网络安全

Topical Requirement

专项要求

The Institute of
Internal Auditors

网络安全专项要求

《专项要求》作为一项强制性要素，与《全球内部审计准则 (Global Internal Audit Standards™)》和《全球指南》共同组成了《国际内部审计专业实务框架 (International Professional Practices Framework®)》。《专项要求》应与《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。

《专项要求》通过设定特定风险专项审计的最低基本要求，为内部审计人员提供了明确的期望。组织的风险状况可能要求内部审计人员考虑有关问题的其他方面。

遵循《专项要求》将提高内部审计服务的一致性，并提高内部审计服务和结果的质量和可靠性。最终，《专项要求》将提升内部审计职业的水平。

内部审计人员在运用《专项要求》的时候必须遵循《全球内部审计准则》。确认服务必须遵循《专项要求》，咨询服务则推荐遵循《专项要求》。

《专项要求》在以下情况适用：

A. 其覆盖领域是内部审计计划中包含的审计项目的审计对象。
B. 在开展审计项目时发现与其覆盖领域属有关的问题。
C. 其覆盖领域属是未列入原内部审计计划的审计项目的审计对象。

必须记录并保留对《专项要求》中每项要求的适用性进行评估的证据。并非所有要求都适用于每个审计项目；如果认定某项要求不适用，必须记录并保留理由。遵循《专项要求》是强制性的，质量评估中将对遵循情况进行评估。

如需了解更多信息，请参阅《网络安全专项要求用户指南》。

网络安全

美国国家标准与技术研究院（NIST）将网络安全简单定义为：“保护或捍卫网络空间使用免受网络攻击的能力”。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”。

网络安全通过加强整体控制环境，保护组织的信息资产免遭未经授权的访问、破坏、篡改或毁坏，从而降低风险。由于计算机、网络、程序、数据和敏感信息是大多数组织的重要组成部分，因此网络攻击可能导致直接和间接的影响，且这样的影响往往是重大的。

评估网络安全治理、风险管理和控制过程

本专项要求为评估网络安全治理、风险管理和控制过程的设计和实施提供了一致、全面的方法。这些要求是评估组织网络安全的最低基本要求。

治理：评价和评估网络安全治理

要求：

内部审计人员必须评估与组织网络安全治理相关的以下内容：

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，以加强控制环境。
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。
D. 有关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、供应商及其他部门。

风险管理：评价和评估网络安全风险管理

要求：

内部审计人员必须评估与组织的网络安全风险管理有关的以下内容：

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。
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。
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。
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。
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. 组织已建立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。

控制：评价和评估网络安全控制过程

要求：

内部审计人员必须评估与组织网络安全控制过程相关的以下内容：

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的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胜任能力的培训机会。

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）。

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。

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；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）是一家国际性专业协会，在全球拥有 255,000 多名会员，并在全球颁发了 200,000 多张国际注册内部审计师® (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。

版权

2025 年 2 月

The Institute of Internal Auditors

全球总部
美国佛罗里达州玛丽湖
1035 Greenwood Blvd.
电话：+1-407-937-1111+1-407-937-1111
传真： +1-407-937-1101