第三方专项要求

征求意见草案

《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有关的问题。
C. 其覆盖领域中包含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。《专项要求》是强制性的，质量评估中将对其遵循情况进行评估。

第三方

第三方是指与组织有业务关系的外部个人、团体或实体。第三方关系可以通过合同、协议或其他方式正式确立，为组织提供产品或服务。“第三方”一词的使用可能因行业或其他背景而异。本指南使用“第三方”一词来指卖方或供应商、承包商或分包商、外包服务提供商、其他机构和顾问，并包括第三方与其分包商（通常称为“下游”分包商）之间的协议。

虽然一级组织可以聘请第三方协助实现其一个或多个业务目标，但一级组织仍要对与实现这些目标相关的风险负责。

本专项要求不用于处理与主要组织的间接关系、利益或参与，如员工、财务合作伙伴、监管机构、代理或受托人等。如果第三方与组织签订的合同或协议允许其将工作分包给第四方或更多的“下游”方，则本专项要求也适用于为这些分包关系的治理和监督提供确认。在这种情况下，内部审计人员必须按照风险评估的结果执行所有要求。不适用情况必须记录在案。

如本专项要求所述，与第三方合作会带来风险，必须通过适当的治理、风险管理和控制流程来识别、评估和管理这些风险。如果第三方未能按合同履约、参与不道德的行为或出现业务中断，主要组织可能会受到影响。与第三方有关的风险类别和示例包括：

- 业务方面，如服务中断或无法实现业务目标。
- 网络安全，如敏感数据泄露。
- 财务方面，如供应商破产。
- 遵守适用的地方、国家和国际监管要求。
- 法律，如利益冲突、纠纷和违约诉讼。
- 声誉，如对环境或主要组织的客户、顾客或利益相关者造成的损害。

第三方的生命周期包括遴选、签约、引入、监控和退出。内部审计人员在评估治理、风险管理和控制过程的要求时，应考虑这些阶段。

评价和评估第三方理、风险管理和控制过程

本专项要求为评估第三方治理、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。这些要求代表了组织内该评估的最低要求。

治理：评价和评估第三方治理

要求：

内部审计人员必须评估组织对第三方治理的以下方面，包括董事会的监督：

A. 制定、实施并定期审查正式的方法，以确定是否与第三方为通过提供产品或服务协助实现业务目标签订了合同。该方法包括确定和评估实现目标的可用资源的适当标准。

B. 制定政策、程序和流程，以便在整个第三方生命周期内界定、评估和管理与第三方的关系和风险。这些政策、程序和流程与适用的监管要求保持一致，并定期接受审查和更新，以加强控制环境。

C. 界定组织内第三方管理的角色和责任，详细说明由谁选择、指导、管理、联系和监督第三方，以及必须向谁通报第三方的活动。建立了一套程序，用以确保被指派承担第三方角色和责任的个人具备适当的知识、技能和能力。

D. 确定与相关利益相关方的沟通要求，包括报告经过优先级排序的第三方的绩效、风险和合规状况。有关利益相关方可能包括董事会、高级管理层、运营、风险管理、人力资源、信息安全、法务、合规、采购及其他部门。

风险管理：评价和评估第三方风险管理

要求：

内部审计人员必须对组织的第三方风险管理的以下方面进行评估：

A. 针对第三方的风险管理流程是标准化的、全面的，包括明确的角色和责任，并能充分应对关键风险（如财务、运营、战略、网络安全、合规、声誉、道德、可持续性、地缘政治和法律）。对流程的遵守情况进行监测，并对任何偏差采取纠正措施。

B. 对整个生命周期中与第三方有关的风险进行识别和评估。风险评估用于对第三方进行分类和排序，并确定风险应对措施的优先次序。对该评估定期进行审查和更新。

C. 风险应对措施充分、准确，与排名相称。实施、审查、批准、监控、评估风险应对措施，并根据需要进行调整。

D. 制定了管理第三方问题的程序，并在必要时将其升级，以确保对结果负责，并提高实现合同或其他协议条款的可能性。如果第三方未能对上报的问题做出回应，则会制定补救程序，直至终止合同。

控制：评价和评估第三方控制过程

要求：

内部审计人员必须对以下针对经过优先级排序的第三方的控制措施进行评估，包括管理层对组织的第三方进行持续评估和监督的流程：

A. 记录在案并经批准的业务案例或其他相关文件，说明与第三方建立关系的必要性和性质。

B. 为遴选和选择第三方建立的一套健全的尽职调查程序。包含有关重要方面标准的程序，如审查网络安全协议、进行财务背景调查和核实银行详细信息等。

C. 合同签订和审批按照组织的第三方风险管理政策、程序和流程进行，并包括与组织适当部门的合作。

D. 最终合同或协议由所有利益相关方审查和批准，包括法务和合规部门（如适用）；由双方授权人员签署；并安全存储。所有合同都由一名合同经理或管理员负责。

E. 记录所有第三方关系的清单保持准确、完整，并且得到及时更新和妥善保存，例如储存在集中的合同管理系统中。

F. 建立第三方引入流程，形成正式文件，并予以遵循，使第三方能够满足合同或协议的条款要求。

G. 建立持续的监控程序，以评估经过优先级排序的第三方是否在整个生命周期内按照合同或协议条款履约，并履行合同义务。这些程序包括核实所提供信息的可靠性，定期以及在协议发生变化时重新评估绩效。

H. 制定相关规程，在第三方未能达到预期目标，或带来了更大或意料之外的风险的情况下，启动纠正措施。这些规程包括根据严重程度上报事件、执行事件后审查以及分析事件的根本原因。

I. 对合同续签日期进行监控，并在必要时进行续签。

J. 对于经过优先级排序的第三方，实施并遵循正式的退出计划。过程包括如何完成以下步骤：
   - 终止第三方。

- 必要时更换第三方。
- 重新分配保管权，归还或销毁第三方存储的组织的敏感数据。
- 禁止第三方访问系统、工具和设施。

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 260,000 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.

免责声明

国际内部审计师协会出版本文件的目的是提供信息和开展教育。本资料无意为个人的具体情况提供明确的答案，因此仅供参考。国际内部审计师协会建议就任何具体情况直接寻求独立的专家建议。对于完全依赖本资料的任何人，国际内部审计师协会不承担任何责任。

版权

2025 年 2 月

