第三方

专项要求

Topical Requirement

The Institute of Internal Auditors

翻译

中国内部审计协会 IIA China CHINA INSTITUTE OF INTERNAL AUDIT

第三方专项要求

《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》通过为特定风险领域的审计设定最低要求，明确了对内部审计人员的期望。组织的风险状况可能需要内部审计人员考虑该主题的其他方面。

遵循《专项要求》将提高内部审计服务的一致性，并提升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整体水平。

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：

1. 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。
2. 在开展审计项目时发现与其覆盖领域有关的问题。
3. 其覆盖领域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。

第三方

第三方是指与组织（以下一般称为主要组织）存在业务关系的外部个人、团体或实体，负责为组织提供产品或服务。第三方关系可以通过合同、协议或其他方式正式确立。本指南使用“第三方”一词来指代卖方或供应商、承包商或分包商、外包服务提供商、其他机构和顾问。此外，这一术语还涵盖了第三方与其分包商（通常称为“下游”分包商）之间的协议。

本《专项要求》适用于内部审计职能对第三方和/或任何分包关系开展确认服务的情况，其中包括了经主要组织与第三方之间的合同或协议所允许的第四方或更“下游”的分包商提供服务的情况。内部审计人员应当依据风险对第三方和“下游”分包商进行优先级排序（详见下文有关风险评估的内容），并对不适用的例外情况进行记录。

本《专项要求》不适用于处理与主要组织的间接外部关系、利益或联系，如监管机构、代理机构、受托人/董事会成员等；以及内部关系，如员工等。

根据所属行业或其他背景情况的差异，对“第三方”的定义和使用可能会存在差异。内部审计人员在使用《专项要求》对主要组织的第三方进行定义时可以保留一定的灵活性，并应当依赖其职业判断作出定义。

虽然主要组织（即与第三方签订协议的组织）聘请第三方来帮助其实现一个或多个目标，但主要组织对于实现目标相关的风险仍然负有责任。与第三方协作会带来新风险，必须使用本《专项要求》中列出的适当的治理、风险管理和控制过程，对这些风险进行识别、评估和管理。如果某个第三方未能履行合同义务，参与了不符合职业道德的行为，或者发生了业务中断，主要组织可能会遭受不利影响。与第三方相关的风险类别和示例包括：

- 战略风险，如完成主要组织使命和/或高层次目标或管理并购和收购的能力。
- 声誉风险，如对环境造成的损害，或者对主要组织与客户、顾客和利益相关方之间的关系和信任造成的损害。
- 道德风险，如诚信缺失、利益冲突、回扣和腐败。
- 运营风险，如实体安全和信息安全、内部人员风险、服务中断或未能实现目标。
- 财务风险，如第三方无力偿还债务和舞弊。
- 对适用的地方、国家和国际监管要求的合规风险。
- 网络安全及其他数据保护风险，如敏感数据泄露。
- 信息技术风险，如缺乏支持关键业务的服务。
- 法律风险，如利益冲突、纠纷以及因合同违约而引发的诉讼。
- 可持续发展风险，如环境、社会和治理。示例包括组织对自然环境的影响所带来的风险以及组织与社区进行互动相关的风险。
- 地缘政治风险，如贸易争端/制裁和政治动荡等。

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。

评估第三方治理、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。这些要求反映了评估的最低标准。

治理

要求：

内部审计人员必须评估主要组织对第三方进行治理的以下方面， 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和必要资源的适当标准。

B. 制定政策、程序和流程，以便在整个第三方生命周期内定义、评估和管理与第三方的关系和风险。这些政策、程序和流程遵循适用的监管要求，并定期审查和更新，以强化控制环境。

C. 明确组织内第三方管理的角色和责任，详细规定由谁遴选、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。建立了相应的程序，用以确保被指派承担第三方角色和责任的人员具备适当的知识、技能和能力。

D. 确定与相关利益相关方的沟通程序，包括及时报告优先级较高的第三方的绩效、风险和合规状况（特别是违反法律和监管要求的情况）。对第三方的优先级排序应当基于风险。有关利益相关方可能包括董事会、高级管理层、采购、运营、风险管理、合规、法务、信息技术、信息安全、人力资源及其他部门。

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，包括明确定义了角色和责任，并能充分应对与组织相关的关键风险（如战略、声誉、道德、运营、财务、合规、网络安全、信息技术、法律、可持续发展和地缘政治风险）。对流程的遵循情况进行监测，并对任何偏差采取纠正措施。

B. 在第三方整个生命周期中，相关风险得到识别和定期评估。利用风险评估结果对第三方（包括“下游”分包方）进行优先级排序，对风险应对措施也应进行优先级排序。对该评估定期进行审查和更新。

C. 风险应对措施充分、准确，与风险排序相匹配。风险应对措施得到实施、审查、批准、监控、评估，并根据需要进行调整。

D. 制定了管理第三方问题的程序，并在必要时上报有关问题，以确保对管理成效的问责，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，管理层将依据既定流程，评估与该第三方维持业务关系的风险，并视情况采取进一步行动、补救措施或终止合作。

控制

要求：

内部审计人员必须评估风险优先级较高的第三方的以下控制措施。评估必须包括管理层对组织第三方持续评估和监督的流程：

A. 为寻找和选择第三方建立了一套健全的尽职调查程序，商业论证和其他相关文件以书面形式进行记录，并获得了批准，描述并证明与第三方建立关系的必要性和性质。

B. 合同签订和审批依据组织的第三方风险管理政策和程序进行，并包括了组织适当部门之间的协作。

C. 最终合同或协议经过了所有利益相关方（包括法务和合规部门）的审查和批准，由双方授权人员签署，并得到了安全存储。每份合同都指派了一名合同经理或管理员负责。

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

E. 建立第三方引入流程，形成正式文件，并予以遵循，为第三方履行合同或协议条款奠定基础。

F. 建立持续的监控程序，以评估优先级较高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，是否履行合同义务。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。

G. 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、实施事后审查以及分析事件的根本原因。

H. 对合同终止和续签日期进行监控，并在必要时进行续签。

I. 对于优先级较高的第三方，实施并遵循正式的退出计划，以确保涉及时间安排和预期成果的合同要求得到妥善处理。具体包括如何完成以下步骤：

- 终止与第三方的合作。
- 在必要的情况下，更换第三方。
- 重新分配保管权，归还或销毁存储在第三方处的组织敏感数据。
- 撤销第三方对系统、工具和设施的访问权限。