网络安全

Topical Requirement

专项要求

用户指南

The Institute of
Internal Auditors

目录

专项要求概述

《专项要求》与《全球内部审计准则 (Global Internal Audit Standards™)》和《全球指南》都是《国际内部审计专业实务框架 (the International Professional Practices Framework®)》的重要组成部分。国际内部审计师协会要求将《专项要求》与《全球内部审计准则》结合使用，为所要求的实务活动提供了权威依据。本指南全文均引用《准则》作为更详细信息的来源。

《专项要求》正式规定了内部审计人员如何应对常见的风险领域，以提升整个职业的质量和一致性。《专项要求》为执行与其主题相关的确认服务确立了基准并提供了相关标准（标准 13.4 评价标准）。确认服务必须遵循《专项要求》，咨询服务则建议遵循《专项要求》。《专项要求》并不打算覆盖开展确认业务时应考虑的所有潜在方面；相反，它的目的是提供一套最低要求，以便能够对有关内容进行一致、可靠的评估。

《专项要求》与国际内部审计师协会的“三线模型”和《准则》之间存在明确的关联。治理、风险管理和控制过程是《专项要求》的主要组成部分，与标准 9.1 了解治理、风险管理和控制过程保持了一致。根据“三线模型”，治理与董事会/治理机构相关，风险管理与第二线职能相关，控制或控制过程与第一线职能相关。管理层在一线和二线都有代表，而内部审计职能则作为第三线，以独立客观的方式提供确认，向董事会/治理机构报告（原则 8 接受董事会监督）。

适用性、风险和职业判断

当内部审计职能围绕《专项要求》的内容开展确认业务，或在其他确认业务中发现《专项要求》的某些内容时，必须遵循《专项要求》。

如《准则》所述，评估风险是首席审计执行官制定计划过程中的重要组成部分。要确定内部审计计划中应包括哪些确认业务，就必须至少每年评估一次组织的战略、目标和风险（标准 9.4 内部审计计划）。在为某个确认项目制定计划时，内部审计人员必须评估与项目相关的风险（标准 13.2 项目风险评估）。

如果在基于风险的内部审计计划过程中发现了《专项要求》的有关内容，并将其纳入审计计划，则必须使用《专项要求》中列出的要求来评估适用业务中的相关内容。此外，当内部审计人员开展审计业务（无论是否包含在计划中）时，如果出现了《专项要求》包含的要素，则必须将《专项要求》的适用性作为业务的一部分进行评估。最后，如果内部审计人员要求开展一项原本不在计划中的工作，但其中包含该相关内容，则必须对《专项要求》的适用性进行评估。

职业判断在应用《专项要求》方面发挥着关键作用。风险评估促使首席审计执行官决定将哪些审计项目纳入内部审计计划（标准 9.4 内部审计计划）。此外，内部审计人员还须利用职业判断来确定每个审计项目将包含哪些方面（标准 13.3 项目目标和范围、13.4 评价标准和 13.6 项目工作方案）。附录 A “实际应用示例”介绍了内部审计人员如何确定《专项要求》是否适用。

必须保留对《专项要求》中所有要求的适用性进行评估的证据，包括解释排除任何要求的理由。必须使用标准 14.6 项目文档中所述的内部审计人员职业判断来记录是否遵循了《专项要求》。

虽然《网络安全专项要求》提供了需要考虑的控制过程的最低要求，但将网络风险水平评估为非常高的组织可能还需要评估其他方面。

如果首席审计执行官认定内部审计职能不具备就《专项要求》有关内容开展审计业务所需的知识，则可将项目外包（标准 3.1 胜任能力、7.2 首席审计执行官的资格、10.2 人力资源管理）。即使如此，外包也不能免除内部审计部门遵循《专项要求》的责任。首席审计执行官仍负有确保遵循要求的最终责任。此外，如果认定内部审计资源不足，首席审计执行官必须告知董事会资源不足的影响以及如何解决资源短缺问题（标准 8.2 资源）。

执行、归档和报告

在运用《专项要求》时，内部审计人员还必须遵守《准则》，按照“领域五：实施内部审计业务”的要求开展工作。领域五中的标准描述了为审计项目制定计划（原则 13 有效计划项目）、实施审计项目（原则 14 实施项目）和沟通项目结果（原则 15 沟通项目结果和监督行动计划的执行情况）。

根据内部审计人员的职业判断，《专项要求》的覆盖范围可记录在内部审计计划或项目工作底稿中。一个或多个内部审计项目可能会涵盖这些要求。此外，并不一定所有要求都适用。必须保留对《专项要求》的适用性进行评估的证据，包括解释任何排除情况的理由。

附录 C 中的可选工具可用作参考，并记录内部审计人员工作开展的情况。

质量保证

《准则》要求首席审计执行官制定、实施和维护覆盖内部审计职能所有方面的质量保证和改进程序（标准 8.3 质量）。审计结果必须向董事会和高级管理层通报。沟通内容中必须包含内部审计职能是否遵循《准则》以及绩效目标的实现情况。

在质量评估中将对是否遵循《专项要求》进行评价。为准备对质量的检查，内部审计人员可使用附录 C 中提供的工具。

网络安全

网络安全是一个宽泛的话题，涉及任何组织的大多数技术方面。除信息技术外，网络安全通常也是业务流程的一部分，这就要求内部审计人员在规划、确定审计范围和实施确认业务时，评估与网络相关的风险。

隶属于美国商务部的美国国家标准与技术研究院（NIST）将网络安全简单定义为“保护或防御网络空间使用免受网络攻击的能力”。《网络安全专项要求》重点关注组织为降低来自未授权用户和恶意网络威胁的风险而确保安全的外部边界。网络安全是总体信息安全的一个子集，NIST 将其定义为 "保护信息和信息系统免遭未经授权的访问、使用、披露、干扰、修改或破坏，以提供保密性、完整性和可用性"。

《网络安全专项要求》包括：

- 治理——明确定义的支持组织目标、政策和程序的网络安全最低目标和战略。
- 风险管理——识别、分析、管理和监控网络威胁的流程，包括迅速上报网络风险的流程。
- 控制——由管理层制定并定期评估用于降低网络风险的控制过程。

考虑因素

内部审计人员可使用以下考虑因素来帮助评估网络安全专项要求。这些考虑因素与要求相互参照，是说明性的，但不是强制性的。内部审计人员在确定评估内容时应依靠职业判断。

治理方面的考虑因素

为评估如何将治理程序应用于网络安全目标，内部审计人员可检查以下内容：

A. 正式、书面的网络安全战略计划和目标，包括董事会定期（一般每季度一次）审查信息安全职能部门负责人（如首席信息安全官，即 CISO）提供的网络安全最新情况的证据。证据可包括以下方面的报告：
   - 对战略目标实现情况的监测。
   - 支持网络安全目标和目的的预算需求。
   - 对风险和内部控制的关注，包括补救措施的进展情况。
   - 衡量成功的关键绩效指标（KPI）。
   - 聘用、培训和培养网络安全人员所需的人力资源。

B. 用于管理网络安全流程的政策、程序和其他相关文件，包括：
   - 至少每年审查和更新一次政策。新出现的网络风险可能需要更频繁地进行审查和更新。
   - 确定政策和程序是否足以支持网络安全操作的程序。
   - 得到广泛采用的框架（NIST、COBIT 等），用于加强网络安全流程和内部控制。

C. 支持实现网络安全目标的角色和职责，包括确保网络安全职能向组织内适当层级进行汇报以获得组织支持的报告结构。
   - 定期评估担任网络安全职务人员的知识、技能和能力的程序。

D. 与利益相关方（如高级管理层、运营部门、风险管理部门、人力资源部门、法律部门、合规部门、战略供应商及其他部门）接触的证据，包括就现有和新出现的网络风险以及已知的潜在漏洞进行沟通。沟通证据可包括会议记录、报告或电子邮件。

风险管理方面的考虑因素

为评估如何将风险管理程序应用于网络安全目标，内部审计人员可检查以下内容：

A. 组织如何评估和管理网络安全风险，包括如何应对威胁和漏洞：
   - 首次被发现并予以报告。
   - 接受分析，评估其为实现组织目标带来的风险。
   - 缓解风险，包括将风险降低到可接受水平的行动计划。

- 进行监测，包括制定持续报告计划，直至威胁得到完全解决。

B. 组织如何从信息技术、企业风险管理、人力资源、法律、合规、运营、会计和财务等职能领域定期获取有关网络安全风险管理的意见。可利用跨职能网络安全团队或 IT 指导委员会来获取信息。

C. 组织如何将网络安全风险管理的责任和义务分配给个人或团队。

- 负责人应定期（每季度、每月或根据需要）在整个组织内传达持续的网络安全风险情况更新，还可包括缓解风险战略的资源要求。

D. 网络安全风险的上报流程，包括如何对威胁或风险等级进行评估、分配并确定优先级。检查内容可包括确定：

- 本组织定义的风险等级（如高、中、低），并详细说明每个风险等级和每个风险类型的上报程序。
- 目前确定的网络安全风险清单以及每个风险事件的缓解情况。
- 适用的法律、法规和合规要求。
- 财务和非财务（如声誉）风险影响。

E. 向管理层和员工传达网络安全风险的流程，包括：

- 定期（至少每年一次）对员工进行网络安全培训，如突击模拟网络钓鱼活动，以测试和跟踪组织范围内对该事项的认识水平。
- 现有网络安全问题的最新补救情况，以及预计完成日期。
- 监测不合规情况，包括向董事会和高级管理层报告最新情况。
- 当组织的风险偏好和风险容忍度发生变化时，重新评估威胁。

F. 组织在事件响应和恢复方面实施的流程，包括：

- 随着组织业务的不断变化而进行审查和更新的书面计划。计划应包括：
  - 如何发现和报告事件。
  - 如何控制事件以防止进一步的破坏。
  - 组织将如何恢复和应对，以恢复运营。
  - 如何对事件进行分析，以确定吸取的教训以及如何防止今后发生类似事件。
- 定期（至少每年一次）测试（桌面演练），并向高级管理层和相关利益方报告结果。通过测试可能会形成行动计划。

控制过程方面的考虑因素

为评估如何将控制过程应用于网络安全目标，内部审计人员可检查以下内容：

A. 管理层建立有效网络安全内部控制环境的方法，包括：
   - 根据组织风险评估流程，评估并实施必要的内部控制措施，以降低高风险并保护敏感、重要、个人或机密数据。
   - 确定维护关键网络安全控制所需的资源。
   - 将基于供应商的控制措施视为控制环境的一部分，包括在开始业务关系之前和整个关系期间审查供应商提交的服务组织控制（SOC）报告。
   - 定期测试网络安全控制措施的运行情况，确定其是否能够降低风险并支持网络安全目标的实现。
   - 纠正内部控制缺陷或处理内部审计职能部门或其他确认提供方所做评估（如渗透测试）中发现的问题的流程。

B. 组织招聘和培训网络安全专业人员的人才管理流程，包括组织如何确定机会，提高网络安全专业人员的能力，以支持技术知识和提高组织对新问题的认识。
   - 这方面的例子包括参加培训、参与知识共享小组，以及包括获得网络相关认证在内的持续职业教育。

C. 管理层为日常运营持续识别、监控和报告新出现的网络安全威胁和漏洞的流程，并为其按优先级排序。检查内容可包括是否建立了评估与新技术或新兴技术（如人工智能的使用）相关的威胁和漏洞的流程。

D. 管理层为在整个生命周期内管理和保护 IT 资产（包括硬件、软件和供应商服务的选择、使用、维护和停用）而制定的流程和控制措施。硬件包括服务器、网络设备（如路由器或防火墙）、台式机、笔记本电脑、手机、平板电脑和外围设备。软件包括操作系统（如 Windows）、企业资源规划软件、应用程序、防病毒程序等。硬件和软件考虑因素可能包括：
   - 组织使用加密、防病毒软件、移动设备管理、复杂的密码要求、虚拟专用网络（VPN）/零信任网络（ZTN）进行身份验证，以及定期更新固件。
   - 资产管理流程，确保公司发放的硬件在发放时具有适当的安全配置，并在资产退役时进行妥善处置。
   - 与数据库相关的控制措施，包括限制用户和管理员的访问权限、确保使用加密技术、备份和测试数据库，以及采取强有力的网络安全控制措施。
   - 如何在系统开发生命周期 (SDLC) 中考虑网络安全威胁或漏洞。
   - 开发、安全和运营（DevSecOps）为确保软件开发流程包含网络安全以主动识别漏洞而采用的方法。

E. 用于加强网络安全的程序，包括：

- 为将网络安全风险降至最低进行安全设置配置。
- 对移动设备管理（包括电子邮件和应用程序的使用）进行配置，以降低网络安全风险，并在用户设备被攻陷时进行远程管理。
- 对“静态”数据（如硬盘上存储的信息）或“传输中”数据（如加密电子邮件）使用加密。
- 为服务器或软件（如操作系统）打上最新版本的安全补丁。
- 用户访问管理，如使用多因素身份验证（MFA）和带有定期过期的复杂密码的唯一用户 ID。
- 监测已存在的控制措施，以确定可用性和资源利用是否充分，从而能够检查和分析威胁控制效能发挥的潜在网络安全问题。
- 将网络安全纳入 SDLC，以便在软件投入生产前发现并解决网络安全漏洞。

F. 确保组织周边安全的网络相关控制措施，包括组织如何利用：
- 网络分段。
- 防火墙。
- 用户访问控制。
- 外部和内部连接的限制。
- 围绕互联网络的物联网 (IoT) 的控制措施。
- 入侵检测/预防系统，用于预防、检测和恢复网络安全攻击。

G. 适用于电子邮件、互联网浏览器、视频会议、消息发送（Zoom、MS Teams 等）、社交媒体、云和文件共享协议等服务的端点通信安全控制。控制措施可包括限制使用某些文件扩展名（如 .exe 文件）和文件共享的多因素身份验证。

附录 A.实际应用示例

以下示例描述了适用《网络安全专项要求》的情况：

示例 1：网络安全被确定为内部审计计划内的一项内部审计工作。

当内部审计职能部门完成其基于风险的计划流程，并在内部审计计划中包含一个或多个有关网络安全的审计项目时，开展此类项目必须遵循《专项要求》。可通过在内部审计计划的一个或多个项目中纳入要求来实现一致性。

网络安全是一个宽泛的主题，《专项要求》中的所有要求并不一定都适用于每个项目。当内部审计人员运用职业判断，确定《网络安全专项要求》中的一项或多项要求不适用，因此应排除在审计项目之外时，内部审计人员必须记录并保留排除这些要求的理由。例如，排除某些要求的理由可能是内部审计职能轮流实施各种网络安全项目，或已确定该风险在项目中的重要性较低。

示例 2：在某个不以网络安全为重点的审计项目中发现了网络安全风险。

内部审计人员在评估与网络安全无直接关系的流程时，也有可能会发现网络安全风险。例如，内部审计人员可能会在某个不以网络安全为重点的审计项目中评估应付账款流程，并且在计划项目时未将网络安全风险确定为工作范围内的风险。然而，在执行初步穿行测试后，内部审计人员确定此类风险应在范围之内；例如，他们确定了与基于网络提交初始采购订单请求有关的网络安全风险（标准 13.2 项目风险评估）。

一旦确定存在相关风险，内部审计人员必须查阅《网络安全专项要求》，并确定哪些要求适用。在本示例中，他们可能会排除网络安全治理程序或网络安全风险管理程序。他们必须在参与项目工作底稿中记录排除《网络安全专项要求》中其他要求的理由，并保留该文件。

示例 3：要求开展最初未列入内部审计计划的网络安全审计项目。

董事会、管理层或监管机构等利益相关方可能会要求内部审计人员在原审计计划之外执行网络安全评估。例如，当组织成为网络攻击的目标时，董事会可能会要求内部审计人员参与评估网络安全控制。《专项要求》是适用的，必须对其要求进行评估，并对任何认定有关要求不适用的情况进行记录。

附录 B.与框架的对应关系

组织可能已经开展了自己的网络安全工作，使用 COBIT 或 NIST 等风险管理和治理框架。内部审计人员可能已经根据这些框架制定了审计计划和测试程序。内部审计人员应将其计划的网络安全控制测试与《专项要求》进行对照，以确保足够的覆盖范围。下图对《网络安全专项要求》与三个常用框架之间的对应关系进行了解析，包括：NIST 网络安全框架（CSF）2.0、COBIT 2019 和 NIST 800-53。之所以选择这些框架进行对照，是因为它们可以免费获取。

治理要求	对应框架的内容		
	NIST CSF 2.0	NIST 800-53	COBIT 2019
A.制定并定期更新正式的网络安全战略和目标。定期通报实现网络**安全目**标的最新情况，并由董事**会**进行审查，包括支持网络安全战略的资源和预算考虑。	GV.RM-01；GV.RM-02；GV.RM-03；GV.RM-04；GV.OC-02；GV.RR-03；GV.RR-04；GV.PO-01；GV.PO-02；GV.OV-01；GV.OV-03	PM-1，PM-4；AT-2；AT-3；PM-9；PM-28	EDM01；EDM03；EDM04；APO06；APO01；APO10；APO12
B.制定并定期更新与网络安全有关**的政策和程序**，以**加**强控制环境。	GV.PO-01；GV.PO-02；GV.OV-01；GV.OV-02；GV.OV-03；GV.SC-01；GV.SC-03；GV.RR-03	AC-1，PM-9；AC-1；AT-1；CA-1；CM-1；IA-1；IR-1；MP-1；PE-1	EDM01；EDM02；EDM03；APO01；APO11
C.确立了**支持网**络安全目标的角色和职责，**并制定**了**定期**评估担任这些角色的人员的**知**识、技能和能力的程序。	GV.RR-02；GV.RR-04；GV.SC-02；GV.OC-02	PM-13；AT-2；AT-3	EDM02；APO01；APO07

D.有关**利益**相关 **方参与**讨论网络安全环境中的现**有漏洞和新**出现的**威**胁，并采取相应行动。利益相**关**方**包括高**级管理层、运营、风险管**理、人力**资源、法务、**合**规、供应商及其他部门。	GV.OC-02；GV.RM-01；GV.RM-05；GV.RM-07；GV.OV-03；GV.SC-03	AC-1; CM-1	EDM05；EDM01.01；EDM03；MEA01.02；APO01；APO08；APO11；APO13；MEA02
风险管理要求	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A.组织的风险评估和风险管理程序，包括识别、分析、降低和监控网络安全威胁及其对实现战略目标的影响。	GV.RM-01；GV.RM-03；GV.OC-01	AT-1；PM-9；PM-28	EDM03；APO01；APO10；APO12
B.网络安全风险管理在整个组织内得以实施，**可能包括以下**领域：信息技术**、企**业风险管理、人力资源、法务**、合**规、运营、供应链、会计、财务及其他。	GV.RM-01；GV.RM-05；GV.RR-01；GV.RR-02；GV.OC-03；GV.SC-07	PM-29；AT-1；PM-9；PM-28	EDM03；APO01；APO10；APO12
C.建立网络安全风险管理的问责制**和**责任制。**确定个人或**团队定期监测和报告**网**络安全风险的管理情况，包括缓解风险和识别新出现的网络安全威胁所需的资源。	GV.RR-01；GV.RR-02；GV.RR-03；GV.0V-01；GV.OV-02；GV.OV-03	PM-9; PM-29	EDM03；APO01；APO10；APO12
D.根据组织既定的风险管理指引**或**为适用的法律法规**要求，建立**了相关**流程，以迅速上**报任何达到**不可接受水平的网**络安全风险（**新出**现的或以前发现的）。应考虑网络安全风险的财务和非财务**影响。**	GV.RM；ID.RA；RS.MA-04	CA-7；RA-3；RA-7	EDM03；APO01、APO10；APO12

E.建立向管理层和员工传播**网**络安全风险意识的流程，并由**管理**层定期检查问题、差距、缺陷或控制失败，及时报告和采取补救措施。	GV.PR.AT；GV.RR.01；GV.RR-04；GV.PO	AT-2	APO01；APO02；EDM03；MEA03
F.组织已实施网络安全事件响应和**恢复流程，包括**检测、控制**、恢复和事件后分析。定期**测试**事件响**应和恢复流程。	RS; RC	IR-4；IR-5；IR-6；IR-7；IR-8；IR-10；SA-15	DSS02；DSS03；DSS04；DSS05.07
控制过程要求	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A.建立相关程序**，确保内部控制和基于供**应商的**控制**得以实施**，以保**护组织系统和数据的保密**性、完整性和可用性。定期**对控**制措施**进行评估，以确定其运作**方式能否促**进组织网络安全目标**的**实现和问题的迅速**解决。**	ID.IM-01；ID.IM-02；ID.IM-03；PR；DE；RS；RC；ID.RA06；GV.RM-05；GV.SC；ID.IM-02；RS.MA-01；DE.CM-06	AC-3; AC-4; AC-10; AC-13; AC-17; PM-30; RA-3; SA-9; SR-2	MEA02；MEA04；EDM03；APO09；APO10；DSS01
B.为网络安全业务建立人才管理流**程并定期**审查，其中包括开发和**保持**网络安全操作**技**术胜任**能力的培**训机会。	PR.AT-01；PR.AT-02；GV.RR-03	AT-2；AT-3；IR-2；PM-14	APOO7; DSS04
C.建立相关程序**，以持**续监控和报告新出现的网络安全威胁和漏洞，确定和实施**改**进网络安全操作的机会并为其确定优先级。	ID.RA-02；ID.RA-03，ID.RA-04	CA-7；PM-31；RA-5	DSS03.05
D.网络安全被纳入所有信息技术资产（包括硬件、软件和供应商服务）的生命周期管理（选择、使**用、**维护和停用）中。	ID.AM；PR.PS-03；PR.IR；DE.CM-09；ID.AM-08；ID.RA-09；PR.PS-06	AU-9；CM-7；SC-49；SC-51；CM-2；SA-3；SA-10；SA-15；SA-17；SA-20；AU-6；IR-7	DSS05.03；BAI03；BAI09；BAI03；BAI11；DSS05.01；DSS02；DSS03；DSS06.06

E.建立促进网络安全的流程，包括**配置、**终端**用**户设备管理、加密、打补丁、**用**户访问管理以及监控可用性和**性能。将网**络安全因素纳入软件**开**发（DevSecOps）中予以考虑。	PR.PS-01；PR.PS-06；PR.DS-01；PR.DS-02；PR.PS-05；DE.CM-03	cm-6; si-2; ac-3; ca-7; sa-4; ac-16; ac-18	BAI10；DSS05；DSS06.03；DSS01.03；MEA01
F.建立与网络相关的控制措施，如**网**络访问控制和分段；使用和设置**防火**墙；限制与外部网络的连接；**虚**拟专用网络（VPN）**/零信任网**络访问（ZTNA）；**物**联网（IoT）网络控制措施；**以及入侵**检测**/防御系**统（IDS **和** IPS）。	pr.ir; de.cm-01	AC-6; AC-17; AC-18; AC-20; SC-7; SC-10; CA-8	DSS05.02
G.针对电子邮件、互联网浏览器、视频会议、信息发送**、社交媒体、云**计算和文件共享协议等服务建立了端点通信安全**控制**。	PR.DS-01；PR.DS-02；PR.DS-10；PR.IR	AC-2；AC-16；AU-10；CA-3；SI-8；SI-20；SC-8	BAI10

附录 C.可选文档工具

内部审计人员应在风险评估的基础上，运用职业判断确定要求的适用性，并适当记录某些要求的排除情况。专项要求可根据审计人员的职业判断记录在内部审计计划或审计工作底稿中。一个或多个内部审计项目可能涵盖这些要求。此外，并非所有要求都适用。下面的可打印表格为记录《网络安全专项要求》的遵循情况提供了一种选择，但并非必须使用。

网络安全 – 治理

要求	已执行的覆盖范围或排除理由	文件参考
A.制定并定期更新正式的网络安全战略和目标。定期通报实现网络安**全目**标的最新情况，并由董事会进行审查，包括支持网络安全战略**的**资源和预算考虑。		
B.制定并定期更新与网络安全有关的政策和程序，加强控制环境。		
C.确立支持网络安全目标的角色和职责，并制定定期评估担任这些角**色的人**员的知识、技能和能力的程序。		
D.让利益相关**方参与**讨论网络安全环境中现有的漏洞和新出现的威胁，并采取相应行动。利益相关方**包括高**级管理层、运营、风险管理、人力资源、法务**、合**规、供应商及其他。		

网络安全 – 风险管理

要求	已执行的覆盖范围或排除理由	文件参考
A.组织的风险评估和风险管理程序包括识别、分析、缓解**和**监控网络安全威胁及其对实现战略目标的影响。		

要求	已执行的覆盖范围或排除理由	文件参考
B.网络安全风险管理在整个组织内得以实施，**可能包括以下**领域：信息技术、企业风险管理、人力资源、法律、**合**规、运营、供应链、会计、财务及其他。		
C.建立网络安全风险管理的问责制和责任制。确定个人或团队定期监测和报告网络安全风险的管理情况，包括降低风险和识别新出现的**网**络安全威胁所需的资源。		
D.根据组织既定的风险管理指引**或适用的法律法**规要求，建立了相关**流程，以迅速上**报达到不可接受水平的任何网络安全风险（新出现**的或以前**发现的）。应考虑网络安全风险的财务和非财务影响。		
E.建立向管理层和员工传播**网**络安全风险意识的流程，并由管理层定期检查问题、差距、缺陷或控制失败，**及**时报告并采取补救措施。		
F.组织已实施网络安全事件响应和恢复流程，包括检测、控制**、恢复和事件后分析。定期**测试事件响应和恢复流程。		

网络安全--控制过程

要求	已执行的覆盖范围或排除理由	文件参考
A.建立相关程序，**确保内部控制和基于供**应商的控制得以实施，**以保**护组织系统和数据的保密性、完整性和可用性。定期对控制措施进行评估，以确定其**运作方式是否**能促进组织网络安全目标的实现**和**问题的**迅速解决。**		
B. 为网络安全业务建立人才管理流程并定期审查，其中包括开发和保持网络安全操作技术能力的培训机会。		

要求	已执行的覆盖范围或排除理由	文件参考
C. 建立相关程序，以持续监控和报告新出现的网络安全威胁和漏洞，确定和实施改进网络安全操作的机会，并为其确定优先级。		
D.网络安全被纳入所有信息技术资产（包括硬件、软件和供应商服务）的生命周期管理（选择、使用、维护和停用）中。		
E.建立促进网络安全的流程，包括配置、终端用户设备管理、加密、打补丁、用户访问管理以及监控可用性和性能。将网络安全因素考虑纳入软件开发（DevSecOps）中予以考虑。		
F.建立与网络相关的控制措施，如网络访问控制和分段；使用和设置防火墙；限制与外部网络的连接；虚拟专用网络（VPN）/零信任网络访问（ZTNA）；物联网（IoT）网络控制措施；以及入侵检测/防御系统（IDS 和 IPS）。		
G.针对电子邮件、互联网浏览器、视频会议、信息发送**、社交媒体、云和文件共享**协议等服务建立端点通信安全控制。		

关于国际内部审计师协会

国际内部审计师协会（IIA）是一个国际性专业协会，在全球拥有 255,000 多名会员，并在全球颁发了 200,000 多张注册内部审计师® (CIA®) 证书。IIA 成立于 1941 年，是全球公认的内部审计职业标准、认证、教育、研究和技术指导的领导者。欲了解更多信息，请访问 www.theiia.org。

免责声明

IIA发布本文件的目的是提供信息和开展**教育**。**本**资料无意为具体的个案

情况提供明确的答案，**因此**仅供参考。IIA**建**议就任何具体情况直接寻求独立专家的意见。对于完全依赖本材料的任何人，IIA **不承担任何**责任。

版权

2025 年 2 月

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101