Third-Party

Topical Requirement

The Institute of
Internal Auditors

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:

1. The subject of an engagement in the internal audit plan.
2. Identified while performing an engagement.
3. 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 ("the primary organization") establishes a business relationship to obtain products or services. The relationship may be formalized through a contract, agreement, or other means. This Topical Requirement uses the term "third party" to refer to vendors, suppliers, contractors, subcontractors, outsourced service providers, other agencies, and consultants. The term includes agreements between a third party and its subcontractors, often known as "downstream" subcontractors.

The Topical Requirement applies when the internal audit function performs assurance engagements on third parties and/or any subcontracted relationships, including those fourth or further downstream, allowed by the third party's contract or agreement with the primary organization. Internal auditors should prioritize third and further downstream parties based on risk, as described in the risk management section below. Internal auditors must apply all requirements as indicated by the results of the risk assessment, and exclusions must be documented.

This Topical Requirement is not intended to address indirect external relationships, interests, or involvements with the primary organization, such as regulators, agents, trustees/board members, or internal relationships, such as employees.

The term "third party" may be defined and used differently based on industry or other contexts. Internal auditors are granted flexibility and should rely on their professional judgment to adapt the Topical Requirement to the primary organization's definition of third party.

The primary organization (the organization entering into a third-party agreement) retains accountability for the risks associated with achieving its objectives, even when it engages a third party to help it achieve one or more objectives. 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:

- Strategic, such as the ability to accomplish the primary organization's mission and/or high-level objectives or to manage the impacts of mergers and acquisitions.
- Reputational, such as damage caused to the environment or to the primary organization's relationship and trust with clients, customers, and stakeholders.
- Ethical, such as failures of integrity, conflicts of interest, kickbacks, and corruption.
- Operational, such as physical and information security, insider risk, service disruptions, and not achieving the objectives.
- Financial, such as third-party insolvency and fraud.
- Compliance with applicable local, national, and international regulatory requirements.
- Cybersecurity and other data protection, such as the compromise and leakage of sensitive data.
- Information technology, such as the lack of services to support critical operations.
- Legal, such as conflicts of interest, disputes, and litigation for contract breaches.
- Sustainability, such as environmental, social, and governance. Examples include risks related to an organization's impact on the natural environment and risks concerning an organization's interactions with communities.
- Geopolitical, such as trade disputes/sanctions and political instability.

The third-party life cycle consists of selecting, contracting, onboarding, monitoring, and offboarding. Internal auditors should consider these stages 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 the assessment.

GOVERNANCE

Requirements:

Internal auditors must assess the following aspects of the primary 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. The approach includes appropriate criteria for defining and assessing the resources necessary and available to meet objectives by providing a product or service.

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

C. The organization's third-party management roles and responsibilities are defined, detailing who selects, directs, manages, communicates with, and monitors third parties and who must be informed about third-party activities. A process exists to ensure individuals assigned third-party roles and responsibilities have the appropriate competencies.

D. Protocols for communicating with relevant stakeholders are defined and include timely reporting on the status of the performance, risks, and compliance (specifically breaches of laws and regulations) of prioritized third parties. Third parties are prioritized based on risk. Relevant stakeholders may include the board, senior management, procurement, operations, risk management, compliance, legal, information technology, information security, human resources, and others.

RISK MANAGEMENT

Requirements:

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

A. Processes for risk management of third parties and their services are standardized and comprehensive, include defined roles and responsibilities, and sufficiently address key risks relevant to the organization (such as strategic, reputational, ethical, operational, financial, compliance, cybersecurity, information technology, legal, sustainability, and geopolitical). Adherence to processes is monitored, and corrective actions are implemented for any deviations.

B. Risks related to third parties throughout the life cycle are identified and assessed regularly. The risk assessment is used to rank and prioritize third parties, including those further downstream. Risk responses are also ranked and prioritized. The risk 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 management to evaluate the risks of its ongoing business relationship and pursue further action, remediation, or termination, as warranted.

CONTROLS

Requirements:

Internal auditors must assess the following controls for the third parties prioritized by risk. The evaluation must include management's processes for the ongoing assessment and monitoring of the organization's third parties.

A. A robust due diligence process for sourcing and selecting third parties is in place with a documented and approved business case or other relevant document describing and justifying the need for and nature of the relationship with the third party.

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

C. Final contracts or agreements are reviewed and approved by all relevant stakeholders, including legal and compliance, signed by authorized individuals from both parties, and stored securely. A contract manager or administrator is assigned responsibility for each contract.

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

E. Documented onboarding processes are established and followed to establish a foundation for third parties to meet the terms of the contract or agreement.

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

G. 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.

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

I. A formalized offboarding plan is implemented and followed to ensure contract requirements involving timing and expectations are adequately addressed. 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 IIA is an international professional association that serves more than 265,000 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 theiia.org.

Copyright

September 2025