网络安全专项要求

什么是《专项要求》？

《专项要求》是《国际内部审计专业实务框架》®的重要组成部分，该框架还包括《全球内部审计标准》™（以下简称《标准》）和《全球指南》。作为内部审计职业标准的制定者，国际内部审计人员协会要求将这些强制性《专项要求》作为《标准》的补充，同时将《标准》作为《专项要求》中所述和引用的必要实践的权威性依据。

《专项要求》为全球内部审计工作中常见的专项问题提供了指引，这些问题通常具有较高风险和普遍性。虽然《标准》适用于所有内部审计服务，但当某专项问题成为内部审计业务的重点时，还必须同时遵循相关的《专项要求》提出的额外强制性要求。

《专项要求》应在实体或组织层面应用于对整个组织有影响的专项问题。内部审计人员必须熟悉《专项要求》，并在专项问题被列入年度审计计划时，或在特定专项问题成为内部审计工作的重点时，做好应用《专项要求》的准备。在确定业务范围时，必须对《专项要求》的要素进行评估。必须记录并保留对专项问题进行评估和处理的证据。只要内部审计业务中包括了专项问题任何方面，都必须评估与业务相关的要求，或记录特定要求不适用的原因。附录 B 提供了工具，用于协助内部审计人员解释纳入或排除要求的理由。

为什么需要《专项要求》？

应用《专项要求》的目的在于加强内部审计职能与不断变化的全球风险环境的持续相关性，并提高各行业和部门内部审计服务的价值。遵循《专项要求》将有助于内部审计人员提高业务质量和一致性。

《专项要求》的结构为在三个领域开展内部审计服务提供了指导：治理、风险管理和控制流程。每个领域包括：

- 要求，强制性要素，涵盖了组织的基本目标。
- 考虑因素，非强制性要素，作为评估组织目标设计和实施的最佳实务。附录 A 提供的考虑因素仅作为证明要求得到遵循的示例。

质量评估将对是否遵循《专项要求》进行评价。在准备质量检查时，内部审计人员应使用附录 B 中提供的工具来说明是否遵循每项要求，或解释未达到要求的原因。

网络安全专项要求

评价和评估网络安全的治理、风险管理和控制流程的有效性

网络安全保护组织的信息资产免遭未经授权的用户、破坏、篡改或毁坏，并加强整体控制环境以降低风险。由于计算机、网络、程序、数据和敏感信息是大多数组织的关键组成部分，因此网络攻击可能导致直接和间接的影响

，而且影响往往很大。由于组织在很大程度上依赖信息技术资源，明确界定网络安全计划、目标、固有风险和有效控制应成为管理层的优先事项。

本专项要求为评估网络安全治理、风险管理和控制流程的设计和实施提供了一致、全面的方法。

治理：评价和评估网络安全治理

要求：

在执行包含网络安全目标的内部审计任务时，内部审计人员必须评估组织的治理流程能否充分应对网络安全问题。内部审计人员必须评估是否 ：

A. 制定并定期更新与网络安全风险管理流程相关的政策和程序，包括推动基于广泛采用的框架（NIST、COBIT 等）加强控制环境的实践。

B. 明确规定支持组织网络安全目标的角色和职责，并由具备所需知识、技能和能力的人员担任这些角色。

C. 定期向董事会通报网络安全目标、战略、风险和用于降低风险的控制措施的更新情况。

D. 有关利益相关方（如领导层、运营部门、战略供应商等）参与讨论如何以最佳方式建立和改进网络安全风险管理流程。

E. 向董事会通报有效执行网络安全风险管理流程所需的资源（如领导力、资金、人才、硬件、软件和培训等）。

风险管理：评价和评估网络安全风险管理

要求：

在执行包含网络安全目标的内部审计工作时，内部审计人员必须评估组织的风险管理程序能否充分应对网络安全问题。内部审计人员必须评估是否：

A. 建立全组织范围的风险管理流程，包括识别、分析和管理与信息技术和安全有关的风险，特别关注网络安全风险以及这些风险可能如何影响实现组织目标的能力。

B. 由一个跨职能团队负责执行网络安全风险管理流程，该团队包括信息技术领导层、整个组织的风险管理、法律、合规、其他管理层（运营、会计、财务等），并酌情吸收外部各方（供应商、外包服务提供商、供应商、客户等）参与。

C. 制定并定期更新网络安全风险管理政策和程序，包括推广基于广泛采用的风险管理框架、权威指南或其他最佳实践的加强网络安全风险管理流程的做法。

D. 建立了网络安全风险管理的问责制和责任制，并确定了个人或团队定期监测和通报网络安全风险的管理情况，包括降低风险所需的资源，以及识别以前未识别的新兴网络安全风险。

E. 根据组织既定的风险管理指引，或为遵守适用的法律和/或监管要求，建立对应的流程，以便在网络安全风险（新出现的或以前发现的）上升到不可接受水平时，快速上报风险。

F. 在网络安全风险管理过程中包括了信息安全、法律、合规和其他管理部门之间的协作，以确定并遵守所有法律和合同义务，如法律和法规等。遵循和不遵循适用要求的情况会定期在组织内部通报。

G. 建立流程来识别和管理与第三方有关的网络安全风险。根据合同要求，销售商、供应商和其他外包流程和/或服务提供商必须实施有效的网络安全控制措施，以充分保护第三方可访问的组织系统和数据的保密性、完整性和可用性。

H. **适当**设计和有效部署了与数据分类、保留、销毁和加密有关的政策和流程，以提供系统的方法，确保完整和准**确地**记录数据，并保护敏感信息的机密性和隐私。

I. 建立了网络安全操作风险沟通流程，确保管理层和员工都能意识到网络安全操作风险。任何问题、差距、缺陷或控制失**灵都会通**报给董事会和管理层，并密切监控和报告补救情况。及时发现、调查、报告和纠正不遵守网络安全政策的情况。

控制：评价和评估网络安全控制流程

要求：

在执行包含网络安全目标的内部审计任务时，内部审计人员必须评估组织的控制流程能否充分应对网络安全问题。内部审计人员必须评估组织是否：

A. **确定了网**络安全控制的优先顺序，确保分配相关预算和资源（如人员、软件、工具等），以实现预期效益最大化。

B. **确保网**络安全控制以促进实现组织网络安全目标和及时解决问题的方式运行。

C. 为负责网络安全操作的人员提供了充分的培训。

D. 制定了充分的政策和程序，以管理网络安全操作和相关控制的各个方面。

E. **确保了管理**层拥有必要的资源，能够随时了解新技术带来的新兴网络安全问题，确定改进运营的机会，并了解如何以最佳方式部署网络安全工作，以影响更广泛的组织目标和目的。

F. 将网络安全充分纳入了业务应用程序的系统开发生命周期，包括软件和购置或定制开发的应用程序等。

G. 已将网络安全纳入了硬件（如笔记本电脑、台式电脑、移动设备等）管理。

H. 已对生产硬件支持实施了有效的控制，如配置、打补丁、支持用户访问管理以及监控可用性和性能等。组织已对这些控制措施设计的适当性和运行的有效性进行了评估。

I. 优化了与网络相关的控制措施，包括网络分段、使用和部署防火墙、限制与外部网络和/或系统的连接，以及使用入侵检测/预防系统等预防和检测技术。

J. 对电子邮件、互联网浏览器、视频会议、信息传递和文件共享协议等常用桌面通信服务实施了有效控制。

K. 已实施适当的服务交付控制，确保网络安全监控已被整合进入以下领域：变更管理、服务/求助台和终端用户设备管理。

L. 已实施适当的实体安全控制，以保护高风险信息中心（如数据中心、网络运行中心和安全运行中心）免受攻击。

M. 已实施事件响应和恢复控制。

相关标准：

3.1 胜任能力
4.2 应有的职业审慎
9.1 了解治理、风险管理和控制流程
9.4 内部审计计划
12.3 监督和改进项目绩效
13.1 项目沟通
13.2 项目风险评估
13.3 项目目标和范围
13.4 评价标准
13.5 项目资源
13.6 项目工作方案
14.1 收集用于分析和评价的信息
14.2 分析和未确定的审计发现
14.3 审计评价
14.4 审计建议和行动计划
14.5 审计结论
14.6 项目文档
15.1 项目结果沟通
15.2 确认建议或行动计划的执行情况

相关的全球技术审计指南 (GTAG)：

评估网络安全风险：三线模型
业务应用程序审计
网络事件响应和恢复审计
网络安全运行审计：预防和检测
身份和访问管理审计
IT 治理审计
移动计算审计
网络和通信管理审计

附录 A.考虑因素

针对各项治理要求的考虑因素：

为评估如何将基本治理流程应用于网络安全目标，内部审计人员可检查以下内容：

A. 组织用于管理日常网络安全责任的政策、程序和其他相关文件，包括：
   1. 文件清晰、简明、一致，并定期更新。最好是在发现新的网络安全风险时及时更新，且至少每年更新一次。
   2. 与识别、分析、解决和报告敏感数据泄露或其他损失相关的程序。
   3. 管理层如何确保政策和程序足以支持网络安全运行的文件。

B. 董事会为支持实现网络安全战略而设立的角色和职责，包括有关网络安全的报告结构能够确保组织内适当的人员能够接收到有关信息，以为解决网络安全问题提供组织层面的支持。

C. 向董事会提交的有**关网**络安全战略、目标、风险和控制措施的材料，包括分析以下情况：
   1. **沟通**频率是否适当，最好每季度一次，并由信息安全职能部门的负责人（如首席信息系统官）介绍情况。
   2. 所提供的信息是否清晰、简洁、一致；风险和控制措施的传达方式是否易于董事会理解。
   3. 是否包括**关**键绩效指标或其他重要的网络安全指标/统计数据。
   4. 在**适当的情况下**，**管理**层能否收到董事会的意见并加以落实，是否将最新的变动情况反馈给董事会。

D. 管理层与相关利益相关方（如领导层、运营部门、战略供应商及其他）进行网络安全相关沟通的证据，包括**沟通的信息是否清晰、**简洁、一致，是否符合以下利益相关方受众的要求：
   1. 员工。
   2. 销售商、供应商、外包服务提供商和第三方。
   3. 客户。
   4. 战略合作伙伴。

E. 管理层对资源需求的分析和沟通，包括：
   1. 了解如何找出差距，以及利用**哪些关**键指标来预测需求的变化。
   2. 管理层如何与人力资源部门合作分析网络安全人才需求。
   3. 管理层如何分析当前的硬件和软件库存，并确定是否需要额外投资来支持网络安全举措。
   4. 内部审计员是否检查管理层如何建立和更新网络安全培训材料并找出差距，包括确保培训涵盖新出现的网络安全目标、风险和控制措施。

针对各项风险管理要求的考虑因素：

为评估网络安全风险管理的必要方面，内部审计人员可检查以下内容：

A. 管理层如何初步识别网络安全风险，包括
   1. 了解**哪些人**员负责组织面临的日常威胁和信息安全领域新出现的风险。
      a. **确**认这些人员是否具备相关的职业经历并接受了适当培训，能够有效发现和向风险管理团队上报有**关威**胁。
   2. **确定管理**层赖以识别网络安全风险的软件应用程序或供应商。
   3. 与网络安全风险管理流程有关的文件，包括：
      a. 会议记录。
      b. 行动项目。
      c. 参与人员或团队成员名单。
      d. 发生问题后的调查/根本原因分析。

B. 管理层如何确定或提名风险管理团队成员，以及用于评估成员的相关业务理由或资格。检查与相关外部机**构定期**讨论网络安全风险的证据。

C. 组织用于制定和定期更新网络安全风险管理相关政策和程序的流程，可能包括：
   1. 对政策和程序进行年度审查和批准。
   2. 了解组织如何确保其风险管理政策和程序得到遵守，以及如何对员工进行政策和程序执行方面的培训。
      a. 了解管理层使用哪些框架或权威指南来管理网络安全风险（如 NIST、COBIT 及其他），以及组织确认遵循所选框架的方式。

D. 负责执行网络安全风险管理的人员，包括确保其专业背景、经验、资格和证书适合管理信息安全风险和威胁。确认责任人在组织内的级别，以提高网络安全风险的可见度，并有效沟通这些风险。

E. 组织用于上报网络安全风险的流程，包括如何评估和确定威胁或风险等级并确定优先级。验证组织是否定义了风险等级（如高、中、低），包括对每个风险等级的详细解释和每类风险的上报程序。审核已识别的当前网络安全风险列表和各项问题的处置情况。

F. 组织为确保遵守所有适用的网络安全法规而采用的程序，包括：
   1. 计划或最新通过的法规对组织有何影响。
   2. 是否编制了适用法规清单，并定期监测、更新和报告，以确保组织充分了解有关情况。
      a. 对于任何不合规项目，核实管理层是否了解相关风险，包括通过定期报告沟通有关信息。

G. 组织管理第三方网络安全风险的流程。核实在开始业务关系之前对供应商的网络安全控制措施进行了审查，并在合同中规定了在整个关系中定期审查的权利。包括获取和分析第三方的服务组织控制报告，核实组织是否已将其 SOC 报告审查记录在案，其中应包括确保用户控制考虑因素已得到实施。了解管理层确定第三方是否拥有与组织控制相称的适当控制环境的方法。
   a. 如果发现第三方控制存在缺陷，了解管理层采用了哪些流程来确保这些缺陷不会危及与运营相关的网络安全，或者了解组织如何传达需要做出改变以维持适用的供应商关系，或可能需要找到替代供应商的信息。

H. 组织在以下方面制定的政策和流程：
   1. 数据分类。
   2. 数据保留。
   3. 数据销毁。

4. 加密。
5. 访问/身份管理。
6. 由谁来准备、审查和更新文件，其中最好包括法律和合规人员，以确保遵守适用法规。
7. 组织如何进行数据分类，以确保能够识别机密和私人数据，并配备适当级别的保护措施，如限制用户访问等。
8. 组织如何定期审查用于对数据进行分类的流程，以及该流程能否继续支持组织实现网络安全目标并遵守组织政策和适用法规。

I. 向管理层和员工传达网络安全操作风险的流程。理想情况下，此类沟通应包括定期网络安全培训（至少每年一次）。了解管理层通报现有网络安全问题补救措施最新情况及预计完成日期的流程。核实是否对不合规情况进行密切监控，并向董事会和高级管理层提供最新信息。

针对各项控制流程要求的考虑因素：

为评估网络安全控制的必要方面，内部审计人员可检查以下方面的内容：

A. 管理层确定如何部署预算资源以支持网络安全控制环境的流程，其中应包括每年的战略规划，以确保有适当水平的组织资源用于实现网络安全目标。应检查年度规划和资源管理定期监测的以书面记录形式呈现的正式结果。

B. 管理层定期评估网络安全控制措施是否以促进实现组织网络安全目标的方式运行的流程。核实管理层是否监控控制措施的有效性，评估现有控制措施是否设计得当或是否需要新的控制措施。在许多组织中，内部审计职能在此过程中发挥着重要作用，通过定期（季度、年度）测试，为控制设计和控制是否有效运行提供确认。核实管理层弥补控制缺陷或处理内部审计职能部门或其他确认提供方评估（如渗透测试）结果的流程。

C. 管理层评估组织内网络安全人员培训需求的流程，以及如何分配资源以提供适当的教育，并确保新兴网络安全威胁得到理解和管理。了解管理层如何确保员工获得足够的网络安全培训，其中可能包括现场培训活动、录制的教学或完成培训模块。

D. 组织创建和更新网络安全政策和程序的流程，以及管理层如何评估上述政策和程序是否充分。了解如何对负责网络安全运营和控制的人员进行遵守政策和程序的培训，以及如何对他们进行内部合规评估。

E. 组织对负责网络安全运营和控制的管理团队进行适当培训的流程，以发展新趋势，并为上述团队和整个组织提供战略领导力。了解组织如何发现提高管理层能力的机会，通过组织培训和继续职业教育等方式，帮助他们更好地认识新兴问题。

F. 组织如何在系统开发生命周期内解决网络安全问题，包括以下阶段的控制：
   1. 计划阶段：网络安全已被确定为评估风险和分析潜在漏洞的关键组成部分。组织在计划阶段评估网络安全控制措施时，应包括软件实现的范围和目标。
   2. 收集需求阶段：在定义功能要求时，应将网络安全要求纳入考虑，包括遵守所有适用的法律法规要求。
   3. 设计阶段：将网络安全考虑因素纳入对具体处理要求的考虑。随着组织更正式地确定系统架构设计的需求（如平台、用户界面、数据库等），应在所有设计方面确定控制措施。
   4. 开发：组织已建立安全的环境，并正式确定开发流程，以最大限度地减少网络漏洞（例如，限制用户访问开发代码、与生产环境适当隔离、使用经批准的工具、存在跟踪开发活动的审计跟踪、对供应商开发的软件提出具体的网络安全要求等）。

5. 测试：组织在测试阶段对网络安全进行审查和评估（如自动测试、渗透测试和漏洞评估等）。组织应能迅速知晓并处理通过测试发现的任何网络漏洞，其中包括对漏洞的详细描述，以及为应对漏洞而进行的代码更改或建立的控制措施。
6. 部署：当新软件投入生产时，组织应仔细监控潜在的网络安全威胁，包括确保终端用户接受了软件使用培训，以最大限度地降低网络安全风险。组织应确保记录和分析与潜在网络安全问题相关的事件和错误。
7. 维护：组织应确保及时应用所有与安全相关的软件版本，并应与软件供应商保持畅通的沟通，以确保新出现的风险和威胁得到适当控制，并确保终端用户了解任何已知的漏洞。

G. 组织为保护硬件（如台式机、笔记本电脑、移动设备和其他设备等）免受网络安全风险而制定的控制措施，包括使用加密、防病毒软件、复杂的密码要求、虚拟专用网络或零信任网络进行身份验证、定期更新固件，以及资产管理流程，以确保公司的硬件在发放时具有适当的安全配置，并在资产报废时进行妥善处置。

H. 组织为确保生产支持免受网络安全风险而部署的控制措施，其中应包括及时为服务器打安全补丁，以应对新兴风险。检查现有的监控控制措施，以确定可用性和资源利用是否充分，从而对威胁性能的潜在网络安全问题进行检查和分析。检查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、备份和测试数据库，以及已部署有效的网络安全控制措施。

I. 与网络相关的控制措施，通过网络分段以限制未经授权访问造成的网络安全风险。检查组织如何使用防火墙，包括防火墙的位置以及用于检查、分析和限制网络访问、以防止未经授权访问的流程，。检查企业如何利用入侵检测/防御系统来预防、检测和处置网络安全攻击。

J. 组织针对常用桌面通信服务实施的控制措施，如使用电子邮件加密、确保及时应用互联网浏览器安全更新、配置视频会议/信息（如 MS Teams、Zoom 等）安全设置以限制使用某些文件扩展名（如 .exe 文件），以及在文件共享中使用多因素身份验证。

K. 组织为降低与提供服务有关的网络安全风险而部署的控制措施，包括：
1. 确保变更管理流程在评估和批准变更时考虑到网络安全风险，并及时应对网络安全事件。
2. 用户服务台记录组织通报的所有网络安全事件，确保及时解决，并上报给适当的管理层成员。
3. 移动设备（如电子邮件、应用程序等）的管理为降低网络安全风险进行了专门配置，并可在用户设备受到威胁时进行远程管理。

L. 保护高风险信息（包括为免受网络安全风险提供保护）的实体安全控制。例如，确保第三方/供应商的访问权限是适当的，并将物理用户访问数据中心、网络运行中心和安全运行中心的权限限制在授权人员范围内等。

M. 组织在事件响应和恢复方面实施的控制措施，其中应包括：
1. 相关书面计划，并随着组织业务的不断变化而进行审查和更新。
2. 定期测试并向管理层报告结果。
3. 确定是否及时纠正了测试中发现的任何问题。

附录 B.记录专项要求遵循情况的工具

网络安全 - 治理

要求	是否遵循 (是/否/部分)	获得的证据或排除的理由
A. 制定并定期更新与网络安全风险管理流程相关的政策和程序，包括推动基于广泛采用的框架（NIST、COBIT 等）加强控制环境的实践。		
B. 明确规定支持组织网络安全目标的角色和职责，且有关职责得到妥善履行。		
C.定期向董事会通报网络安全目标、战略、风险和用于降低风险的控制措施的更新情况。		
D. 有关利益相关方（如领导层、运营部门、战略供应商等）参与讨论如何以最佳方式建立和改进网络安全风险管理流程。		
E. 向董事会通报有效执行网络安全风险管理流程所需的资源（如领导力、资金、人才、硬件、软件和培训等）。		

网络安全 - 风险管理

要求	是否遵循 (是/否/部分)	获得的证据或排除的理由
A.建立全组织范围的风险管理流程，包括识别、分析和管理与信息技术和安全有关的风险，特别关注网络安全风险以及这些风险可能如何影响组织实现其目标的能力。		
B.由一个跨职能团队负责执行网络安全风险管理流程，该团队包括信息技术领导层、整个组织的风险管理、法律、合规、其他管理层（运营、会计、财务等），并酌情吸收外部各方（供应商、外包服务提供商、供应商、客户等）参与。		
C.制定并定期更新与网络安全风险管理有关的政策和程序，包括推广基于广泛采用的风险管理框架、权威指南或最佳做法的加强网络安全风险管理流程的做法。		
D.建立了网络安全风险管理的问责制和责任制，并确定了个人或团队定期监测和通报网络安全风险的管理情况，包括降低风险所需的资源和发现新兴网络安全风险。		
E.根据组织既定的风险管理指引，或为遵守适用的法律和/或监管要求，建立对应的流程，以便在网络安全风险（新出现的或以前		

要求	是否遵循 (是/否/部分)	获得的证据或排除的理由
发现的）上升到不可接受水平时，快速上报风险。		
F.在网络安全风险管理过程中包括了信息安全、法律、合规和其他管理部门之间的协作，以**确定并遵守所有法律和合同**义务，如法律和法规等。遵循和不遵循适用要求的情况会定期在组织内部通报。		
G. 制定了识别和管理与第三方有关的网络安全风险的流程。根据合同规定，销售商、供应商和其他外包流程和/或服务的提供商必须实施有效的网络安全控制措施，以充分保护他们所访问的组织系统和数据的保密性、完整性和可用性。		
H.**适当**设计和有效部署了与数据分类、保留、销毁和加密有关的政策和流程，以提供系统的方法，确保完整和准确地记录数据，并保护敏感信息的机密性和隐私。		
I.建立了网络安全操作风险沟通流程，确保管理层和员工有适当的认识。向董事会和管理层通报问题、差距、缺陷和控制失误，并密切监控和报告补救状况。及时发现、调查、报告和纠正不遵守网络安全政策的情况。		

网络安全--控制流程

要求	是否遵循 (是/否/部分)	获得的证据或排除的理由
A.**确定了网**络安全控制的优先顺序，确保分配相**关**预算和资源（如人员、软件、工具），以实现预期效益最大化。		
B.**确保网**络安全控制以促进实现组织网络安全目标和及时解决问题的方式运行。		
C.为负责网络安全操作的人员提供足够的培训。		
D.制定了充分的政策和程序，以管理网络安全操作和相**关控制的各个方面。**		
E.**确保管理**层拥有必要的资源，能够随时了解新技术带来的新兴网络安全问题，确定改进业务的机会，并了解如何以最佳方式部署网络安全工作，以影响更广泛的组织目标和目的。		

要求	是否遵循 (是/否/部分)	获得的证据或排除的理由
F.将网络安全充分纳入业务应用程序（包括软件和购置或定制开发的应用程序）的系统**开**发生命周期。		
G. 已将网络安全纳入硬件（笔记本电脑、台式电脑、移动设备等）管理。		
H.已对生产硬件支持实施有效控制，如配置、打补丁、支持用户访问管理以及监控可用性和性能。组织已对这些控制措施设计的**适当性和运行的有效性**进行了评估。		
I.优化与网络有关的控制措施，包括网络分段、使用和部署防火墙、限制与外部网络和/或系统的连接，以及使用入侵检测/预防系统等预防和检测技术。		
J. 对电子邮件、互联网浏览器、视频会议、信息传递和文件共享协议等常用桌面通信服务实施有效控制。		
K.已实施适当的服务交付控制，确保网络安全监控已被整合进入以下领域：变更管理、服务/求助台和终端用户设备管理。		
L.已实施适当的实体安全控制，以保护高风险信息中心（如数据中心、网络运营中心和安全**运**营中心）免受攻击。		
M.已实施事件响应和恢复控制。		

关于国际内部审计师协会

国际内部审计师协会（IIA）是一个专业协会，为全球 245,000 多名会员提供服务，并在全球范围内颁发了 195,000 多张国际注册内部审计师 (CIA) 证书。IIA 成立于 1941 年，是内部审计职业在标准、认证、教育、研究和技术指导方面全球公认的领导者。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教育。本资料无意为具体的个人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

2024 年 4 月

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