第三方

专项要求

Topical Requirement

用户指南

The Institute of Internal Auditors

翻译

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

Contents

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®》(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《第三方专项要求》提供了需要考虑的控制过程的最低要求，但将第三方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，首席审计执行官必须确定如何获得资源，并及时向董事会和高级管理层报告存在的限制以及如何解决资源短缺。不论最终如何获得资源，首席审计执行官对确保内部审计职能遵循《专项要求》负有最终责任（标准 3.1 胜任能力、7.2 首席审计执行官的资格、8.2 资源、10.2 人力资源管理）。

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循《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）。

《专项要求》的设计目的在于支持一致、高质量的内部审计实务。当地法律、监管要求、监督期望和其他得到专业认可的框架可能会提出额外或更加具体的要求。根据标准 1.3 合法和职业道德行为，内部审计人员必须了解和遵守组织所属行业或所在地的法律和/或监管要求，包括进行必要的信息披露。内部审计人员可能已经将这些额外的要求整合到审计项目方案和测试程序中，应当将其与《专项要求》进行对照，确保适当的覆盖范围。

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。可以通过一个项目覆盖《专项要求》的所有内容，也可以通过多个项目达成这一目的。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。

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。

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、协议或其他为组织提供产品、服务、劳动力、制造能力或信息技术解决方案（如数据储存、处理和维护）的方式正式确立。

注

《专项要求》使用《全球内部审计准则》中定义的一般内部审计术语。读者应当通过《准则》的词汇表部分了解专业术语及其定义。

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（签订第三方服务协议的组织）的第三方进行定义时可以保留运用其职业判断的灵活性。在《第三方专项要求》及其用户指南中，“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。“第三方”还涵盖了所有此类安排和关系，包括第三方与其分包商（通常称为“下游”分包商）或“第四方”“第五方”乃至“第 N 方”之间的协议。

《第三方专项要求》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、投资人、受托人/董事会成员、公共服务机构和一般社会公众等；以及内部关系，如员工或集团内部的服务提供方等。

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。

对组织管理第三方关系的程序有效性的评估，可以在整个组织范围内开展，也可以针对一项或多项合同、协议或关系。内部审计人员应当采取自上而下的方法，了解组织的第三方政策、流程、程序、框架和生命周期。内部审计人员应当运用其职业判断，根据行业、组织和业务领域的特点，理解第三方风险的具体特征。根据标准 5.1 信息的使用，内部审计人员应当了解并遵循所有与他们可能接触到的第三方信息有关的政策和程序。

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）。内部审计人员必须根据风险评估的结果应有所有要求，并对不适用的例外情况进行记录。

《第三方专项要求》及其用户指南提到了组织与第三方关系的各个阶段，也被称为生命周期的各个阶段：遴选、签约、引入、监控和退出。这些阶段将被用于实现《第三方专项要求》及其用户指南的目的，尽管部分行业对各阶段可能存在不同的划分方式。上述阶段的具体内涵如下：

- 遴选：包括确定第三方需求、为使用第三方制定计划、为遴选开展尽职调查的过程。此外，遴选阶段应当包含评估潜在或已接触的第三方存在的风险。
- 签约：包括起草、协商、批准和执行与第三方的法律协议的尽职调查过程。
- 引入：在合同被签订、合同关系启动时开始，为第三方达成合同或协议条款要求奠定了基础。
- 监控：包括建立和批准对在合同周期中的第三方的管理流程和合同已终止的第三方的持续监控流程。此类方法一般是系统化的、基于风险的，并应考虑持续改进。监控包括了在必要的情况下更新目前有效的合同或协议。
- 退出：包括结束合同或协议、维护风险优先级较高的第三方的退出机制、在必要时终止关系的程序。此类程序一般使用基于风险的方法，并可能会引入正式的退出计划。

虽然聘请了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。与第三方协作可能会降低组织运营的某些成本，但是也可能会带来新的运营风险，因为主要组

织对第三方控制过程的了解和掌控力相对较低。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。

主要组织必须通过适当的治理、风险管理和控制过程，对这些风险进行识别、评估和管理。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。

内部审计人员在评估治理、风险管理和控制过程的要求时，应考虑第三方生命周期的所有阶段。

根据标准 9.1 了解治理、风险管理和控制过程，《第三方专项要求》中的要求被分为了三个部分：

- 治理 – 明确定义了使用第三方来支持组织目标、政策和流程的最低目标与战略。
- 风险管理 – 用于识别、分析、管理和监控使用第三方的风险的流程，包括及时上报事件的流程。
- 控制 – 由管理层建立的、接受定期评价的控制过程，用于降低使用第三方带来的风险。

除了本《专项要求》及其用户指南外，内部审计人员还可以参考其他有关第三方的职业指引，包括 IPPF 的《全球指南》和其他行业专属的资源等。

考虑因素

内部审计人员可使用以下考虑因素来帮助评估第三方专项要求。每个部分中字母标号的内容是对《专项要求》原文的重申或者重新组织。其下的非强制性考虑因素则进一步作了展开，提供了评估这些要求方法的示例。内部审计人员在确定将哪些内容纳入评估范围时应依据其职业判断。

治理方面的考虑因素

为评估如何将治理程序（包括董事会的监督）应用于第三方目标，内部审计人员可检查以下证据：

A. 为确定是否使用第三方制定的、基于风险的书面正式方法或战略。上述方法定期接受审查，并包含以下内容：
   - 为实施方法制定了明确和标准化的程序，且程序的使用得到了组织的批准。
   - 依据成本效益分析结果证明引入第三方的必要性，并基于此为确保战略上的一致性和资源的有效性，确定所需资源。
   - 管理层对风险和控制（包括有关第三方问题的风险和控制）的评价。
   - 用于获取、管理和监督第三方绩效的适当资源。
   - 将利益相关方的反馈意见整合到方法或战略中。

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、程序可能包括：
   - 促进关键治理、风险管理和控制过程的标准化工具和模板。
   - 定期评价政策和程序、确定其适当性、并在必要时进行更新的流程。
   - 第三方遴选、签约、引入、监控和退出的既定原则。
   - 为遵循政策和程序，识别和定期检查适用的监管要求。
   - 为识别和比较第三方管理先进实务的对标举措。

C. 明确了支持第三方管理目标的角色和责任。进一步的证据可能包括：
   - 评估第三方的价值观、职业道德和企业社会责任是否符合主要组织有关原则的流程。上述流程应包括如何及时解决潜在的利益冲突或不道德行为。
   - 对承担第三方管理职责的人员开展定期培训，并对他们的胜任能力进行定期评估。
   - 评价是否开展适当培训使整个组织对第三方有所了解的流程。
   - 角色和职责符合三线模型。

D. 在第三方的整个生命周期中，及时向有关利益相关方(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)报告有关情况并推动其介入，包括：

- 有关第三方的风险和已知潜在缺陷被记录在会议纪要、报告和电子邮件中。
- 交换第三方管理信息和促进协作（例如：通过定期召开跨部门会议等）。

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第三方目标，内部审计人员可检查以下证据：

A. 第三方服务的使用者建立了标准化的、全面的风险管理流程，包括明确定义角色和责任，充分应对与组织相关的关键风险：

- 评估和管理第三方风险的流程包括：
  - 如何首次识别和报告风险。
  - 如何分析风险，以评估它们对实现组织目标能力的影响。
  - 如何缓解风险，包括将风险降至可接受水平的行动计划。
  - 如何监控风险，包括发现和应对早期警示信号、持续报告直至威胁被完全解除等。
- 对遵循有关流程和对任何偏差实施纠正措施进行监督，以防止削弱组织的长期目标或战略。
- 建立了风险管理委员会或其他团队，对第三方进行直接监督，并为董事会提供意见。明确成立委员会的目的，且委员会定期召开会议。证据可以包括会议纪要等。

B. 在第三方整个生命周期中，与第三方相关的风险得到识别和定期评估。利用风险评估结果对第三方进行优先级排序，同时对风险应对措施也进行优先级排序。

- 主要组织在开展对第三方的评估时，考虑了自身规模、成熟度、合作的第三方数量等因素。
- 对风险评估进行了书面记录，识别了固有和剩余风险。
- 组织依据尽职调查程序对风险评估进行审查和更新。
- 建立了根据风险对第三方进行优先级排序的标准。此类标准的示例包括：
  - 第三方提供的服务对组织的运营是否重要。
  - 与第三方合作带来的财务价值是否显著。
  - 合作关系是新建立的，在短时间内达成的，还是长期的。
  - 涉及到多个外部组织。
  - 第三方计划进一步分包部分或所有工作。
- 组织遵循得到广泛接受的风险评估实务，包括尽早开展风险评估（开展时间一般在遴选阶段对建议进行分析时、引入第三方之前）。

- 供应商完成一份问卷，以确定其基于固有风险的风险优先级排序。组织确保问卷由相关的人员填写，并得到检查以确保准确性。
- 组织定期获取职能部门（包括信息技术、采购、企业风险管理、人力资源、法务、合规、运营、会计和财务等）对于第三方风险管理的意见。

C. 风险应对措施（包括降低、接受、消除和分担等）得到确认，且与风险排序相匹配。

- 风险应对措施以书面方式得到记录，包括了对第三方控制环境的考虑。
- 对超出主要组织风险容忍度的风险应对措施进行合理性审核的书面记录，特别是在风险被接受的情况下。风险应对措施包括了处置与第三方潜在的利益冲突。

D. 管理和上报第三方风险的流程，包括如何对威胁或风险水平进行评价，如何分派任务和如何对风险进行优先级排序等。检查内容包括了确定以下方面：

- 对组织风险水平的定义和解释——例如高、中、低——以及上报每个风险类别的程序。
- 根据已识别风险进行排序的第三方清单和记录所有风险事件缓解状态的清单。
- 适用的法律、监管和合规要求。
- 风险的影响，包括财务影响和非财务影响（例如声誉）。
- 与管理层和员工沟通第三方风险的流程，包括定期向董事会（或其他适当的机构）报告整体风险态势。沟通内容应当包括与优先级较高的第三方有关的所有补救措施的进展情况。
- 当主要组织的风险偏好和风险容忍度发生变化时，对优先级排序进行重新评估的流程。

控制方面的考虑因素

为评估如何将控制过程应用于第三方关系，内部审计人员可检查以下内容：

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。

- 商业论证还可以包含：
  - 如何处置与第三方满足期待能力的风险以及可能对组织造成的影响。
  - 具体的成本效益分析。
- 遵循了既定的遴选程序——如竞标、邀标、定向采购等。具体程序包括：
  - 重要方面的标准，如检查网络安全协议，核实银行信息，开展财务背景检查，研究第三方的组织架构、犯罪记录、驾驶记录、政治活动、与犯罪活动的联系等。
  - 明确的遴选标准，包括评估过往绩效、参考信息、声誉和合同成本等。

- 为确保妥善选择供应商的尽职调查，例如组建跨职能团队审核提案。为降低偏见的风险，对于审核团队的控制措施包括组建团队的程序和对披露潜在利益冲突的要求。
- 评估第三方控制环境的尽职调查。如，进行实地考察或检查第三方的以下情况：
  - 系统和组织控制（SOC）报告。
  - 财务稳定性。
  - 公司章程或良好信誉证明。
  - 关键管理层和利益相关方决策的透明度。
  - 组织架构。
  - 运营稳定性。
  - 网络安全协议。
  - 对相关法律、监管要求和准则的遵循情况。
  - 道德状况。
  - 与主要组织的合作历史。
  - 声誉。
- 证明潜在供应商或承包商只有在相关尽职调查程序完成且结果得到分析之后，才会开始生命周期的证据。

B. 组织制定并遵循了合同签订的政策和程序。

- 合同中不存在模糊不清的条款。
- 在合同起草阶段考虑了关键风险，并加入了相关条款。在这个阶段与第三方就需要解决的问题进行了沟通。
- 根据组织签订合同的政策和程序以及第三方的优先级确定了合同的关键要素，具体要素可能包括：
  - 不得披露信息的（保密）条款。
  - 终止协议的条款和数据获取的范围。
  - 网络安全要求，包括在特定时间段内评估和分享所有信息的要求，以及报告发生事件和信息泄露的要求。
  - 对于发生影响主要组织数据的信息泄露进行告知的要求。
  - 用于核实第三方身份的标准程序，包括完整的法定名称、地址、实体所在地和网址。标准的实务是在身份核实的过程中使用清单检查信息的准确性。
  - 明确对服务水平的要求，指出期望获得的成果以及各方的权利、义务、惩罚、奖励和职责，包括支付人力成本（包括“下游”分包商）的责任。

- 有关审计权利的条款（包含对“下游”分包商），或者对由声誉良好的独立确认机构对签约方进行审计的证据要求。如果没有在合同中写明审计权利，内部审计职能获得或提供确认的能力可能会受到限制。

- 主要组织能够获取独立审计人员出具的控制评估报告；例如，有关财务、合规或数据安全的报告，包括依据《国际鉴证业务准则》出具的报告或 SOC 报告等。
  - 如果依赖第三方聘用的外部确认提供方的工作成果，需对相关文档进行审核，以确保其可靠性。
  - 报告被用于识别未得到妥善管理的风险和改善管理流程。

- 被用于处置对特定组织或合同类型具有重要意义的组成要素的政策和程序：
  - 环境和可持续发展条款。
  - 举报机制。
  - 对绩效进行评价的要求。
  - 第三方经过测试的业务连续性方案。
  - 在提供服务的过程中对人工智能的使用。
  - 所有“下游”分包商工作得到识别和披露，其条款和范围得以明确。
  - 变更管理流程，列出如何在合同期限内处理范围、条款或运营要求的变化（例如技术的变化或监管要求的更新）。
  - 变更要求次数或计费次数的限制。

- 要求在付款或支付尾款前对最终产品进行正式验收的政策或程序。
- 第三方被要求分享其道德政策或行为守则，和/或遵循主要组织的相关要求。
- 在第三方起草合同的情况下，主要组织应组织法律团队进行审核，理解关键风险并制定适当的风险缓解策略作为支持。

C. 最终合同或协议经过了适当的利益相关方（包括法律和合规部门）的审查和批准，得到了安全存储，并指派了合同经理或管理员负责。

- 表明外包关系和第三方义务的合同或其他法律文件，和证明进行了必要的法律和合规检查的证据。

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。

- 将新的第三方合同或协议增加到清单或系统中的流程。
- 将潜在的第三方加入供应商系统和在合同未获批准的情况下从系统中将其删除的流程。
- 从第三方合同和协议从清单或系统中删除的流程。
- 记录特定承包商或供应商存在问题、以便未来参考的跟踪系统。

- 检查第三方情况是否准确和完整的流程。

E. 建立第三方引入流程，形成正式文件，并予以遵循，帮助第三方履行合同或协议条款。检查的内容可以包括核实以下情况：

- 标准化的引入程序，可确保所有必要的文件、培训和合规检查都得到完成。
- 第三方的系统和流程能够与主要组织的技术无缝整合。
- 共同使用的系统是兼容且安全的。证据可以包括在 SOC 报告中包含互补用户实体控制（CUeC）。
- 主要组织对第三方的业务连续性方案进行评估，以确保在紧急情况下能够持续提供服务。其中应包含为应对潜在业务中断制定的应急预案。

F. 持续监控供应商完成合同或协议目标绩效情况的程序，包括对关键绩效指标的评价。

- 监控程序可以为第三方风险评估提供信息，并可根据需要，对已发现的控制缺陷进行检查、上报和处置。
- 有关为管理实时监控建立的流程、使用的技术和工具的报告或信息。
- 确保依据合同或协议条款（例如遵循项目时间表、进度节点或沟通要求等）完成支付的流程。只有经过批准并完成引入阶段工作、且被纳入供应商支付系统的承包商才能接受支付。如果合同中对交付产品有明确约定，只有在对交付产品进行验收后，才能进行支付。
- 对与第三方协议有关的控制成本的监控，以确保通过投入获得的价值和产出。投入效益分析的结果可以用于重新协商合同条款。
- 用于评估对未能遵守合同或协议约定的情况进行处罚的流程。在进行处罚时，计算了罚款金额并要求第三方支付。
- 根据风险对第三方的优先级排序会定期接受重新评估，或是在协议变更和合同即将到期或自动续期时进行重新评估。
- 对经优先级排序的检查，如实地走访或季度业务回顾等，以核实控制措施和运营完整性。
- 其他持续监控的证据可能包括：
  - 对第三方财务稳定性的分析。
  - 对针对第三方投诉的评估。
  - 管理层对独立审计人员出具的报告（如第三方依据《国际鉴证业务准则》《鉴证业务准则公告》出具的报告，第三方提供的财务报告、审计报告、合规报告和数据安全报告，ISO 认证等）的意见。
  - 管理层对第三方开展的业务复原力测试结果（包括发现的重大问题）的意见。
  - 使用“下游”分包商的条件和限制。
  - 对第三方道德价值观、组织文化和行为守则的评价。

- 对媒体质询的回复。
- 对用于保护主要组织数据和信息存储和传输的隐私和网络安全协议（包括对人工智能等先进技术的使用）的评价。
- 组织对有利于持续改善绩效和实现合同或协议目标的机会的发现。
- 对职责分离情况的检查。

G. 制定相关规程，在发现第三方未能满足合同或协议的要求，或第三方的行为提高了主要组织的风险时，启动纠正措施。

- 根据事件的严重性和第三方的优先级排序上报事件的程序。
- 实施事后审查，包括开展根本原因分析。

H. 提示合同和协议即将到期或自动续签的程序。对于自动续签程序，需要检查以下情况：

- 第三方的绩效。
- 合同或协议条款和附录。
- 风险因素。

I. 对于优先级较高的第三方（包括所有“下游”分包商），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。

- 通过清单或者与关键利益相关方的访谈，确保安全措施的有效性。
- 第三方持有的组织信息或数据得到归还或销毁。
- 第三方对组织数据、系统或设施的访问权限被撤销。
- 主要组织的资产（如设备、软件授权、知识产权和文件）被归还。
- 如果与第三方的关系出于特定原因被终止，应了解具体情况，并上报高级管理层和/或董事会。
- 当与优先级较高的第三方关系被终止时，应当依据相同的风险评估确定后继者，除非合同目的已经达成或者不再被需要。

附录 A. 实际应用示例

以下示例描述了适用《第三方专项要求》的情况：

示例 1：内部审计计划内的审计项目工作范围包含了目前由第三方提供的服务或成果。

当内部审计职能部门完成其基于风险的计划流程，且在内部审计计划中包含一个或多个审计项目，覆盖了目前由签订合同或协议的第三方提供的服务或成果时，开展此类项目必须遵循《专项要求》。

《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《第三方安全专项要求》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确认组织在关键服务方面对第三方的依赖程度较低，或者与第三方的长期合作关系带来的财务影响较低。

示例 2：在某个不以第三方或合同管理为重点的审计项目中发现了第三方风险。

内部审计人员在评估与第三方或合同管理没有直接关系的流程时，也有可能会发现重大的第三方风险。例如，在为评估数据储存的审计项目制定计划时，内部审计人员发现云服务由第三方提供。在与第三方提供服务的管理人员进行访谈后，内部审计人员发现了与第三方相关的网络安全风险。

一旦确定存在这样的风险，内部审计人员必须查阅《第三方专项要求》和《网络安全专项要求》，并确定哪些要求适用。有时审计人员可能不会在项目中包括第三方治理程序或第三方风险管理程序，而是专注于第三方提供服务的控制。审计人员在应用《网络安全专项要求》时也需要运用这样的职业判断。审计人员必须在项目工作底稿中记录排除《第三方专项要求》和《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第三方审计项目。

组织内部出现了有关重要第三方的问题，需要内部审计职能立即关注。出现的问题包括控制失败。首席审计执行官应当报告董事会，讨论重新确定内部审计职能审计计划的重点，并重新分配必要的资源。审计人员应当与受影响的管理层协作，确定审计项目的目标，评价当前情况，并未避免未来再次出现问题提出建议。首席审计执行官应当查阅《专项要求》，确定审计项目范围，决定哪些要求适用，并对任何认定有关要求不适用的情况进行记录。

附录 B. 可选文档工具

内部审计人员应当运用其职业判断，来根据风险评估的结果确定哪些要求适用，并妥善记录排除了哪些要求。根据审计人员的专业判断，有关《专项要求》的内容可以被记录在内部审计计划或项目工作底稿中。可以通过一个项目覆盖《专项要求》的所有内容，也可以通过多个项目达成这一目的。此外，并非所有要求都一定适用。下方的可打印表格展示了记录对《第三方专项要求》遵循情况的一种方式，但对该表格的使用并不具有强制性。

第三方治理

要求	已执行的覆盖范围 或排除理由	文件参考
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。		

要求	已执行的覆盖范围或排除理由	文件参考
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。		

第三方风险管理

要求	已执行的覆盖范围或排除理由	文件参考
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。		

要求	已执行的覆盖范围或排除理由	文件参考
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。		

第三方控制

要求	已执行的覆盖范围或排除理由	文件参考
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。		

要求	已执行的覆盖范围 或排除理由	文件参考
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. 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。		

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 9 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