伴以及个人和买

方机构建立并保持牢固的关系。

各实体在选择实施层级时，要考虑风险管理惯例、威胁环境、法律监管要求、信息共享实践、业务/任务目标、网络供应链风险管理需求和各实体结构上的限制因素，确保所选层级符合其目标并切实可行，以便将关键资产和资源所面临的网络安全风险降至可接受水平。此外，还应考虑联邦政府部门、信息共享和分析中心（ISAC）、现有的成熟度模型或其他渠道的外部指导，从而确定所需的实施层级。实施层级的选择与运用会影响框架文件；预期层级所表现出的风险状况，也会影响目标文件的轻重缓急。

（三）框架文件

框架文件能够根据实体的业务需求、风险承受能力和资源对功能、类别和子类别进行调整，帮助各实体建立降低网络安全风险的路线图，确保既能兼顾整体与部门目标，考虑法律/法规要求和行业成熟经验，又能反映风险管理的轻重缓急。

框架文件可用于描述特定网络安全活动的当前状态或预期的目标状态，当前文件是指目前正在实现的网络安全结果。目标文件是指实现网络安全风险管理预期目标所需的成果。文件能够支持业务/任务要求，并有助于在实体内部和实体之间进行风险沟通。框架文件并没有给出既定的文件模板，允许灵活实施。通过文件对比，发现为实现网络安全风险管理目标而需要弥补的差

距。弥补差距的行动计划将有助于建立上述路线图。各实体可根据业务需求和风险管理流程来安排解决差距的优先次序。这种基于风险的策略，使各实体能够量力而行，以高效率、低成本的方式安排优先主次，让每一美元支出都能发挥最大效用。

（四）框架实施的协调

图 2 描述了各实体内部常见的信息和决策流程，包括三个层级：高级行政决策层、业务/流程层和实施/运营层。行政层向业务/流程层传达任务优先级、可用资源和总体风险承受能力，再将信息输入风险管理流程，然后与实施/运营层进行协作，以传达业务需求并创建文件。实施/运营层向业务/流程层传达文件实现进度，然后业务/流程层可使用该信息来评估影响，再将评估结果报告到行政层，为各实体的整体风险管理流程提供实用信息，使实施/运营层认识到业务影响。

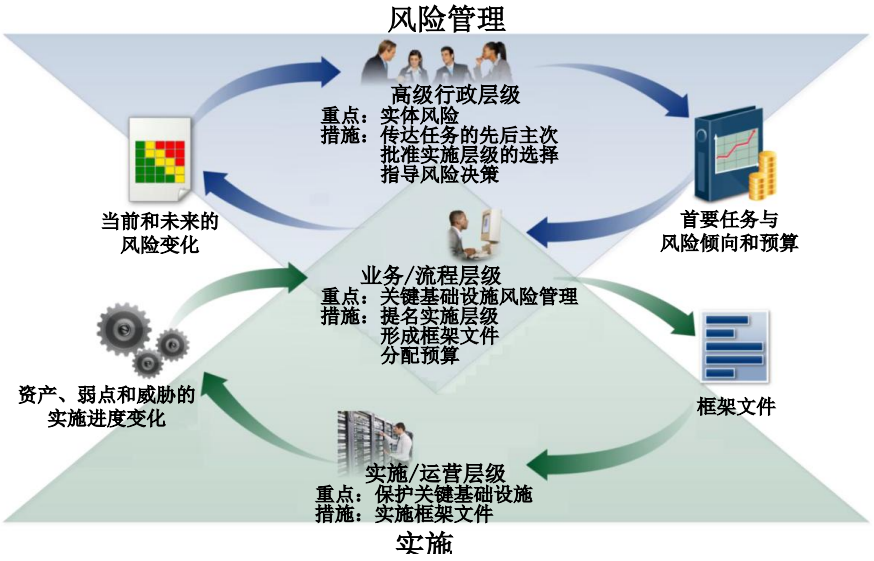

图 2　各实体内部的信息和决策

三、框架的使用流程和规则

各实体组织可将框架用作安全管理系统流程的关键部分，用来识别、评估和管理网络安全风险。框架并不是要取代现有网络安全风险管理流程，旨在补充现有业务和网络安全措施，并可以在此基础之上制定全新网络安全计划，或根据网络安全管理差距形成针对现有计划的改进机制，并确定事关关键服务的最重要活动，安排支出的轻重缓急，让投资发挥最大效用。

框架可应用于各主体设计、构建/购买、部署、运营和停用系统生命周期的各个阶段。设计阶段应考虑网络安全要求，其关键节点是，验证系统网络安全规范是否符合框架文件中所规定的需求和风险处置。框架文件优先安排的网络安全成果应当在以下阶段激活：一是在构建阶段进行系统研发时；二是在购买阶段进行系统采购或外包时。在系统部署阶段，应评估系统的网络安全特性，以验证设计是否有效。随后，将框架的网络安全成果作为系统持续运行的基础，包括不断进行重新评估，以验证是否仍能满足网络安全要求。通常情况下，系统之间有着十分复杂的相互依赖关系，意味着当一个或多个系统退役时，应仔细考虑框架结果。以下章节介绍了各实体使用框架的不同方法。

（一）网络安全管理的基本概况

框架可用于对比分析现有的网络安全活动与框架核心所列出

的网络安全活动。通过创建当前框架文件，各实体就可以按照识别、保护、检测、响应、恢复这五种高级功能，来检查核心类别与子类别所描述结果的实现程度，并实施与已知风险相匹配的网络安全管理措施。虽然这五个高级功能并不能取代风险管理流程，但却能为高级管理人员和其他人员提供并提炼网络安全风险基本概念的简要方法，让他们能够评估管理已知风险的方法，以及如何从较高层级应对现有的网络安全标准、指南和惯例。框架还可以帮助各实体解答怎么办等基本问题，从而采取更加有理有据的方法，在适时必要的情况下加强网络安全。

（二）网络安全计划的建立与改进

以下步骤详细说明各实体如何运用本框架来创建新的网络安全计划或改进现有计划。必要时可重复执行这些步骤，从而不断提高网络安全。

步骤 1: 确定优先级和范围。各实体找出业务/任务目标和高级别的优先事项，据此做出网络安全实施方面的战略决策，再根据所选择的业务范围或流程来确定相应的系统和资产范围。

步骤 2: 找出漏洞。各实体找出系统和资产面临的威胁漏洞。

步骤 3: 创建当前框架文件。各实体从框架核心中确定当前正在实现的类别与子类别结果，进而创建当前框架文件。

步骤 4: 开展风险评估。各实体通过分析运营环境，洞察发

生网络安全事件的可能性以及事件可能对实体产生何种影响。重要的是，实体要识别新兴风险，运用来自内外部的网络威胁信息，更好地了解网络安全事件的可能性和影响。

步骤 5: 创建目标框架文件。各实体要创建目标框架文件，重点评估能够描述预期网络安全结果的框架类别和子类别。也可以制定额外的类别和子类别，来应对特别的风险。

步骤 6: 差距的确定、分析和优先安排。各实体对比当前框架文件和目标框架文件，以找出差距。然后，再制定解决这些差距的优先行动计划。随后实体再确定解决这些差距的必要资源，以此来运用框架文件做出有理有据的网络安全决策。

步骤 7: 实施行动计划。各实体要确定解决差距所采取的措施。再根据目标文件监控当前的网络安全措施。

（三）与利益相关者沟通网络安全要求

框架提供了通用语言，以便向负责交付关键基础设施服务的利益相关者传达需求。如各实体可使用目标文件向外部服务提供商（如向其发送数据的云服务商）传达网络安全风险管理要求。

在利益相关者之间沟通和验证网络安全需求的做法之一是网络供应链风险管理（SCRM）。SCRM 主要目的是识别、评估和减轻“网络供应链中可能含有潜在恶意功能、伪劣假冒、或因为制造开发不良而存在缺陷的产品和服务”。SCRM 活动可能包括:

确定供应商以及信息技术（IT）和运营技术（OT）合作伙伴的网络安全要求；通过正式协议（如合同）明文规定网络安全要求；向供应商和合作伙伴传达确认和验证网络安全要求的方法；通过各种评估方法来验证是否满足网络安全要求；管理上述活动。

如图 3 所示，SCRM 包括 IT 和 OT 供应商和买方，也包括非 IT 和 OT 合作伙伴。其中，买方是指产品或服务的消费者。供应商涵盖为实体内部（如 IT 基础设施）或者为买方提供产品和服务的供应商。非 IT 和 OT 合作伙伴也拥有实体安全系统的访问权限，也将成为各实体面临的风险因素。这些关系更加凸显了 SCRM 在关键基础设施乃至整个数字经济中解决网络安全风险的关键作用。各实体在构建保护与探测能力以及制定应对与恢复程序时，应当认真对待并慎重考虑网络供应链风险管理。不管是考虑核心的单个子类别，还是对文件进行整体考虑，框架都能为实体及其合作伙伴提供确保新产品或服务符合最优安全结果的方法。

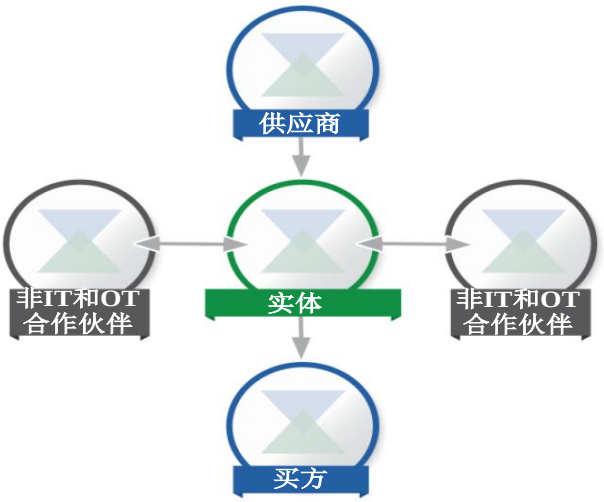

图 3　网络供应链关系

（四）采购决策

框架的目标文件已经列出实体网络安全要求的轻重缓急，可以据此做出产品和服务采购的相关决策。这种交易无法向供应商施加整套的网络安全要求。因此不同于网络供应链风险管理，目标文件旨在通过预先确定的网络安全要求列表，在多个供应商之间做出最佳采购决策。通常，这需要进行一定程度的权衡分析。因此，购买产品或服务时，就知道了与目标文件的差距。采购产品或服务后，可以运用文件来跟踪剩余的网络安全风险。例如，采购的服务或产品如果不能满足目标文件中规定的所有目标，实体可以将剩余的网络安全风险纳入整体风险管理之中，通过其他管理措施来解决剩余风险。文件还允许通过定期审查和测试机制，确保产品满足网络安全结果。

（五）发现机会，制定全新或修改现有信息参考

框架可用于发现机会，制定全新或修改现有的标准、准则或惯例，通过更多信息参考来帮助各实体应对新需求。实施现有子类别或开发新子类别的实体可能无法找到相关活动的信息参考。为了满足这一需求，实体需与技术和/或标准部门合作起草、制定和协调标准、准则或惯例。

（六）保护隐私和公民自由的方式

隐私保护和网络安全密切相关。各实体的网络安全活动在使用、收集、处理、维护或披露个人信息时，也可能对隐私保护和公民自由造成风险。政府在实施网络安全活动时，负有保护公民自由的责任。拥有或运营关键基础设施的政府应当制定流程，保证网络安全活动遵守隐私保护法律、法规和宪法的相关要求。各实体在实施措施时，也需要考虑在网络安全计划中纳入以下隐私保护原则：尽量收集、披露、保留网络安全事件相关个人信息资料的最少数据；限制网络安全活动专用信息的外部使用；部分网络安全活动要公开透明；网络安全活动在使用信息时征得个人同意，并在产生不利影响时实施补救；数据质量、完整和安全；责任追究和审计。在评估框架核心时，各实体可考虑通过以下活动来解决上述问题：网络安全风险治理、资产与系统使用权限的识别与授权策略、网络安全意识和培训措施、异常活动检测和系统

与资产监控、活动响应，包括信息共享或其他减灾工作。

（七）遵守联邦规定

对于联邦信息系统，包括关键基础设施中的系统，联邦机构必须遵守《联邦信息安全现代化法案（FISMA）》、美国政府管理预算局（OMB）出台的政策以及联邦信息处理标准和特颁文件中所规定的 NIST 标准和指导。网络安全框架是现有联邦风险管理方法的良好补充。联邦机构可以通过以下方式予以应用:

- 运用框架实施层来表达风险处置;
- 运用框架核心来组织和传达网络安全概念、活动和结果;
- 运用框架文件来做出优先决策;
- 运用七步骤流程来实施评估和补救活动。

此外，OMB 还根据框架功能整理了最新的 FISMA 报告和改进计划（如网络安全战略和实施计划）。联邦机构应当从工作惯例中了解框架核心，确保在联邦和非联邦合作伙伴之间实现准确高效的高级别网络安全对话。

四、框架的衡量与验证

网络安全度量为实体组织内部和外部的强信任关系提供了基础，对于关键基础设施网络安全管理具有重要意义。随着时间的推移，通过外部审计和通过合规性评估来衡量状态和趋势，使实

体组织能够理解并向第三方、合作伙伴和客户传达有意义的风险信息。

运用框架进行衡量的关键术语是“指标”和“措施”。指标可以用于“促进决策、提高业绩和问责”。实施层级、子类别和类别都是很好的指标。指标能够对措施进行整合与关联，让各实体认清安全态势的意义和形势。措施是“支持指标的可量化、可遵守的客观数据”。措施与技术控制密切相关，如信息参考等等。从安全指标收集到的信息，能够显示网络风险状态。同时跟踪安全指标和业务成果，就可以察觉安全控制的细微变化如何影响业务目标的完成。通过滞后的指标来衡量是否已达成业务目标固然十分重要，但通过预先指标，来了解实现未来目标的可能性则更为重要。而实体确定网络安全与业务成果之间因果关系的能力，取决于衡量系统的准确性和精度。为了让各实体减少不必要的开支，系统的准确性和费用要符合相应业务目标所需的衡量精度。

（一）业绩相关性

衡量网络安全的目的，是要将网络安全与业务目标相关联，从而理解和量化其中的因果关系。常见业务目标包括：推动业务/任务结果、提高成本效益、降低企业风险。将网络安全指标与业务目标相关联，往往要比简单地衡量单个网络安全结果更为复杂。因为给定业务目标涉及大量多样的影响因素，如零售银行可

以加强验证程序，来增加网上银行客户数量；但是，在线银行客户的增加，还需要开发基于短信的可靠在线交易、定位特定消费者群体、选择最具针对性的沟通渠道、以及在这些沟通渠道之上进行必要时长的营销。总之，实现客户增长要取决于信息、营销、广告网络安全和其他因素。不同网络安全活动的相对成本效益（指实现既定业务目标所需要的最小网络安全工作和开支）也是重要的考虑因素。为了解成本效益，各实体必须首先对业务目标有个清楚了解，明白业务目标和网络安全指标之间的关系，以及业务目标和非网络安全因素之间的关系。

通常情况下，并不清楚网络安全结果对业务目标的影响。各实体能否找出网络安全结果和业务目标之间的因果关系，还取决于能否在网络安全结果和业务目标之间实现充分关联。这是衡量网络安全的最大挑战之一。必须要格外注意，确保网络安全结果和业务目标之间存在真正的相关性。一般来说，将网络安全措施与更高级别的网络安全指标相关联，要易于在网络安全指标与业务指标之间实现相关。

（二）衡量网络安全的种类

与框架有关的指标和措施如表 1 所示。框架实施层是整体网络安全风险管理惯例的定性指标。除了定性指标之外，也包括风险管理流程、综合风险管理计划、外部参与和网络供应链风险管

理的个别实施层属性，以及代表特定风险管理活动的流程。例如，综合风险管理计划反映了网络安全风险治理与应对流程的程度；外部参与指标能够反映从信息共享论坛和来源收到的威胁和漏洞信息数量。框架核心的网络安全结果是网络安全管理全套综合指标的基础，这些指标合并使用能减少（或避免）网络安全风险。控制目录等信息参考提供了模块化的详细技术措施，能够对框架形成良好补充。

表 1　框架衡量的种类

衡量指标	衡量对象	相应的框架组成	衡量类型
惯例	一般风险管理行为	实施层	指标
流程	具体风险管理活动	包括七步骤（“网络安全计划的建立与改进”）和运用特定情况特别流程（例如“与利益相关者沟通网络安全要求”和“保护隐私和公民自由的方式”）	措施
管理	实现一般网络安全	核心/文件功能，类别和子类别	指标

	结果		
技术	实现特别网络安全结果	信息参考	措施

译自：*Framework for Improving Critical Infrastructure Cybersecurity（Draft Version 1.1）, January 2017 by National Institute of Standards and Technology*

赛迪智库
面向政府 服务决策

思想，还是思想
才使我们与众不同

《赛迪专报》
《赛迪译丛》
《赛迪智库·软科学》
《赛迪智库·国际观察》
《赛迪智库·前瞻》
《赛迪智库·视点》
《赛迪智库·动向》
《赛迪智库·案例》
《赛迪智库·数据》
《智说新论》
《书说新语》

《两化融合研究》
《互联网研究》
《网络空间研究》
《电子信息产业研究》
《软件与信息服务研究》
《工业和信息化研究》
《工业经济研究》
《工业科技研究》
《世界工业研究》
《原材料工业研究》

《财经研究》
《装备工业研究》
《消费品工业研究》
《工业节能与环保研究》
《安全产业研究》
《产业政策研究》
《中小企业研究》
《无线电管理研究》
《集成电路研究》
《政策法规研究》
《军民结合研究》

编 辑 部：赛迪工业和信息化研究院
通讯地址：北京市海淀区万寿路27号院8号楼12层
邮政编码：100846
联 系 人：刘 颖 董 凯
联系电话：010-68200552 13701304215
010-68207922 18701325686
传 真：0086-10-68209616
网 址：www.ccidwise.com
电子邮件：liuying@ccidthinktank.com

报：部领导

送：部机关各司局，各地方工业和信息化主管部门，
相关部门及研究单位，相关行业协会

编 辑 部：工业和信息化部赛迪研究院

通讯地址：北京市海淀区紫竹院路 66 号赛迪大厦 15 层国际合作处

邮政编码：100048

联 系 人：张滢星

联系电话：（010）88559658　18614088989

传　　真：（010）88558833

网　　址：www.ccidgroup.com

电子邮件：zyx@ccidgroup.com