Draft

The Institute of Internal Auditors

Third-Party Topical Requirement User Guide

Overview of Topical Requirements

Topical Requirements are an essential component of the International Professional Practices Framework®, along with the Global Internal Audit Standards™ and Global Guidance. The Institute of Internal Auditors requires the Topical Requirements to be used in conjunction with the Global Internal Audit Standards, which provide the authoritative basis of the required practices. References to the Standards appear throughout this guide as a source of more detailed information.

Topical Requirements formalize how internal auditors address prevalent risk areas to promote quality and consistency within the profession. Topical Requirements establish a baseline and provide relevant criteria for performing assurance services related to the subject of a Topical Requirement (Standard 13.4 Evaluation Criteria). Conformance with Topical Requirements is mandatory for assurance services and recommended for evaluation during advisory services. Topical Requirements are not intended to cover all potential aspects that should be considered when performing assurance engagements; rather, they are intended to provide a minimum set of requirements to enable a consistent, reliable assessment of the topic.

Topical Requirements clearly link to The IIA's Three Lines Model and the Global Internal Audit Standards. Governance, risk management, and control processes are the main components of Topical Requirements aligning with Standard 9.1 Understanding Governance, Risk Management, and Control Processes. In reference to the Three Lines Model, governance links to the board/governing body, risk management links to the second line, and controls or control processes link to the first line. While management is represented in both the first and second lines, the internal audit function is depicted in the third line as an independent and objective assurance provider, reporting to the board/governing body (Principle 8 Overseen by the Board).

Applicability, Risk, and Professional Judgment

Topical Requirements must be followed when internal audit functions perform assurance engagements on subjects for which a Topical Requirement exists or when aspects of the Topical Requirement are identified within other assurance engagements.

As described in the Standards, assessing risk is an important part of the chief audit executive's planning. Determining the assurance engagements to include in the internal audit plan requires assessing the organization's strategies, objectives, and risks at least annually (Standard 9.4 Internal Audit Plan). When planning individual assurance engagements, internal auditors must assess risks relevant to the engagement (Standard 13.2 Engagement Risk Assessment).

When the subject of a Topical Requirement is identified during the risk-based internal audit planning process and is included in the audit plan, then the requirements outlined in the Topical Requirement must be used to assess the topic within the applicable engagements. In addition, when internal auditors perform an engagement (either included or not included in the plan) and elements of a Topical Requirement emerge, the Topical Requirement must be assessed for applicability as part of the engagement. Lastly, if an engagement is requested that was not originally in the plan and includes the topic, the Topical Requirement must be assessed for applicability.

Professional judgment plays a key role in the application of the Topical Requirement. Risk assessments drive chief audit executives' decisions about which engagements to include in the internal audit plan (Standard 9.4). Additionally, internal auditors use professional judgment to determine what aspects will be covered within each engagement (Standards 13.3 Engagement Objectives and Scope, 13.4 Evaluation Criteria, and 13.6 Work Program).

Evidence that each requirement in the Topical Requirement was assessed for applicability must be retained, including a rationale explaining the exclusion of any requirements. Conformance with the Topical Requirement must be documented using auditors' professional judgment as described in Standard 14.6 Engagement Documentation.

While the Topical Requirement provides a baseline of control processes to consider, organizations that evaluate the risk topic as very high may need to assess additional aspects.

If a chief audit executive determines that the internal audit function does not have the required knowledge to perform audit engagements on a Topical Requirement subject, the engagement work may be outsourced (Standards 3.1 Competency, 7.2 Chief Audit Executive Qualifications,10.2 Human Resources Management). Even then, outsourcing does not release the internal audit function from its responsibility for conforming with the Topical Requirements. The chief audit executive retains the ultimate responsibility for ensuring conformance. In addition, if the chief audit executive determines internal audit resources are insufficient, the chief audit executive must inform the board about the impact of insufficient resources and how any resource shortfalls will be addressed (Standard 8.2 Resources).

Performance, Documentation, and Reporting

When applying Topical Requirements, internal auditors also must conform with the Standards, conducting their work in alignment with Domain V: Performing Internal Audit Services. The standards in Domain V describe planning engagements (Principle 13 Plan Engagements Effectively), conducting engagements (Principle 14 Conduct Engagement Work), and communicating engagement results (Principle 15 Communicate Engagement Results and Monitor Action Plans).

Coverage of the Topical Requirement can be documented in either the internal audit plan or the engagement workpapers based on auditors' professional judgment. One or more internal audit engagements may cover the requirements. In addition, not all requirements may be applicable. Evidence that the Topical Requirement was assessed for applicability must be retained, including a rationale explaining any exclusions.

Quality Assurance

The Standards require the chief audit executive to develop, implement, and maintain a quality assurance and improvement program that covers all aspects of the internal audit function (Standard 8.3 Quality). The results must be communicated to the board and senior management. Communications must report on the internal audit function's conformance with the Standards and achievement of performance objectives.

Conformance with Topical Requirements will be evaluated in quality assessments.

Third Party

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, services, labor, manufacturing, or information technology solutions, such as data storage, processing, and maintenance.

> The Topical Requirements use general internal auditing terminology as defined in the Global Internal Audit Standards™. Readers may find it helpful to review the terms and definitions in the Standards' glossary.

The term "third party" may be used differently based on industry or other contexts. In the Third-Party Topical Requirement and user guide, the term "third party" refers to vendors, suppliers, contractors, subcontractors, outsourced service providers, other agencies, and consultants. The term "third party" encompasses all such arrangements, including those between a third party and its subcontractors, often known as "downstream" subcontractors, or "fourth parties," "fifth parties," or "Nth parties."

This Topical Requirement is not intended to address indirect relationships, interests, or involvements with the primary organization, such as contracted employees, financial partners, regulators, agents, trustees, or other similar relationships, interests, or involvements with the primary organization. When applying the Third-Party Topical Requirement, internal auditors must clearly understand their organization's definition of third party.

When assessing the effectiveness of an organization's third-party processes, internal auditors should employ a top-down approach to develop an understanding of the organization's third-party policies, procedures, processes, framework, and life cycle. Internal auditors should use judgment to understand nuances in third-party risks based on individual industries, organizations, and engagement topics.

The Third-Party Topical Requirement and user guide refer to stages in an organization's relationship with its third parties, also known as life cycle stages: selecting, contracting, onboarding, monitoring, and offboarding. These stages will be used for the purposes of the Third-Party Topical Requirement and user guide, even though some industries have their own versions of the life cycle.

- **Selecting:** includes processes to determine the need for a third party, the plan for its use, and the due diligence for selection. Additionally, selection should include assessing the risks of potential and engaged third parties.
- **Contracting:** includes due diligence processes for drafting, negotiating, approving, and implementing a legal agreement with the third party.
- **Onboarding:** the stage that begins when the contract is signed to start the relationship.
- **Monitoring:** the post-contract stage, which includes processes for "in-life" management and ongoing monitoring of the third party. Usually, the approach is systematic and risk-based and should consider continuous improvement. It includes renewing ongoing third-party contracts or agreements when necessary.

- **Offboarding:** includes processes for ending contracts and agreements, maintaining an exit strategy for prioritized third parties and, when necessary, terminating the relationship with the third party. The processes typically use a risk-based approach and may involve a formal exit plan.

Although the primary organization may 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, the 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.

Engaging with third parties may reduce some costs of performing processes within the organization. However, it may introduce operational risks because the primary organization has less visibility into and authority over the third party's control processes. Working with third parties introduces risks that must be identified, assessed, and managed through appropriate governance, risk management, and control processes. 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 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.

Internal auditors should consider each stage of the third-party life cycle when assessing the requirements for governance, risk management, and control processes.

The requirements in the Third-Party Topical Requirement are divided into three sections:

- **Governance** – clearly defined baseline objectives and strategies for using third parties that support organizational goals, policies, and procedures.
- **Risk management** – processes to identify, analyze, manage, and monitor risks related to using third parties, including a process to escalate incidents promptly.
- **Controls** – management-established, periodically evaluated control processes to mitigate risks related to third parties.

Considerations

Internal auditors may use the following considerations to aid their implementation of the requirements in the Third-Party Topical Requirement. The lettering of each consideration is cross-referenced to its corresponding requirement. These considerations are illustrative but not mandatory. Internal auditors should rely on professional judgment when determining what to include in their assessments.

Governance Considerations

To assess how the governance processes, including board oversight, are applied to third-party objectives, internal auditors may review:

A. A formalized and documented risk-based approach or strategy for determining whether to use a third party. The strategy should be periodically reviewed.
   - Budgeted resources based on a cost-benefit analysis to justify engaging a third party, ensuring strategic alignment, and resource efficiency.
   - Management's evaluation of risks and controls, including those addressing issues with third parties.
   - Adequate human resources to contract, manage, and monitor third-party performance.
   - The integration of stakeholder feedback into the approach or strategy.

B. Policies, procedures, and other relevant documentation used to manage third-party processes, which could include standardized tools and templates to facilitate key governance, risk management, and control processes.
   - Processes to periodically evaluate policies and procedures, determine their adequacy, and update them as necessary.
   - Established criteria for selecting, contracting, onboarding, monitoring, and offboarding third parties.
   - The identification and periodic review of applicable regulatory requirements for alignment with policies and procedures.
   - Benchmarking exercises conducted to identify and compare leading third-party management practices.

C. Defined roles and responsibilities that support the achievement of third-party objectives, which could be done in alignment with The Three Lines Model.
   - Processes to evaluate whether the third party's values, ethics, and corporate social responsibility align with the primary organization's principles. The process should include how to address potential conflicts of interest or unethical practices early.
   - Processes to train personnel filling third-party management roles and periodically assess their competencies.
   - A process to evaluate whether training has been implemented to create organizationwide awareness about third parties.

D. Communication and engagement with relevant stakeholders throughout the third-party life cycle (for example, the board, senior management, operations, risk management, human

resources, information technology, information security, legal, compliance, procurement, and others), which includes:

- Information about third-party risks and known potential vulnerabilities in meeting minutes, reports, or emails.
- An exchange of information on third-party management and the promotion of collaboration (for example, through periodic cross-functional meetings).

Risk Management Considerations

To assess how risk management processes are applied to third-party objectives, internal auditors may review:

A. Standardized and comprehensive risk management processes that include defined roles and responsibilities.
   - Processes for assessing and managing third-party risks, including how key risks are:
     - Initially identified and reported.
     - Analyzed to evaluate their impact on the ability to achieve organizational objectives.
     - Mitigated, including action plans to reduce risk to an acceptable level.
     - Monitored, including detection and response to early warnings and a plan for ongoing reporting until threats are fully resolved.
   - Monitoring for adherence to processes and implementation of corrective actions for any deviations, to prevent undermining the organization's long-term goals or strategy.
   - Activities of a risk management committee or other group created to provide direct oversight of third parties and input to the board. Such a group should have a defined purpose and meet regularly. Evidence may include meeting minutes.

B. A documented risk assessment that identifies both inherent and residual risks and is appropriately reviewed and regularly updated following a due diligence process.
   - The primary organization's consideration of factors such as its size, maturity, and number of engaged third parties when developing a third-party risk assessment.
   - The existence of established and clear criteria for classifying and ranking third parties according to risks.
   - The organization's adherence to widely accepted risk assessment practices, including that the risk assessment be performed at the earliest possible stage, typically during the selection stage, such as proposal analysis, and before the onboarding stage.
   - Whether vendors complete a questionnaire to determine their risk ranking and priority based on inherent risks. The organization ensures that the questionnaires are completed by relevant personnel and are reviewed to ensure accuracy.
   - How the organization obtains periodic input regarding third-party risk management from functional areas, such as information technology, procurement, enterprise risk management, human resources, legal, compliance, operations, accounting, and finance.

C. Identified and documented risk responses, such as mitigation, acceptance, elimination, and sharing, that are commensurate with risk ranking and include consideration of the third party's control environment.
    - Documentation that responses to risks that exceed the primary organization's risk tolerance are reviewed for appropriateness, especially when the risks are accepted. These responses should include those addressing potential conflicts of interest with third parties.

D. The escalation processes for third-party risks, including how the level of threat or risk is evaluated, assigned, and prioritized. The review may include identifying the:
    - Definitions and explanations of the organization's risk levels – such as high, moderate, and low – and escalation procedures for each risk category.
    - List of third parties prioritized by identified risks and the mitigation status of any risk events.
    - Applicable legal, regulatory, and compliance requirements.
    - Impacts of risks, both financial and nonfinancial (for example, reputation).
    - Processes for communicating third-party risks to management and employees, including regular reporting of risk profile to the board (or other appropriate body). Communications should include updates on the remediation of any issues noted with prioritized third parties.
    - Processes for reassessing the ranking and prioritization when the primary organization's risk appetite and risk tolerance levels change.

Control Process Considerations

To assess how control processes are applied to cybersecurity objectives, internal auditors may review:

A. A documented business case or other relevant documentation for prioritized third parties that is approved as appropriate.The business case:
    - Justifies the need for a third party to achieve an organizational objective.
    - Outlines the nature of the relationship with the third party.
    - May address risks to the third party's ability to meet expectations and outline the potential impacts to meeting organizational objectives.
    - May include a detailed cost-benefit analysis.

B. Established sourcing processes – such as competitive bidding, requests for proposals, and sole sourcing – are followed.
    - Selection criteria are well-defined and include assessing past performance, references, reputation, and contract costs.
    - Due diligence includes processes to ensure the appropriate selection of vendors, such as forming cross-functional teams to review proposals. To mitigate the risk of bias, controls for review teams include procedures for team creation and requirements for disclosure of potential conflicts of interest.

- Due diligence includes assessing the third party's control environment; for example, conducting a site visit or reviewing the third party's:
  - Service organization controls (SOC) reports.
  - Financial stability.
  - Articles of incorporation or certificate of good standing.
  - Transparency of the decision-making of key management and stakeholders.
  - Organizational structure.
  - Operational stability.
  - Cybersecurity protocols.
  - Compliance with relevant laws, regulations, and standards.
  - Ethics.
  - History with the primary organization.
  - Reputation.
- Evidence that potential vendors or contractors only advance to the contracting stage of the life cycle after relevant due diligence processes have been performed and results have been analyzed.

c. Contracting processes and procedures are established and followed.
- Contracts are written with clear and unambiguous terms.
- Essential elements of contracts are determined based on the organization's contracting policies and procedures and the third party's level of priority. Elements may include:
  - Nondisclosure (privacy) agreements.
  - Termination clauses and defined data access parameters.
  - Cybersecurity requirements, including those for accessing and sharing data and reporting on incidents or breaches within a specified period.
  - Requirements for notifications of a breach affecting the primary organization's data.
  - A standardized process for verifying identification, including full legal name, address, physical location, and website. A standard practice is to use a checklist during the identification process and to review the accuracy of the information.
  - Clearly defined service-level agreements, specifying the rights and obligations, penalties, rewards, and responsibilities of each party, the expected outcomes, and the parties responsible for paying all labor costs (including downstream subcontractors).
  - A right-to-audit clause that includes downstream subcontractors, or a requirement for evidence that vendors or contractors have been audited by a reputable, independent assurance provider.
- Access to the control assessment reports of independent auditors; for example, financial, audit, compliance, and data security, such as International Standards for Assurance Engagements or SOC reports.

- Additional contract components that may be essential to specific organizations or types of contracts:
  - Environmental and sustainability clauses.
  - Whistleblowing protocols.
  - Requirements for performance measure assessments.
  - Tested business continuity plan for third parties.
  - Usage of artificial intelligence in service delivery.
  - Clear identification, disclosure, terms, and scope for any downstream subcontracted work.
  - Change management process, outlining how to handle changes to the scope, terms, or operational requirements (like changes in technology or regulatory updates) during the contract term.
  - Limits on the number of change orders or amounts that can be billed.
- Final products are formally accepted before payment is made or any retainage is released.
- Requirements to share the ethics policies that the third party follows or to adhere to the primary organization's ethics policies (such as a code of conduct).

D. A contract or other official document signifying an outsourced relationship and the third party's obligation, and evidence of any required legal and compliance reviews.
- Key risks are considered during the contract drafting stage, and relevant clauses are included. Issues requiring resolution are communicated with the third party during this stage.
- Finalized contracts or agreements are reviewed and approved by appropriate stakeholders, stored securely, and assigned to a contract manager or administrator for responsibility.

E. An accurate, complete, and current listing of all third-party relationships is maintained. This may be within a centralized contract management system.
- A process for adding new third-party contracts or agreements to the listing or system.
- A process to enter potential third parties into the vendor system and remove them if the contract is not approved.
- A process for removing third-party contracts or agreements from the listing or system.
- A tracking system is used to document issues with specific contractors or vendors for future reference.

F. Standardized onboarding procedures that ensure all necessary documentation, training, and compliance reviews are completed. Reviews may include verifying whether:
- The third-party's systems and processes can seamlessly integrate with the primary organization's technology.
- Shared systems are compatible and secure. Evidence may include complementary user entity controls as part of SOC reporting.

- The primary organization assesses the vendor's business continuity plans to ensure ongoing service during emergencies. Contingency plans are included to address potential disruptions.

G. Processes for the ongoing monitoring of vendor performance relative to the contract or agreement objectives, including evaluations of key performance indicators.
  - Monitoring processes inform the third-party risk assessment, and identified control weaknesses are reviewed, escalated, and addressed as needed.
  - Reports or observations of processes, technologies, and tools established to manage monitoring in real time.
  - Processes to ensure payments are made in accordance with contract or agreement terms, such as meeting project timelines, milestones, and communication requirements. Payments are made only to approved contractors that have completed the onboarding stage and been entered into the vendor payment system. When deliverables are specified in the contract, final payments are only made once the deliverables have been verified.
  - Monitoring to control costs associated with third-party agreements to ensure value and determine return on investment. Results of cost-benefit analyses are used to renegotiate contracts.
  - Processes for assessing penalties for noncompliance with any service-level agreements in the contract or agreement. Penalties are calculated and charged when incurred.
  - The ranking of prioritized third parties is reevaluated periodically, when there are changes to an agreement, and when a contract is close to expiration or auto-renew.
  - Reviews of prioritized third parties, such as on-site or quarterly business reviews, to validate controls and operational integrity.
  - Evidence of additional ongoing monitoring may include:
    - Analyses of the third party's financial stability.
    - Assessments of complaints against third parties.
    - Management's reviews of independent auditor reports such as International Standards for Assurance Engagements, Statement on Standards for Attestation Engagements, financial, audit, compliance, and data security reporting provided by third parties; ISO certifications.
    - Management's reviews of business resilience tests conducted by the third party, including any significant issues identified.
    - Conditions for and restrictions on the use of subcontracted or downstream parties.
    - Evaluations of third-party ethical values, culture, and conduct.
    - Responses to media inquiries.
    - Evaluations of privacy and cybersecurity protocols to protect the storage and transfer of the primary organization's data and information, including the usage of advanced technologies such as artificial intelligence.
    - The organization's identification of opportunities for continuous improvement of performance and meeting contract or agreement objectives.

H. Protocols to initiate corrective action on identified incidents when a third party fails to meet the requirements of a contract or agreement, or if third-party actions increase risk to the primary organization.
    - Protocols for escalating incidents based on the incident's severity and the priority of the third party.
    - Post-incident review, including root cause analysis.

I. Processes to provide alerts for contracts and agreements approaching expiration or auto-renewal. Auto-renewal processes include reviewing:
    - The third party's performance.
    - Contract or agreement terms and any addenda.
    - Risk factors.

F. A formalized offboarding plan is implemented and followed.
    - Checklists or interviews with key stakeholders to ensure security measures are effective.
    - Organizational information or data in the custody of a third party has been returned or destroyed.
    - The third party's access to the organization's data, systems, or facilities has been revoked.
    - The primary organization's assets, such as devices, software licenses, intellectual property, and documentation, have been returned.
    - When a third party is terminated for cause, the extenuating circumstances or risks are identified and escalated to senior management and/or the board.
    - When the contract of a prioritized third party is terminated, the party is replaced.

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 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

March 2025