Public Consultation Draft

Third-Party Topical Requirement

The International Professional Practices Framework® comprises Global Internal Audit Standards™, Topical Requirements, and Global Guidance. Topical Requirements are mandatory and must be used in conjunction with the Standards, which provide the authoritative basis for the required practices.

Topical Requirements provide clear expectations for internal auditors by setting a minimum baseline for auditing specified risk areas. The organization's risk profile may require internal auditors to consider additional aspects of the topic. Conformance with Topical Requirements will increase the consistency with which internal audit services are performed and improve the quality and reliability of internal audit services and results. Ultimately, Topical Requirements elevate the internal audit profession.

Internal auditors must apply Topical Requirements in conformance with the Global Internal Audit Standards. Conformance with Topical Requirements is mandatory for assurance services and recommended for advisory services. The Topical Requirement is applicable when the topic is one of the following:

A. The subject of an engagement in the internal audit plan.
B. Identified while performing an engagement.
C. The subject of a requested engagement that was not on the original internal audit plan.

Evidence that each requirement in the Topical Requirement was assessed for applicability must be documented and retained. Not all individual requirements may apply in every engagement; if requirements are excluded, a rationale must be documented and retained. Conformance with the Topical Requirement is mandatory and will be evaluated during quality assessments.

Third Parties

A third party is an external individual, group, or entity with whom an organization has a business relationship. A third-party relationship may be formalized through a contract, agreement, or other means to provide the organization with products or services. The use of the term “third party” may differ based on industry or other contexts. This guide uses the term “third party” to refer to vendors or suppliers, contractors or subcontractors, outsourced service providers, other agencies, and consultants and includes agreements between a third party and its subcontractors, often known as “downstream” subcontractors.

This Topical Requirement is not intended to address indirect relationships, interests, or involvements with the primary organization, such as employees, financial partners, regulators, agents, or trustees.

Although the primary organization can engage a third party to assist with achieving one or more of its business objectives, the primary organization retains accountability for the risks associated with achieving those objectives. If a third party's contract or agreement with the organization allows it to subcontract to a fourth or further "downstream" party, this Topical Requirement applies when providing assurance over the governance and oversight of those subcontracted relationships as well. In these cases, internal auditors must apply all requirements as indicated by the results of a risk assessment. Exclusions must be documented.

Working with third parties introduces risks that must be identified, assessed, and managed through appropriate governance, risk management, and control processes, as outlined in this Topical Requirement. If a third party fails to perform as contracted, participates in unethical practices, or experiences a business disruption, the primary organization may suffer repercussions. Categories and examples of risks related to third parties include:

- Operational, such as service disruptions or not achieving the business objectives.
- Cybersecurity, such as compromised sensitive data.
- Financial, such as vendor insolvency.
- Compliance with applicable local, national, and international regulatory requirements.
- Legal, such as conflicts of interest, disputes, and litigation for contract breaches.
- Reputational, such as damage caused to the environment or to the primary organization's clients, customers, or stakeholders.

The third-party lifecycle consists of selecting, contracting, onboarding, monitoring, and offboarding. Internal auditors should consider these phases when assessing the requirements for governance, risk management, and control processes.

Evaluating and Assessing Third-Party Governance, Risk Management, and Control Processes

This Topical Requirement provides a consistent, comprehensive approach to assessing the design and implementation of third-party governance, risk management, and control processes. The requirements represent a minimum baseline for this assessment in an organization.

Governance: Evaluating and Assessing Third-Party Governance

Requirements:

Internal auditors must assess the following aspects of the organization's governance of third parties, including board oversight:

A. A formal approach is established, implemented, and periodically reviewed to determine whether to contract with a third party to assist with meeting a business objective by providing a product or service. The approach includes appropriate criteria for defining and assessing available resources to meet objectives.

B. Policies, procedures, and processes are established to define, assess, and manage relationships and risks with third parties throughout the third-party lifecycle. The policies, procedures, and processes are aligned with applicable regulatory requirements and are periodically reviewed and updated to strengthen the control environment.

C. Third-party management roles and responsibilities within the organization are defined, detailing who selects, directs, manages, communicates with, and monitors third parties as well as who must be informed about third-party activities. A process exists to ensure individuals assigned third-party roles and responsibilities have the appropriate knowledge, skills, and abilities.
D. Communication protocols with relevant stakeholders are defined and include reporting the status of the performance, risks, and compliance of prioritized third parties. Relevant stakeholders may include the board, senior management, operations, risk management, human resources, information security, legal, compliance, procurement, and others.

RISK MANAGEMENT: Evaluating and Assessing Third-Party Risk Management

Requirements:

Internal auditors must assess the following aspects of the organization's third-party risk management:

A. Risk management processes for third parties are standardized and comprehensive, include defined roles and responsibilities, and sufficiently address key risks (such as financial, operational, strategic, cybersecurity, compliance, reputational, ethical, sustainability, geopolitical, and legal). Adherence to processes is monitored and corrective actions are implemented for any deviations.

B. Risks related to third parties throughout the lifecycle are identified and assessed. The risk assessment is used to classify and rank third parties and prioritize risk responses. The assessment is reviewed and updated periodically.

C. Risk responses are adequate and accurate, commensurate with ranking. Risk responses are implemented, reviewed, approved, monitored, evaluated, and adjusted as needed.

D. Processes are in place to manage and escalate, if necessary, issues that arise from third parties, ensuring accountability for outcomes and increasing the likelihood of achieving the terms of contracts or other agreements. If a third party fails to respond to escalated concerns, processes are in place for remediation up to and including termination.

CONTROLS: Evaluating and Assessing Third-Party Control Processes

Requirements:

Internal auditors must assess the following controls for prioritized third parties, including management's processes for ongoing assessment and monitoring of the organization's third parties:

A. A documented and approved business case or other relevant document describes and justifies the need for and nature of the relationship with a third party.

B. A robust due diligence process for sourcing and selecting third parties is in place. The process includes criteria for important aspects, such as reviewing cybersecurity protocols, conducting financial background checks, and verifying bank details.

C. Contracting and approval are performed according to the organization's third-party risk management policies, procedures, and processes and include collaboration with appropriate parts of the organization.

D. Final contracts or agreements are reviewed and approved by all relevant stakeholders, including legal and compliance when applicable; signed by authorized individuals from both parties; and stored securely. All contracts are assigned to a contract manager or administrator for responsibility.

E. An accurate, complete, and current listing of all third-party relationships is maintained, such as in a centralized contract management system.

F. Documented onboarding processes are established and followed to enable third parties to meet the terms of the contract or agreement.

G. Ongoing monitoring processes exist to assess whether prioritized third parties perform in accordance with contract or agreement terms throughout the lifecycle and fulfill contractual obligations. The processes include verifying the reliability of information provided and reevaluating the performance periodically and whenever the agreement changes.

H. Protocols are established to initiate corrective actions if a third party fails to meet expectations or poses increased or unexpected risk. The protocols include escalating incidents based on severity, performing post-incident reviews, and analyzing the root cause of incidents.

I. Contract renewal dates are monitored, and renewal actions are taken as necessary.

J. For prioritized third parties, a formalized offboarding plan is implemented and followed. Processes include how to:
   - Terminate the third party.
   - Replace the third party if necessary.
   - Reassign custody and return or destroy the organization's sensitive data stored with the third party.
   - Revoke the third party's access to systems, tools, and facilities.

About The Institute of Internal Auditors

The Institute of Internal Auditors (The IIA) is an international professional association that serves more than 260,000 global members and has awarded more than 200,000 Certified Internal Auditor (CIA)© certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information, visit www.theiia.org.

Disclaimer

The IIA publishes this document for informational and educational purposes. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The IIA recommends seeking independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this material.

Copyright

February 2025