Third-Party

Topical Requirement User Guide

The Institute of
Internal Auditors

Contents

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 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 risks 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 the internal audit function does not have the required competencies to perform engagements on a Topical Requirement subject, the chief audit executive must determine how to obtain the resources and communicate timely to the board and senior management the impact of the limitations and how any resource shortfalls will be addressed. The chief audit executive retains the ultimate responsibility for ensuring the internal audit function's conformance with the Topical Requirements, regardless of how the resources are obtained (Standards 3.1 Competency, 7.2 Chief Audit Executive Qualifications, 8.2 Resources, 10.2 Human Resources Management).

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).

Topical Requirements are designed to support consistent, high-quality internal audit practices. Local laws, regulations, supervisory expectations, and other professionally recognized frameworks may impose additional or more specific requirements. Internal auditors must understand and abide by the laws and/or regulations relevant to the industry and jurisdictions in which the organization operates, including making disclosures as required, according to Standard 1.3 Legal and Ethical Behavior. Internal auditors may have already integrated these additional requirements into audit programs and testing procedures and should reconcile them against the Topical Requirement to ensure adequate coverage.

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 ("the primary organization") establishes a business relationship to obtain products or services. The 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.

> **Note**
>
> The Topical Requirements use general internal auditing terminology as defined in the Global Internal Audit Standards. Readers should refer to the terms and definitions in the Standards' glossary.

The term "third party" may be used differently based on industry or other contexts. Each internal audit function has the flexibility to use its judgment in application of the Topical Requirement according to how the primary organization (the organization entering into a third-party agreement) defines third parties. 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 external relationships, interests, or involvements with the primary organization, such as regulators, agents, brokers, investors, trustees/board members, public services, and members of the general public, or internal relationships, such as employees or intragroup service providers.

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 effectiveness of an organization's processes to manage its third-party relationships can be assessed across the organization and/or at the level of one or more individual contracts, agreements, or relationships. 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. In alignment with Standard 5.1 Use of Information, internal auditors should be aware of and compliant with any policies and procedures related to the third-party information they may access.

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.

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. The stages are:

- 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: begins when the contract is signed to start the relationship and establishes a foundation for third parties to meet the terms of the contract or agreement.
- Monitoring: includes processes for "in-life" management and ongoing monitoring of the third party after the contract has been established and approved. The approach is usually systematic and risk-based and should consider continuous improvement. Monitoring includes renewing ongoing third-party contracts or agreements when necessary.
- Offboarding: includes processes for ending contracts and agreements, maintaining an exit strategy for third parties that have been prioritized based on risk, and terminating relationships when necessary. The processes typically use a risk-based approach and may involve a formal exit plan.

The primary organization 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. Engaging with third parties may reduce some of the organization's costs of performing processes. However, it may introduce operational risks because the primary organization has less visibility into and authority over the third party's 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.

The primary organization must identify, assess, and manage risks through appropriate governance, risk management, and control processes. Categories and examples of risks related to third parties include:

- Strategic, such as the ability to accomplish the 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.

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 as per Standard 9.1 Understanding Governance, Risk Management, and Control Processes:

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

In addition to the Topical Requirement and this user guide, internal auditors may want to refer to additional professional guidance on third parties, such as IPPF Global Guidance and industry-specific resources.

Considerations

The following considerations may help internal auditors implement the requirements in the Third-Party Topical Requirement. The lettered statements in each section below restate or paraphrase the corresponding requirements of the Topical Requirement. These nonmandatory considerations are illustrative to provide examples of ways to assess the requirements. Internal auditors should apply 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 evidence of:

A. A formalized and documented risk-based approach or strategy for determining whether to use a third party. The approach is periodically reviewed and includes:

- A clearly defined and standardized process to implement the approach, approved for use by the organization.
- 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 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 define, assess, and manage third-party relationships throughout the life cycle. The polices and procedures may 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. Further evidence may include:

- 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 promptly address potential conflicts of interest or unethical practices.
- Regular training of personnel filling third-party management roles and periodic assessment of their competencies.
- A process to evaluate whether training has been implemented to create organizationwide awareness about third parties.
- Roles and responsibilities are aligned with the Three Lines Model.

D. Timely communication and engagement with relevant stakeholders throughout the third-party life cycle (for example, the board, senior management, procurement, operations, risk management, compliance, legal, information technology, information security, human resources, 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 evidence that:

A. Standardized and comprehensive risk management processes for the user of third-party services include defined roles and responsibilities and sufficiently address key risks relevant to the organization:

- Processes for assessing and managing third-party risks include 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 takes place for adherence to processes and implementation of corrective actions for any deviations, to prevent undermining the organization's long-term goals or strategy.
- A risk management committee or other group provides direct oversight of third parties and input to the board. The committee has a defined purpose and meets regularly. Evidence may include meeting minutes.

B. Risks related to third parties throughout the life cycle are identified and assessed regularly. The risk assessment ranks and prioritizes third parties. Risk responses are ranked and prioritized.

- The primary organization considers factors such as its size, maturity, and number of engaged third parties when developing a third-party risk assessment.
- The risk assessment is documented and identifies inherent and residual risks.
- The organization follows a due diligence process for reviewing and updating the risk assessment.
- Criteria are established to rank and prioritize third parties according to risks. Examples of such criteria include:
    - The services provided are critical to the organization's operations.
    - The financial value of the arrangement is material.
    - The relationship is new, entered into quickly, and/or its duration is long.
    - Several external parties are involved.
    - The third party plans to subcontract some or all of the work.
- The organization adheres to widely accepted risk assessment practices, including that the risk assessment be performed at the earliest possible stage, typically when the proposal is analyzed during the selection stage, and before onboarding.
- 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.
- 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. Risk responses, such as mitigation, acceptance, elimination, and sharing, are identified and commensurate with the risk ranking.

- Risk responses are documented 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. The responses include those addressing potential conflicts of interest with third parties.

D. The processes for managing and escalating 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 Considerations

To assess how control processes are applied to third-party relationships, internal auditors may review evidence that:

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 documentation describing and justifying the need for and nature of the relationship with the third party.

   - The business case also may:
     - Address risks to the third party's ability to meet expectations and the potential impacts to the organization.
     - Include a detailed cost-benefit analysis.
   - Established sourcing processes — such as competitive bidding, requests for proposals, and sole sourcing — are followed. The processes include:
     - Criteria for important aspects, such as reviewing cybersecurity protocols, verifying bank details, conducting financial background checks, and researching the third party's organizational structure, criminal and legal records, driving records, political activities, and ties to criminal activities.
     - Well-defined selection criteria including for assessing past performance, references, reputation, and contract costs.
     - Due diligence 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 in assessing the third party's control environment; for example, conducting a site visit or reviewing the third party's:
       - System and Organization Control (SOC) reports.
       - Financial stability.
       - Articles of incorporation or certificate of good standing.
       - Transparency in 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 the results have been analyzed.

B. Contracting policies and procedures are established and followed.

- Contracts are written in unambiguous terms.
- 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.
- 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 parameters for data access.
    - Cybersecurity requirements, including those for accessing and sharing all 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 the third party's identification, including full legal name, address, physical location(s), 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 expected outcomes and the rights, obligations, penalties, rewards, and responsibilities of each party, including the responsibility for paying labor costs (including downstream subcontractors).
    - A right-to-audit clause that includes downstream subcontractors, or a requirement for evidence that a reputable, independent assurance provider has audited the parties. Without a right-to-audit clause, the internal audit function's ability to obtain or provide assurance may be limited.
- The primary organization has access to the control assessment reports of independent auditors; for example, those on financial, compliance, and data security, such as International Standard on Assurance Engagements or SOC reports.

        - If relying on the work of the third party's external assurance providers, documents are reviewed to ensure reliability.
        - SOC reports are used to identify inadequate risk and change management processes.

    - Policies and procedures address any components 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 (such as changes in technology or regulatory updates) during the contract term.
        - Limits on the number of change orders or amounts that can be billed.
    - Policies and procedures require formal acceptance of final products before payment is made or any retainage is released.
    - Third parties are required to share their ethics policies or code of conduct and/or to adhere to those of the primary organization.
    - Where the third party provides the contract, the primary organization has conducted a legal review, and key risks are understood and supported by a suitable risk mitigation strategy.

C. Finalized contracts or agreements are reviewed and approved by appropriate stakeholders, including legal and compliance, stored securely, and assigned to a contract manager or administrator for responsibility.

    - 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.

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

    - A process for adding new third-party contracts or agreements to the listing or system.
    - A process for entering potential third parties into the vendor system and removing them if the contract is not approved.
    - A process for removing third-party contracts or agreements from the listing or system.

- A tracking system to document issues with specific contractors or vendors for future reference.
- A review process to determine whether the third-party population is accurate and complete.

E. Documented onboarding processes are established and followed to enable third parties to meet the terms of the contract or agreement. Reviews may include verifying whether:

   - Standardized onboarding procedures ensure all necessary documentation, training, and compliance reviews are completed.
   - 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 third party’s business continuity plans, which ensure service continues during emergencies. Contingency plans are included to address potential disruptions.

F. 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 risk-based 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-renewal.
   - 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 Standard on Assurance Engagements, Statements 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.
- Review of segregation of duties.

G. 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.

H. 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.

I. A formalized offboarding plan is implemented and followed to ensure contract requirements involving timing and expectations are adequately addressed, including for any downstream subcontractors.

- 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 based on the same risk assessment, unless the contract is completed or no longer needed.

Appendix A. Practical Application Examples

The following examples describe scenarios in which the Third-Party Topical Requirement would be applicable:

Example 1: An internal audit engagement on the internal audit plan includes a service or output that is currently provided by a third party.

When the internal audit function completes its risk-based planning process and includes one or more engagements in the internal audit plan of services or outputs that are currently provided by third parties under a contract or agreement, the Topical Requirement is mandated.

Not every requirement in the Topical Requirement may apply in every engagement. When internal auditors apply professional judgment and determine that one or more requirements of the Third-Party Topical Requirement are not applicable and therefore should be excluded from an engagement, internal auditors must document and retain the rationale for excluding those requirements. For example, the rationale for excluding certain requirements could be that the internal audit function has determined that the organization's reliance on third parties for mission-critical services is low, or it is an established relationship with low financial impact.

Example 2: Third-party risks are identified during an assurance engagement on a topic other than third parties or contract management.

Internal auditors may identify a significant third-party risk while assessing a process not initially determined to be related to third parties or contract management. For example, when planning an engagement to assess data storage, internal auditors learn that cloud services are hosted through a third party. During interviews with the management of the third-party provided services, internal auditors identify cybersecurity risks related to the third party.

Once relevant risks have been identified, internal auditors must review both the Third-Party and Cybersecurity Topical Requirements and determine which requirements are applicable. Auditors might exclude the third-party governance process or the third-party risk management process in the scope of the engagement and focus on third-party controls over the services being audited. This same professional judgment applies to the application of the Cybersecurity Topical Requirement. Auditors must document in the engagement workpapers the rationale for excluding any requirements of the Third-Party or Cybersecurity Topical Requirements and retain the documentation.

Example 3: A third-party engagement that was not originally included in the internal audit plan is needed.

An issue arises within the organization involving a prioritized third party that requires immediate attention from the internal audit function. The issue involved a control failure. The chief audit executive should communicate with the board about reprioritizing the internal audit function's audit plan and resources to accommodate the need. The auditor should engage with impacted management to develop engagement objectives to evaluate the situation and make recommendations to prevent future occurrences. The chief audit executive should review the Topical Requirement to scope the engagement, determine which requirements apply, and document any exclusions accordingly.

Appendix B. Optional Documentation Tool

Internal auditors are expected to exercise professional judgment in determining the applicability of the requirements based on the risk assessment and appropriately document the exclusions of certain requirements. The Topical Requirement can be documented in the internal audit plan or in the engagement workpapers based on the auditor's professional judgment. One or more internal audit engagements may cover the requirements. In addition, not all requirements may be applicable. The printable form below provides one option for documenting conformance with the Third-Party Topical Requirement, but its use is not mandatory.

Third-Party Governance

Requirement	Executed Coverage or Rationale for Exclusion	Documentation Reference
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.		

Requirement	Executed Coverage or Rationale for Exclusion	Documentation Reference
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.		

Third-Party Risk Management

Requirement	Executed Coverage or Rationale for Exclusion	Documentation Reference
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.		

Requirement	Executed Coverage or Rationale for Exclusion	Documentation Reference
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.		

Third-Party Controls

Requirement	Executed Coverage or Rationale for Exclusion	Documentation Reference
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.		

Requirement	Executed Coverage or Rationale for Exclusion	Documentation Reference
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 life cycle 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.		

Requirement	Executed Coverage or Rationale for Exclusion	Documentation Reference
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.

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

September 2025

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