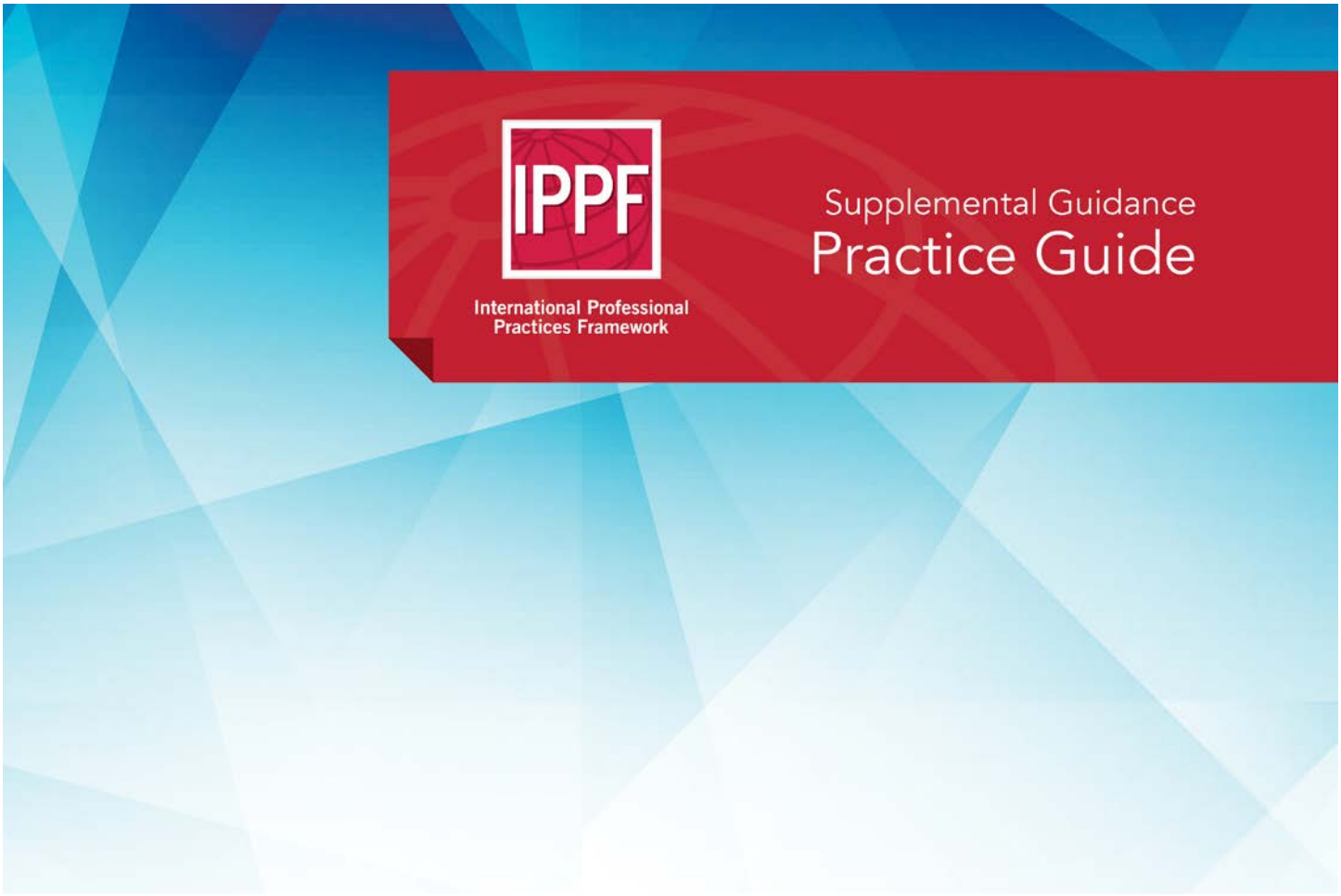


Auditing Third-party Risk Management

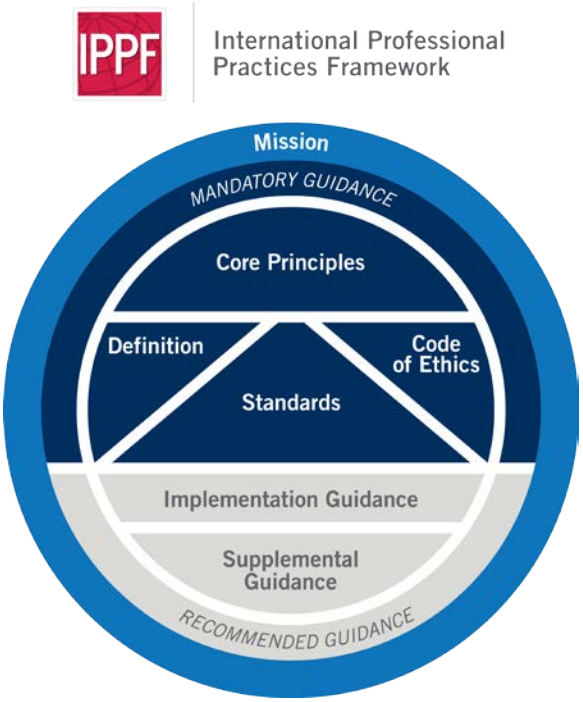
The Institute of Internal Auditors | Global

About the IPPF

The International Professional Practices Framework® (IPPF®) is the conceptual framework that organizes authoritative guidance promulgated by The IIA. A trustworthy, global, guidance-setting body, The IIA provides internal audit professionals worldwide with authoritative guidance organized in the IPPF as Mandatory Guidance and Recommended Guidance.

Mandatory Guidance is developed following an established due diligence process, which includes a period of public exposure for stakeholder input. The mandatory elements of the IPPF are:

- Core Principles for the Professional Practice of Internal Auditing.
- Definition of Internal Auditing.
- Code of Ethics.
- *International Standards for the Professional Practice of Internal Auditing*.



About Supplemental Guidance

Supplemental Guidance is part of the IPPF and provides additional recommended, nonmandatory guidance for conducting internal audit activities. While supporting the *Standards*, Supplemental Guidance is intended to address topical areas, as well as sector-specific issues, in greater procedural detail than the *Standards* or Implementation Guides. Supplemental Guidance is endorsed by The IIA through formal review and approval processes.

Practice Guides

Practice Guides are a type of Supplemental Guidance that provide detailed step-by-step approaches, featuring processes, procedures, tools, and programs, as well as examples of deliverables.

Practice Guides are intended to support internal auditors. Practice Guides are also available to support:

- Financial Services.
- Public Sector.
- Information Technology (GTAG®).

For an overview of authoritative guidance materials provided by The IIA, please visit www.globaliia.org/standards-guidance.

Table of Contents

Executive Summary

Organizations leverage and rely on third-party providers, as well as subservice or "fourth-party" providers, to conduct business activities.[1] These relationships continue to expand and evolve, introducing numerous risks that must be continuously assessed and appropriately managed by the organization to achieve desired business outcomes. In regulated industries, courts of law, and the court of public opinion, an organization cannot escape blame, including potentially severe repercussions in terms of reputation or financial penalties, if a third-party provider fails to perform as contracted or suffers its own unfortunate event or unethical practices.

Because organizations and their customers can suffer adverse consequences as a result of the actions (or inaction) of their third-party providers, regulators and standard-setting organizations for some industries (e.g., financial services) have established rules, regulations, and guidance concerning the management of third-party providers. These rules can mandate sophisticated third-party risk management models, but the principles used to construct these regulatory requirements are adaptable by other industries that may not have defined benchmarks or parameters to guide them in developing and executing third-party risk management.

This guide introduces internal auditors to the concept of a third-party risk management framework as an element of a larger enterprise risk management framework. It also considers that organizations come in all shapes and sizes, with differing availability of resources, tools, and techniques. To that end, this guide prompts internal auditors to learn the objectives of the organization's third-party provider selection and management process. It also provides practical considerations for developing an audit of the organization's third-party risk management methods.

Learning the elements of an organization's third-party risk management processes may enable the internal audit function to identify areas where the organization may obtain additional value from their third-party relationships while helping the organization protect itself from unnecessary risk exposure.

[1] A subservice or fourth party is an organization engaged and contracted by the third party to perform all or part of the outsourced activities that the third party was originally contracted to undertake. The *International Professional Practices Framework, 2017 Edition*, defines risk as "the possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood."

Introduction

The engagement of third-party providers, as well as subservice or "fourth-party" providers, presents risks that organizations should take action to manage. Risks posed by an organization's third-party providers should be considered in the development of a comprehensive risk-based audit plan. To facilitate efficient and effective information gathering and assessment criteria, internal auditors must understand how the organization structures its third-party risk management programs; how third-party risk management processes relate to the organization's risk appetite; and the roles and responsibilities of participants in the third-party provider risk management process.

Embarking on a formalized plan of auditing third-party risk management can help internal audit functions explore how their organization addresses questions such as:

- Does the organization have a comprehensive inventory of its third-party providers?
- Does the organization's third-party risk management program align with its risk appetite?
- Does the organization have a list of the types of risks (reputational, strategic, compliance, financial, human resources, IT, etc.) third parties may pose?
- How does the organization identify, define, and manage third-party risks?
- What are the appropriate assessment criteria for third-party risks (e.g., impact and likelihood scales)?
- How does the organization gauge the impact individual third parties may have on its business continuity strategy?
- How far down the supply chain should third parties be considered? Should subservice or fourth-party providers be monitored?
- What metrics should be reviewed to ensure a third-party provider is performing within the organization's risk tolerance?
- Will the organization have recourse to recover damages from a third party if problems arise?
- Do contracts with third parties include the right for the contracting organization's internal audit activity or other control functions to conduct audits if there is a need or desire to do so?
- Is the third party handling data that requires a specific level of control? How does the organization validate that the third party is following all relevant laws, regulations, and technical requirements for data security?
- How does internal audit coordinate with the organization's second line of defense (e.g., legal, compliance, procurement) that may be performing risk management activities regarding third parties?
- How does the organization ensure ethical behavior by the third parties?

Internal audit must weigh the importance of the organization's third-party risks and the governance entity's need for assurance against the stated risk profile and the cost of providing that assurance. This practice guide will assist internal auditors in ensuring adequate and valuable third-party internal audit coverage and in finding the right balance for their organization.

After reading this guidance, internal auditors will be able to:

- Understand key roles, responsibilities, and risks related to managing an organization's third-party providers.
- Appropriately assess third-party risk management activities across the first-line business, oversight, and control functions.
- Define a third-party risk management internal audit coverage approach and framework.
- Scope and deliver internal audit engagements that provide appropriate risk-based coverage of the organization's third-party risk management framework and processes.

Business Significance: Key Risks and Opportunities

When key third parties fall short of service expectations or fail altogether, the resulting reputational and operational damage to clients can be as significant as or may even exceed the damage suffered by the third party itself.

Significant data breaches involving third parties have occurred in recent years, resulting in material losses. In the aftermath of a severe incident, no one remembers the name of the third-party provider contracted by an organization that may have been the source of the breach. Rather, the fault and possible reputation damage — warranted or not — lies with the organization itself. Reputational damage is difficult to anticipate and measure, which makes robust third-party risk assessment, due diligence, and monitoring even more critical.

When an organization relies on third-party suppliers or service providers, risk exposures change. The term "third party" is often used in reference to significant projects — such as outsourced labor, data processing, or manufacturing — but the associated risks can apply to every contractual relationship, no matter how small. Risks may also extend to include the organization's vendor relationships with their service providers or suppliers, known as subservice or fourth parties.

Internal auditors have an opportunity to provide valuable third-party risk management assurance to management. Well-informed internal auditors may uncover missed revenue or opportunities for cost savings, contribute to reducing fraud and operational risk, and identify third-party risk management process improvements, thus helping management improve the control structure of the organization overall.

Elements of a Third-party Risk Management Program

Risk Management Approach

In accordance with Standard 2200 – Engagement Planning and planning an assessment of an organization's third-party risk management processes, internal auditors should first determine if

the organization employs a defined third-party risk management program for this specific element of their organization's enterprise risk management framework. If so, internal auditors can identify the policies, processes, and tools used to control risks related to third parties.

Reputational damage is difficult to anticipate and measure, which makes robust third-party risk assessment, due diligence, and monitoring critical. However, rather than implementing a thoughtfully designed and complete third-party risk management program, many organizations continue with processes that have grown organically within the business over time. Processes developed or evolved this way are often inconsistent or fragmented across business lines, regions, products, etc.

Internal audit can provide value by identifying the elements comprising the organization's risk management framework. If the framework is unclear, internal audit may introduce one of the many frameworks available to use as models for a more cohesive approach to enterprise risk management, such as COSO's Enterprise Risk Management framework and ISO 31000:2018. A third-party risk management framework would be a component of that overarching enterprise risk management framework.

There are three key elements of third-party risk management that may be present:

1. A framework specifically geared toward third-party risk management.
2. Risk appetite statement (could be an overall statement, a business-unit level statement, or a statement for each third party).
3. Third-party risk management governance structure.

The following sections will assist internal auditors in identifying the risk management framework and risk appetite that informs and shapes the organization's third-party risk management efforts, and provide information regarding potential roles, responsibilities, and information flows throughout the third-party risk management framework.

Third-party Risk Management Framework

The purpose of a third-party risk management framework is to ensure the risk exposures associated with third parties are managed and monitored according to the organization's risk appetite and governance requirements. If an organization is considering engaging with a third party (including cosourcing), it must consider whether the purpose of doing so is in the scope of the third-party risk management framework. If so, it is obligated to manage the organization's relationship with that third party according to the organization's agreed-upon third-party risk management framework and process(es).

Effective third-party risk management frameworks often have common characteristics including:

1. Sufficient policies, procedures, and activities that support it, including alignment with the organization's risk appetite, stakeholder expectations, and industry standards.
2. Effectual governance structures supporting the policies, procedures, and activities that support it.
3. A structured support system comprising:

   - Defined roles and responsibilities for each of the Three Lines of Defense and governing bodies.[2]
   - A third-party inventory (vendor master file), risk rating criteria, and risk assessment process.
   - Expectations related to third-party risk management controls.
   - Reporting requirements for third-party risk exposures including the expectations of an organization's board.[3]
   - A risk-based third-party review process executed on a regular basis as appropriate.
   - Processes for the classification, escalation, and tracking of findings that result from third-party monitoring activities.

Risk Appetite

The IIA defines risk appetite as the level of risk that an organization is willing to accept.[4] For an organization to determine whether a third-party relationship is consistent with their risk appetite, ask this question: Is the level of risk exposure the organization may incur by outsourcing (or cosourcing) this service, product, raw material, or component in line with the organization's risk appetite?

[2] The Institute of Internal Auditors. The IIA's Position Paper: *The Three Lines of Defense in Effective Risk Management and Control* (Altamonte Springs: The Institute of Internal Auditors, 2013).

[3] The *International Professional Practices Framework (IPPF), 2017 Edition,* defines board as "the highest level governing body (e.g., a board of directors, a supervisory board, or a board of governors or trustees) charged with the responsibility to direct and/or oversee the organization's activities and hold senior management accountable. Although governance arrangements may vary among jurisdictions and sectors, typically the board includes members who are not part of management. If a board does not exist, the word "board" in the *Standards* refers to a group or person charged with governance of the organization. Furthermore, "board" in the *Standards* may refer to a committee or another body to which the governing body has delegated certain functions (e.g., an audit committee)."

[4] The Institute of Internal Auditors, *International Professional Practices Framework (IPPF), 2017 Edition,* (Lake Mary: Internal Audit Foundation, 2017), 243.

The answer should take into account the negative and positive levels of risk exposure the organization may incur and evaluate them against its stated risk appetite. Outsourcing the manufacturing of a product may carry with it the risks of regulatory fines, reputational damage, etc. However, the positive benefits in terms of quality, cost, and efficiency may offset the potential negative exposures.

If the positive benefits outweigh the risk exposure, and the organization can be reasonably sure the third party will perform as agreed, the venture may be determined to be worthwhile by senior management and/or the board as required by policy. Ensuring the third party will perform as agreed with both contracted parties having the same understanding of the terms is the challenging aspect of evaluating the proposed third-party venture against the organization's risk appetite.

Example of a Risk Appetite Disparity

The organization's business continuity plan requires an inoperable software program be restored to working order within 48 hours after going down, but there is no corresponding service level agreement (SLA) with the third-party provider requiring they accomplish working-order recovery in this timeframe.

This constitutes a disparity between the SLA and the organization's risk appetite.

When an organization agrees to pursue a strategy that involves engaging a third party, management should clearly communicate the minimum standards required regarding the capabilities of the candidate(s) in terms of governance, risk management, and internal control for the third party to stay within the limits of the organization's risk appetite. If an organization struggles with imposing their "minimum standards" of internal control and risk management on third parties they wish to engage, this can affect the risk exposure at the organizational level. If the organization uses a third-party risk management framework, internal auditors can assess whether each third party it audits complies with the organization's stated or implied risk appetite and whether minimum standards are enforced.

Whatever system is used to track risk information, dashboards and reports produced should be supplied to senior management, the board, and appropriate committees (such as the risk management committee if one exists) to evaluate and ascertain changes to risk conditions and measures and determine if action is needed to keep risk exposure consistent with the organization's risk appetite.

Third-party Risk Management Governance

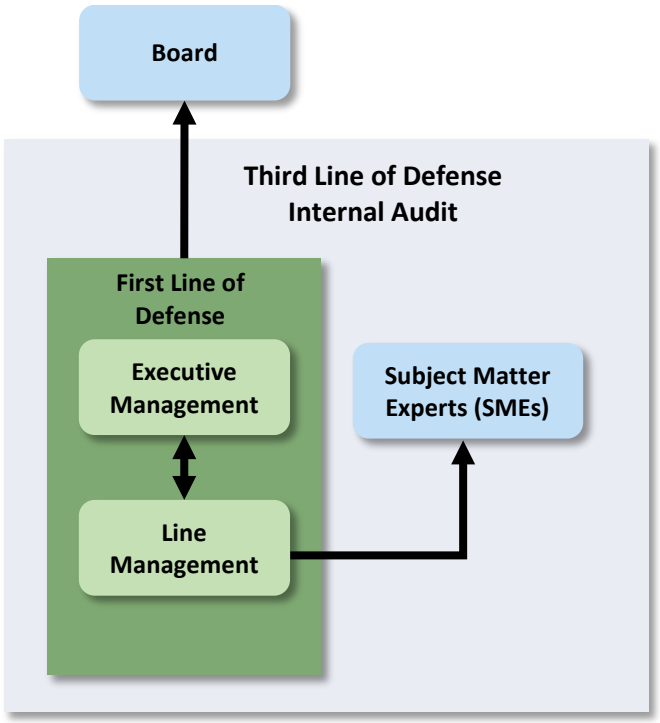
Third-party risk management governance structures can vary widely depending on the organization's use of third parties, the complexity and size of the organization, and the organization's maturity level with regard to third-party risk management and the expression of its risk appetite.

The governance structure can be simple with business managers making their own decisions about qualifying third parties, or complex as in having hundreds of procurement managers managing thousands of third-party relationships. Variations appear throughout this guidance as a convenience.

However, these governance structures share a common characteristic: those requesting the product or service are responsible for managing the overall risk exposure the third party brings to the organization. They become the owners and enforcers of the organization's risk appetite no matter how simple or sophisticated the third-party risk management program is in terms of governance structure and process.

In organizations with more informal third-party risk management processes and procedures, internal auditors may encounter a "basic" third-party risk management governance structure as shown in Figure 1.[5]

Figure 1: Third-party Risk Management Governance – Basic



[5] The graphics illustrating various third-party risk management program structures use the traditional concepts of first, second, and third lines of defense as noted in The IIA's position paper, *The Three Lines of Defense in Effective Risk Management and Control*. In this paper, The IIA includes procurement functions in the second line of defense, which is reflected in this practice guide. Your organization may differ in its interpretation of the three lines of defense's control and risk functions that may have a role in third-party risk management.

In this decentralized structure, managers are responsible for identifying needs for third-party products and services, thus acting as relationship owners. They are also responsible for executing any due diligence requirements the organization may have. Regarding recordkeeping, managers (as relationship owners) may store third-party files and monitor the third parties under their control according to a defined or undefined process. After finalization of the contract between the third party and relationship owner, upper level management would review it and either offer approval or request modifications.

Documentation for this basic structure may consist of checklists regarding required due diligence documentation and perhaps lists or inventories of third parties. Policies and procedures may exist regarding the organization's engagement of third parties. However, the documentation and processes may be informal at this level with documentation standards enforced inconsistently among business areas.

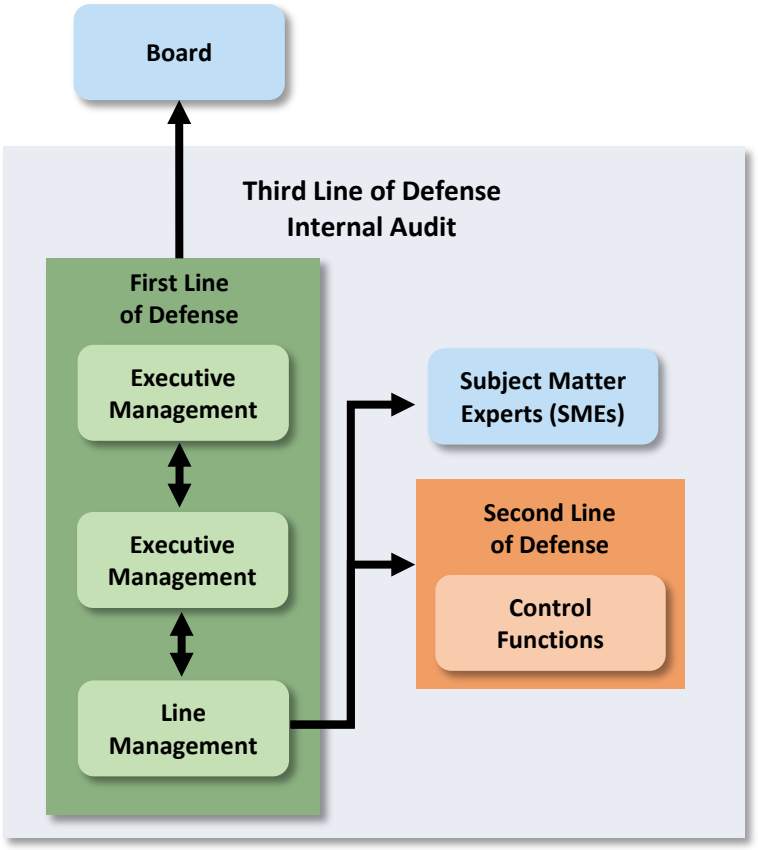
This structure may create a conflict of interest, especially when relationship owners have a bias to a specific third party. Close supervision from oversight functions, senior management, and/or the board is advised to address this risk. One common control employed by organizations to manage this risk is documentation that specifies expenditure restrictions for various levels of management (e.g., senior management individuals may have the authority to sign a contract worth up to $1 million, with contracts exceeding that ceiling requiring two senior management signatures). Third-party relationships that involve large expenditures (according to the organization's materiality standards) and/or present a significant organizational risk exposure may be sent to senior management and, possibly, to the board for approval. Managers' authorities are often more restricted requiring higher levels of approval when the relationship is established on a sole-source basis rather than employing a competitive bidding process.

Another risk to consider with this decentralized model of third-party risk management is inconsistency in the level of due diligence and review third parties may receive from management. To address this risk, organizations at this basic level may assign ownership to one individual or area for filing third-party information including contracts, Service Level Agreements (SLAs), and ancillary documents. This individual may create a file for each third party, following it through the contract's life cycle.

At a minimum, this oversight control facilitates the effective gathering of third-party documentation. Beyond managing third-party documentation, it is ideal if this individual operates additional controls in terms of reviewing documents for completion, appropriate signatures, etc. There should also be a list of documents required for each third party with processes to ensure their collection and validation. If, in internal audit's opinion, third-party documentation is not consistently gathered and reviewed, internal audit may recommend better control and monitoring of third-party information.

In organizations with more defined third-party risk management processes and procedures, internal auditors may encounter a governance structure similar to that shown in Figure 2. At this level, managers are still responsible for contracts and SLAs. The difference between a basic governance structure and a more defined one is that personnel who constitute a formal second line of defense assist managers acting as relationship owners.[6]

Figure 2: Third-party Risk Management Governance – Defined



Personnel performing this second line of defense function should have attributes qualifying them to perform the duties listed below depending on the nature of the third party and its relationship to the organization. Those performing second line of defense functions may do so in two capacities:

1. In partnership with the business, they may own the third-party documentation including due diligence, contracts, SLAs, insurance certificates, and anything else required by the organization. They may or may not communicate an opinion on the appropriateness or validity of the contract to management.

[6] IIA Position Paper, The Three Lines of Defense in Effective Risk Management and Control.

2. In partnership with the business or encompassed within the control function(s), they may own the contracting process in its entirety. They may review the contract, make revisions, and play an active role alongside management during the due diligence process. Staff in these control functions may or may not have veto power regarding use of management's preferred third party. In addition, they may or may not retain all third-party documentation; however, they may retain the contract and any other documentation they have reviewed.

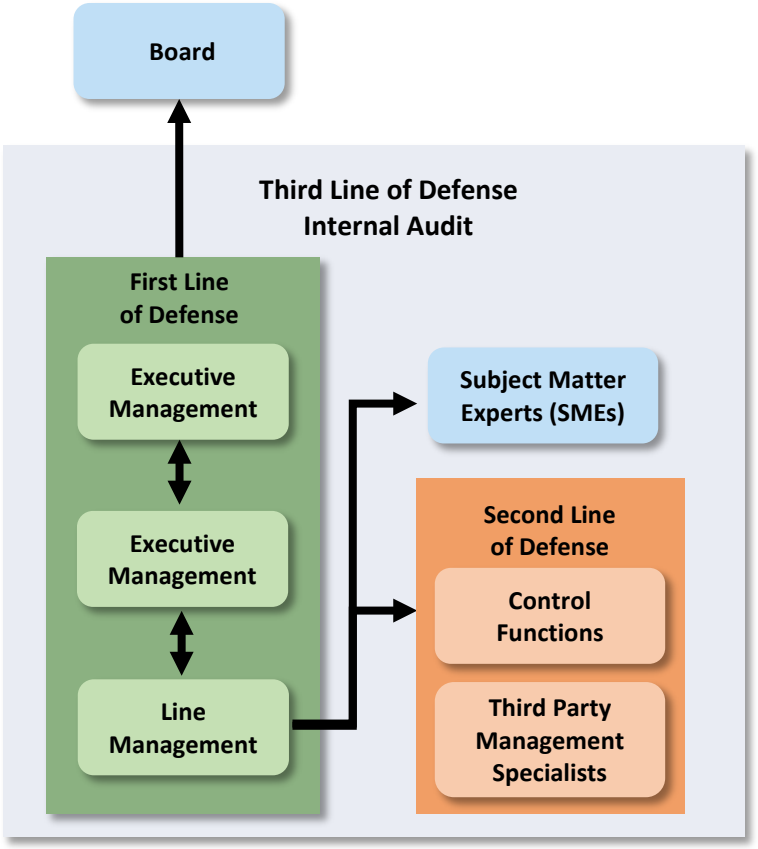
In this stage of third-party risk management development, committees or groups may be tasked with addressing third-party business cases, selection and, perhaps, contracting prior to sending the contract and/or other required information to senior management and/or the board for approval if required by the process. These committees or groups may be formed ad hoc or third-party risk management may be a recurring meeting agenda item. Consider these scenarios:

- An ad hoc committee may be formed to address a specific third-party need. For example, the organization may form a committee on engaging a third party to move and store data in the cloud. This committee might include representatives from business management, legal, procurement, risk management, compliance, cybersecurity, and IT, among others. The committee may develop the due diligence requirements for cloud vendors and ensure the organization properly executes the third-party selection process.
- Departments such as compliance, engineering, legal, accounting, cybersecurity, IT, and product managers may have a regular meeting schedule. At these meetings, they may include third parties on the agenda. Discussion topics may include third-party monitoring with product or service updates, incidents, external and internal audit results, scorecards for high-risk vendors, vendor incidents, etc.
- The organization may have a third-party oversight committee. In this case, any program changes the organization wishes to make to the third-party risk management governance or processes may require committee approval.

Consistency in documentation and due diligence may still be an issue at this stage. However, internal audit may be able to use information generated by the review processes in place under Standard 2050 – Coordination and Reliance. Internal audit may also find the structure of having a committee review third party information helpful to identify risks and controls present in individual third party relationships.

In highly regulated industries and for globally complex organizations, a standardized governance structure, as shown in Figure 3, is highly recommended. At this level, third-party specialists (potentially referred to as procurement, supply chain, vendor managers, etc.) form an important part of the first or second line of defense in third-party risk management depending on how the organization defines the lines of defense. Each third-party specialist may manage hundreds of vendor relationships and work with as many contracts. Organizations in this category may find having a centralized area responsible for doing the daily work of third-party sourcing, evaluation, and management more effective. However, as previously mentioned, managers are still the third-party risk exposure owner in the first line of defense.

Figure 3: Third-party Risk Management Governance – Standardized



In an organization with a standardized third-party risk management program, internal audit would typically assess the work of both the first and the second lines of defense. The latter may own the third-party risk management program processes and perform different types of assurance activities to ensure compliance throughout the organization. If the organization faces a significant regulatory or market change that affects their third-party risk management program or processes, the second line would be responsible for ensuring the frameworks and processes are adjusted appropriately.

Because third-party risk management is often an organizationwide activity, newly acquired information may affect the engagement objectives, scope, work program, and methods of analysis. Therefore, the information acquired during the planning phase should be well documented, promptly updated, and taken into account throughout the engagement. The information may also be useful in the CAE's long-range planning for future engagements.

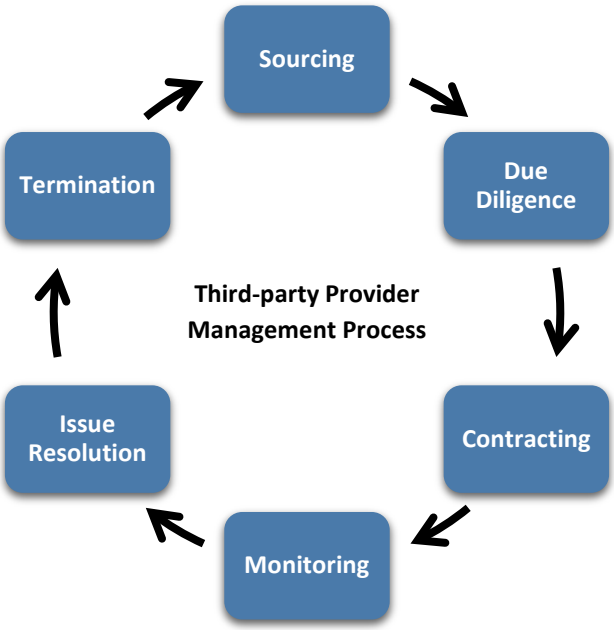
Third-party Risk Management Process

Before internal auditing can do its part to assess and audit the organization's third-party risk management processes, it should be aware of the key elements that should be present in some

form in informal and more structured programs. To be thorough, this section of the guide will assume the "Standardized" third-party risk management program structure (refer to Figure 3) to ensure a careful review of the processes involved.

To perform an internal audit engagement of third-party risk management, the internal audit activity should understand what management's processes are in the selection and monitoring of third parties. Elements of the entire process are shown in Figure 4. In general, third-party risk management policy and program procedures are intended to help achieve organizational business objectives for entering into a third-party provider relationship while satisfying regulatory requirements/expectations (if any) and minimizing the risk of unanticipated costs, legal disputes, and asset losses.

Figure 4: The Elements of Third-party Provider Management Processes



Management must, as the owners of organizational risk, identify, assess, manage, and monitor the risks associated with each third-party relationship on an ongoing basis. Their level of sophistication in terms of familiarity and/or implementation of a third-party risk management framework may be key in this undertaking. Engaging third parties may provide economies of scale, cost savings, productivity gains, or other benefits to the organization, but these relationships also reduce the organization's control over their product or service, which makes the third-party risk management process that much more important. The level of due diligence varies depending on the level of risk exposure that exists within each third-party contract.

Sourcing

Practices for sourcing third parties vary widely depending on the nature of the service or product, the complexity of the organization, and other factors. However, during the process of identifying third parties, management may begin conducting research and due diligence to narrow potential candidates to a manageable number.

Leading Practice

Implement a request for proposal (RFP) process for third-party contracts that exceed a certain monetary value or level of risk exposure.

Business Case

Before choosing to engage a third party, management should understand the business context and drivers that determine the risks associated with the effort. Some elements management should consider before deciding to issue the RFP include:

- What organizational strategies are the main drivers of the decision to pursue this arrangement?
- Is the organization pursuing cost reduction via economies of scale enabled by the third party?
- Is the organization trying to improve the effectiveness of an existing process by leveraging the service provider's expertise and investment in solutions?
- Has the organization pursued an arrangement like this one in the past? If so, what were the risks and benefits of that arrangement?
- If the objective of this third-party arrangement is to enable innovation or a higher level of service, is the organization ready to be a proof of concept or first to market?
- Is the number of service providers, or "vendor survival" rate, adequate to avoid dependence on a sole-source provider?
- Is the process too strategically important to outsource?

Engaging a third party should make business sense in the long term and create value based on reliable information and projections – risks should be understood. Management should have a process whether informal or formal to build a sound business case addressing key benefits and risks of outsourcing. The organization's governance structure should require that the sponsor and major stakeholders involved in this third-party relationship are involved and considered in the final decision. Outsourcing may be a solution to address business risks, or it may create new business risks, but risk assessments at this stage also should include implementation risks and probable impacts if the third-party relationship or the third party itself fails to deliver the anticipated results.

To gather a full understanding of the risks associated with engaging third parties, management should also consider risks that arise if a decision is made to engage a third party. Decisions should include an acceptable risk exposure level aligned with the organization's risk appetite. Alternatively, management may consider other options or variations, such as partial outsourcing, splitting the work between two or more third parties, housing the third parties on the

organization's premises, and choose the optimal solution. The decision to outsource entails a wide variety of considerations.

Management should also consider the risks associated with change management. What changes in policies, operational procedures, and infrastructure support might this arrangement generate? Is the organization ready for those changes?

Risk scoring criteria should be defined for each risk. Many organizations use a simple high (3), medium (2), and low (1) scoring system to designate the risk exposure for each risk and use a method such as averaging the scores to create a risk profile for the third-party initiative.

Due Diligence

Once management narrows the group of third-party candidates, building on any preliminary risk assessment work done while building the business case in the sourcing phase, management should identify and assess the risks posed by each party remaining under consideration. The organization must also measure the degree to which each meets the needs and criteria, and answer other critical questions required during the due diligence process before making a selection.

Leading Practice

Formalize communication between the organization and third-party candidates during the due diligence phase and incorporate it into a recurring vendor communications process.

Third-party Risk Assessment

To perform a risk assessment of potential third parties, management should contact the parties under consideration to gather basic documentation focusing on people, processes, and technology directly related to the product or service the organization is seeking.[7] Categories of information gathered for due diligence might include:

- Ownership structure and background.
- Company performance and financial health.
- Company location.
- Business model and practices.
- Potential conflicts of interest.
- References.

[7] This document will indicate management as performing the third-party risk assessment, recognizing that this activity may be undertaken by procurement personnel, supply chain personnel, sourcing personnel, or others in the organization. Management is referenced because they represent the owners of the third-party relationships and the risk exposure to which the organizations may be subject through these relationships.

- Service delivery capability, status, and effectiveness.
- Pricing and billing.
- Press coverage/legal actions.
- Corporate governance policies.
- Environmental policies.
- Ethics, code of conduct, and/or anti-corruption policies.

Leading Practice

Management should gather examples of media coverage (positive or negative), lawsuits, regulatory issues, etc., attempting to ascertain perceptions of the third party's conduct and ethical values.

It may be desirable to complement the gathering of documentation with an on-site visit, especially for significant and/or material relationships as defined by the organization. On-site reviews or visits by subject matter experts (SMEs) can provide insight by validating the information gathered, assuring the operating effectiveness of documented controls, and identifying concerns or issues not addressed by the information gathered.[8]

As a leading practice, management may choose to involve SMEs in the risk identification and assessment process. To protect the organization, specialists should evaluate potential third-party relationships considered complex or critical.

Financial services regulators may require institutions to consider third parties in terms of critical and noncritical categories that pose low, medium, or high risk to the institution. Organizations in some industries have adopted the financial services industry approach of assessing and measuring the risk posed by third parties in terms of criticality to their business because of its comprehensiveness.

About Subject Matter Experts

SMEs could include specialists in environmental, health and safety; quality; legal; cybersecurity; and compliance personnel among others.

In a manufacturing organization, an SME may be a quality engineer consulted to ensure the quality of raw materials or components. The engineer may work with suppliers to agree on quality standards and inspection processes to monitor incoming material.

The criticality and/or risk level of a third party should determine the frequency and intensity of ongoing monitoring as well as periodic reviews. High risk/complexity third parties should be reassessed in relatively frequent intervals (e.g., annually) with reviews of lower criticality/lower risk third parties performed less frequently. The result of this approach is a process of continuous monitoring that can provide a timelier analysis of the organization's third-party risk profile. Figure 5 offers criticality and risk level descriptions from the financial services industry that may be suitable for adaptation.

[8] SMEs may exist in the first or second line of defense. SMEs may be part of the first line as a product expert, an IT security expert, or someone directly employed in the business line. They may also be part of the second line as a member of a control function such as a compliance expert, safety expert, attorney, etc.

Figure 5: Financial Services Industry Descriptions of Criticality and Risk Level

Criticality refers to the dependency of the institution as a whole, not a single department, on the third party.

Critical means there is not a ready substitute in the marketplace, or the service provided is customized to the point a change in third parties is not feasible. The loss of the third party would provide a substantial risk to financials, services, or operations of the institution. Workflow would be disrupted. Errors may be visible to account holders. The third party has access to members' personally identifiable information (PII), account records, and other key data.

Noncritical means substitutes exist in the marketplace and could readily replace the existing third party. The loss of the third party would be inconvenient but not damaging in the long term. The third party has limited or no access to members' personally identifiable information (PII), account records, and other key data.

Risk Level refers to the risk exposure created should something go wrong with the third party.

High Risk means the institution could be exposed to significant financial and/or account holder losses. Key services will be impacted. Issues may have extended timelines to resolve and/or may result in errors visible to account holders. Event may result in extensive regulatory fines, penalties, lawsuits, and reputational damage.

Medium Risk means the institution could be exposed to moderate financial and/or account holder losses. Account holders may notice and comment on issues and/or issues may have extended timelines to resolve. Event may result in regulatory fines and penalties with minor impact on earnings, lawsuits, and reputation.

Low Risk means the institution could be exposed to some financial and/or account holder losses. Event has low account holder visibility, little impact to technology and services affecting account holders, and/or issues may have short timelines to resolve. Event would not result in regulatory fines, penalties, or lawsuits.

This type of risk scoring criteria will result in a matrix:

Tier	Criticality	High Risk	Medium Risk	Low Risk
1	Critical	X		
2	Critical		X	
3	Noncritical		X	
4	Noncritical			X

The level of due diligence for each tier should be predetermined and documented in third-party risk management policy and procedures. The documentation requirements for due diligence should include not only the documents gathered during the process, but also the results of the due diligence analysis and the decisions made as a result.

Review/escalation protocols and red flags should be described in third-party risk management policy and procedure documents, and the board should ensure management is held to those standards because they are a key component in managing risk exposures consistently with the organization's risk appetite.

For example, if management performs a risk assessment and decides to use a third party that poses a high risk to the organization when lower-risk third parties were available, that decision should be justified and approved by senior management and/or the board. Both the justification and approval should be documented and retained in the third-party file and updated on a regular basis. This may be useful if the third party's operations or the relationship later becomes unfavorable to the organization. (See Appendix D. Considerations for Small Internal Audit Departments and Appendix H. Sample Third-party Risks and Red Flags/Warning Signs.)

Contracting

The contract is an important control in the third-party risk management process because it is the organization's best resource to communicate its risk appetite and minimum standards of internal control to the third party and clearly state expected standards regarding the service, product, component, etc.

Many decisions must be made when negotiating a third party contract. Some questions management should consider prior to and during negotiations include:

- Should the organization use its standard contract or the third party's standard contract?
- Should legal review the contract? If so, are legal resources present in house or must the review be outsourced? If outsourced, what protections exist to ensure the contract is reviewed with a focus on the organization's business, rather than focusing on standard contract terms or the third party's interest?
- Should the contract include clauses that may be controversial, such as data breach disclosure requirements, penalties, termination conditions, dispute resolution, customer complaint handling, and right to audit? If not, do the omissions materially increase the risk exposure?
- Should SLAs be included in the contract? What constitutes an SLA acceptable to this organization in terms of this third-party service or product?
- Should the contract be translated into a language better understood by the third party's personnel?

If the third party's product or service cannot be easily replaced or if it is a sole-source provider, a high risk is presented to the organization (e.g., failure by the third party could result in significant

damage to the organization). The contract should provide for a mutually beneficial relationship and protect the organization if there are disputes, complaints, or failures. For example, an organization may enter into sales and purchase agreements to reduce their dependence on a small number of third parties.

Typically, organizations review new contracts from a legal standpoint, which may be in house or outsourced. In large organizations, management may be required to complete an evaluation process with the procurement team to obtain a requisition. In these cases, a procurement team may assume management of the contracting process.

One significant risk faced by organizations in contract negotiations is a failure to evaluate "soft controls," such as cultural norms and expectations on both sides. Contract negotiators should be aware that global rules and expectations vary. Contract negotiators and management should be aware of the unwritten rules that govern the society in which the third party is operating. (See Appendix B. Evaluating a Third Party's Conduct and Ethical Values.)

The Potential Result of Inadequate Contract Review and Negotiation

An organization is engaging a third party that will have access to personally identifiable information of its customers. If a contract bypasses review of data security expertise personnel, the organization may encounter significant risk exposure if the third party suffers a data breach.

Proper contract review would require SMEs to consider what may occur if the contract excluded clauses and issues of responsibility regarding disclosures of data breaches, restricted access to servers, firewall requirements, etc.

The organization could suffer significant damage and may be unable to recoup losses from the third party if such specialized issues were omitted from the contract and/or the associated SLAs.

Some organizations require third parties to agree to abide by the organization's code of conduct. Others may give the third party's employees access to report issues to the organization's ethics hotline. However the organization chooses to manage these issues, an important control in the third-party risk management process considers "hard to define" areas of ethics and values.

Another contracting risk is inadequate review. This may include organizations having contracts reviewed only by legal or procurement personnel who may not possess necessary detailed knowledge of the third party and its product or service. This can leave the organization exposed to risks that cannot be remedied due to unfavorable contract terms after one has been finalized by both parties.

Organizations should not allow the manager requesting the product or service to negotiate the relevant contracts. Management should evaluate the product or service, gaining insight from SMEs on SLAs and other technical content, leaving the purchasing team and/or legal team to negotiate and settle the contract terms. The procurement function should also review SLAs for completeness

and validate the pricing is competitive, etc. In small organizations, an independent manager may be appointed to negotiate a contract and take it through legal review.

The size of the organization is irrelevant when it is presented with a third party's standard contract for acceptance. Organizations large and small may request revisions, additions, or deletions to a contract according to their needs. A leading practice for organizations is to maintain their own standard contract containing those provisions deemed necessary or desirable but that may be customized to accommodate requirements from the third party.

Audit Consideration

Conflicts of interest or other ethical issues may arise (in fact or appearance) if the organization's representative who requested the product or service is also the person selecting the vendor and negotiating the contract.

If significant concessions are made to the organization's standard terms and conditions, depending on their magnitude, senior management and/or board review and approval prior to finalization should be required.

As the end user of the service or goods, the relationship owner should provide technical input into the contracting process and review the contract before finalizing it with the third party. Some companies use standard sections in the contract, excluding the scope of work section that may best be developed by the relationship owner. However, this section may be omitted from an otherwise comprehensive SME review, presumably because it is written and reviewed by the requesting department. This is a potential risk. (See Appendix D. Considerations for Small Internal Audit Departments and Appendix E. Contract Review Considerations.)

Monitoring

In general, even in organizations with basic and defined third-party risk management governance structures, personnel with knowledge of the product or service being provided should be appointed to manage the overall third-party relationship. Managing third parties may be decentralized in smaller organizations in which each business manager owns the third-party relationships in their area(s), or it may be centralized in a function, position, or governance body such as procurement, the chief operating officer, or senior management team respectively.

A key responsibility of third-party relationship owners is to monitor the third party to ensure compliance with the finalized contract and the requirements for the product or service within the SLA parameters. Key performance indicators (KPIs) may be a mix of both standard KPIs relevant to all third parties and customized KPIs related to the product or service provided. The internal audit function must be aware of the organization's agreed-upon monitoring KPIs so it may design audits appropriately.

In addition to monitoring relevant KPIs, third-party relationship owners should:

- Complete or update periodic analyses of risks and exposures for each assigned third party and their products or services.
- Obtain the third party's required attestation, audits, and financial reports (if applicable).
- Ensure reports are reviewed by relevant SMEs.
- Obtain and review relevant third-party policies, compliance programs, and data security programs to ensure they are operating within contracted/required parameters.
- Obtain and review reports specified in the contract of the third party's activities on behalf of the organization.
- Conduct any on-site monitoring visits as agreed in the contract, which may include unannounced visits where necessary.

For critical third parties with International Standards for Assurance Engagements (ISAE) No. 3402, Assurance Reports on Controls at a Service Organization (and related reports) available to the organization, these reports should be gathered annually and reviewed by the third-party relationship owner and relevant SMEs as needed.

These reports come in two forms: for both the international and United States reports, Type 1 reports include basic information of the service organization's description of controls and the independent service auditor's opinion of suitability of control design. There is no opinion provided with a Type 1 report that the controls as designed are effective or performed consistently; just that the service controls are in place and appear suitably designed to achieve their control objectives.

Type 2 reports contain the information found in Type 1 reports plus results of the independent auditor's testing of the controls and additional information provided by the service organization.

SLAs

During the negotiation phase, both parties' understanding of SLAs should be clear and unambiguous. If there is confusion or misunderstanding on either side's part, the organization may wrongly exercise the right-to-audit clause (or may claim default) or the third party may fail to meet the agreed-upon requirements.

The Potential Consequences of Inadequate SLAs

An organization has signed a long-term contract with a third party, but the contract's SLAs covering product quality are vague or unrealistic, resulting in the organization and the third party disagreeing on the product's quality.

In this situation, protracted disputes between the parties could have multiple negative repercussions: interruption of the organization's business, continued production of subpar products or services, even litigation if the parties are unable to settle and rectify the issue.

Well-designed SLAs at the outset are crucial to avoid unnecessary business interruptions, including expensive litigation that carries the risk of unpredictable outcomes.

Both scenarios impair the organization's ability to fulfill its mission, so care should be taken to avoid the possibility. If the contract includes penalties (financial or otherwise), the third party may meet that obligation if called upon to do so, yet continue in the same unsatisfactory manner.

Contract negotiators should seek the expertise of SMEs and other knowledgeable resources to ensure SLAs are reasonable, specific, and measurable with appropriate, responsive action. Penalty clauses in the contract must effectively deter the third party from attempting to subvert the spirit of the agreements.

Issue Resolution

Usually, it is the responsibility of the third-party relationship owner to monitor and address issues. In a standardized third-party risk management structure, procurement managers with full-time responsibilities may be managing critical third-party providers. As reviewed in the Monitoring section, relationship owners should be conducting periodic risk assessments of third parties on a schedule commensurate with the risk exposure levels presented by the third party. Further, they should be monitoring third parties for changes in their business, organizational structure, legal actions, regulatory issues, etc. (See Appendix C. Due Diligence Considerations.)

Termination

In contract negotiations, termination conditions are necessary to protect the organization. Numerous risk factors can contribute to the amount of loss or damage the organization may sustain from early termination. Further, certain risk factors can contribute to the amount of loss or damage the organization may sustain if the contract is not renewed. Risks that may be managed through appropriate and complete termination conditions include:

- Data, equipment, materials, or technology retrieval.
- Evidence of material, technology, or data destruction.
- Circumstances requiring arbitration.
- Events that may lead to litigation.
- Responsibilities for separation and termination costs.
- Alternatives in the event the third party becomes unavailable.

Audit Consideration

Internal auditors should be wary of contracts that auto-renew. The timing of auto-renew and termination notice periods may conflict or not match. For example, auto-renew notification dates are often substantially earlier than termination notice periods.

A missed auto-renew date for a third party the organization wishes to terminate may result in large financial or other penalties and possibly a requirement to pay total contract fees up front before the organization is released from the agreement.

When approaching the end of a contract or other conditions that may necessitate termination, the third-party relationship owner should determine future contracting needs based on current business needs and past experience with the third party. If an activity or service is to continue beyond the end of the contract, the owner must establish a transition plan with the third party. The transition plan, at a minimum, should include an update of the due diligence and risk assessment elements of the third-party risk management process as well as a contract review to update and correct any issues.

The Role of Internal Audit in Auditing Third-party Risk Management

Sourcing

To assess the effectiveness of an organization's third-party risk management processes, internal auditors should start at the beginning. Obtaining the business case and any other relevant strategy-related documents concerning the initiative to engage a third party provides valuable information that will be useful throughout the internal audit engagement.

When evaluating management's business case, internal auditors should verify these elements:

- Reliability of the information used in the business case.
- Whether governance and approval processes were executed according to the organization's third-party risk management policies and procedures.
- Whether estimates of the third party's failure to meet expectations and resulting impact are included in the business case.
- The sensitivity of cost-benefit analysis to assumptions.
- Any KPIs or other data included in the business case that should be included in the monitoring process.

Due Diligence

Third-party due diligence reviews are not only critical when engaging a new third party but also to routinely check and ensure the third party has been vetted for any changes from previous reviews. The goal is to validate that the third party continues to meet the standards necessary to provide their service or product without causing unacceptable organizational risk.

Based on the risk assessed in the internal audit activity's engagement planning process, internal auditors may evaluate the status and accuracy of a third-party relationship owner's risk assessment of providers under their control. Gather and review supporting documentation management used to resolve risk concerns and/or issues that may have arisen with the third party.

An organization may believe if they obtain copies of an ISAE 3402 report from a third party, there is less cause to gather additional due diligence information. However, considerations to discuss before making that decision include:

- The level of assurance provided by the Type 1 or Type 2 report.
- A third party's past performance.
- The level of competency of the independent service auditors.
- Any conflicts of interest the independent service auditors may have.
- The effect of the performance or nonperformance of compensating controls at the organization versus the third party's control system as described and tested in the reports.

In general, there is more due diligence information to gather outside of applicable ISAE 3402 reports.

Audit Consideration

Anticipate ways in which managers may try to circumvent third party due diligence requirements.

Controls such as accounts payable requiring third parties be listed in a vendor master file before sending payment is a good practice. If a third party does not appear on this list but an invoice exists, internal auditors should examine who is notified and who is responsible for investigating how a contract for payment was agreed to outside the standard due diligence process. Internal audit should address how these issues are escalated and resolved (e.g., escalation and approval protocols).

Internal audit can add value to the organization by ensuring proper due diligence and risk assessments have been conducted not only at the beginning of a relationship with a third party but also on a regular basis commensurate with the third party's risk exposure level.

Contracting

When evaluating the organization's contracting process, tie findings back to the stated risk appetite. The organization must be clear with third parties regarding the conditions it deems important and what it will and will not accept regarding minimum standards of internal control. What the organization agrees to in its contracts as opposed to its risk appetite is a key piece of information internal auditors can use to illustrate their findings and recommendations.

Right to Audit/Access to Data

An organization's standard contract should include a robust right-to-audit clause. If a significant vendor proposes changes to this content within the contract, management should consult the internal audit activity and/or any other auditor it relies on to perform third-party audits, prior to acceptance if feasible. Management and internal audit may choose to waive their right to audit; however, it is a leading practice to have such language included in the contract in the event of an

occurrence suggesting an audit may be in order. The right-to-audit clause should be clear on who is able to exercise that right and to what extent.

For example, contracts often include separate audit rights for the organization's cybersecurity function, but this should not limit management or other entities' right to audit. A third party's standard contract may attempt to limit the right to audit to one audit annually, but the organization should ensure the right of its internal audit activity to perform its duties is clearly articulated in the contract without limits and outside of any other discipline that may require audit access.

Enforcing the right-to-audit clause in contracts can be challenging. Even if third parties allow the clause in the contract, they may employ tactics making it difficult for the organization to exercise their contractual right. Third parties attempt to have the organization pay for data and/or for the time its personnel must spend working with the organization's auditors. Some third parties may attempt to deny the organization's internal auditors on-site access, insisting that the relationship owner perform audits instead. Management's responsibility is to protect the organization, and a comprehensive contract with clear rights to audit and access to data to accomplish this is in the best interest of the organization. (See Appendix F. Right to Audit Clause Illustration.)

Right to Audit Clauses

The internal audit activity should actively advocate for the right to audit as well as being granted unfettered access to the necessary data and information from third parties when conducting audit activities.

Third parties may attempt to protect against internal auditors or other organizational personnel from having back-end access to their systems (e.g., direct database connectivity), but management can request provisions during the negotiation process that will make exercising the right-to-audit clause easier.

For example, if the organization is considering an outsourced model, management must work with internal audit and other relevant stakeholders (e.g., finance, legal) to determine what level of visibility the organization should have to the information or processes that will be sent to, transferred to, or generated by the third party:

- Transfer data required for the organization's use in-house to a data warehouse.
- Require the third party to create an audit or "read only" ID on their systems.
- Document the process by which the third party will gather the required data into a format easily accessed by the organization's management, external auditors, or by the internal audit activity.

Monitoring

Performing internal audit engagements that aim to assess the effectiveness of an organization's third-party monitoring processes can be difficult to scope. If the organization engages with third parties that outsource parts of their services (e.g., fourth parties), the question arises: How far down the supply chain should other parties be considered? Should subservice or "fourth party" providers be monitored? If so, to what extent? Typically, organizations choose from these two approaches:

1. Monitor fourth parties according to the risk exposure presented by the third-party relationship. High-risk third parties that outsource would have to provide more information and access to their fourth parties than those presenting lower risk exposures.
2. Choose to rely on the contract to ensure the third parties adequately manage their own third-party relationships.

In the first case, internal auditors would want to examine fourth party information and ensure it was integrated into management's due diligence process. In the second case, internal auditors would need to carefully evaluate the contract itself and the contracting process to ensure management conducted proper reviews. (See Appendix I. Audit Considerations for Fourth Parties.)

One leading practice that may assist internal auditors in designing their work programs involves using a third-party relationship tracking system. This can be as simple as an Excel spreadsheet or as complex as custom-coded software. Relationship owners may document third-party due diligence, contracts, SLAs, and other information in the tracking system. The most functional and beneficial tracking systems aggregate risks by third party, product, relationship owner, department/function, and more.

Prioritizing Third Parties for Tracking Purposes

Organizations may track all third parties or a subset of third parties. It may be useful for an organization (especially smaller organizations) to use its risk assessment results to organize the third parties by risk level tiers.

If an organization does not track its third party relationships, there is a risk that a lack of communication may occur. This situation is especially problematic if the organization has multiple contracts with a third party and issues arise, that may have subsequent effects for other departments within the organization. Departments or business lines using the same third party for different products or services should share information gathered during the regular third-party monitoring process with each other. Each department or business line should conduct its own monitoring pertaining to its needs, but should inform relevant internal parties of issues that may arise. Once again, obtaining this information will benefit internal audit during an engagement.

Issue Resolution

Examine the organization's escalation process for elevating concerns regarding third-party risk exposure levels, nonperformance, lack of quality, as well as other issues that may arise. Determine whether the organization is collecting any penalties that may be due from a third party as set forth in the contract. Additionally, confirm that management is addressing potential contract breaches appropriately by increasing or changing SLAs, monitoring processes, etc.

One risk organizations may struggle with in terms of third-party risk management is obtaining customer complaint information from the third party. Often, what constitutes a customer complaint is not well-documented in a contract, giving the third party flexibility in interpreting consumer correspondence. If an organization prefers to monitor or resolve customer complaints in-house, internal auditors should confirm management receives a complete list of all customer data that could constitute a complaint on a timely basis.

Working Directly with Third Parties

In general, internal audit does not work directly with third parties engaged by the organization unless the activity is performing an internal audit engagement.

However, management may call upon internal auditors to work directly with third parties to resolve issues. Internal auditors should know the organization's practices for resolving vendor issues that concern internal audit and any laws or regulations of the location governing that interaction before embarking on the assignment.

Termination

In normal circumstances, internal audit would not be involved in the termination of third party relationships. However, on an exception basis, it is possible that internal audit may get involved in an advisory capacity, subject to Standard 1210 – Proficiency and 1210.C1 in the interpretation, or may validate that appropriate conditions (such as retrieval or destruction of data) are satisfied. At a minimum, internal audit should confirm thorough descriptions of termination conditions in each contract as part of routine audit procedures.

Performing the Engagement

Gather Information to Understand the Area or Process Under Review

While developing the individual engagement plan, internal auditors gather information through procedures such as reviewing prior assessments (e.g., risk assessments, reports by assurance, and consulting service providers), understanding and mapping of process flows and controls, and interviewing relevant stakeholders. To identify key risks and controls for the third-party risk management process, internal auditors should have a thorough understanding of the way their organization approaches third-party risk management. Understand these elements of third-party risk management during the planning process:

- Third parties engaged by the organization.
- Sophistication of the organization and its third party risk management framework, if there is one; if not, work with management to implement one.
- Level of documentation available for third-party risk management roles, responsibilities, and activities across the organization.
- Board reporting related to third-party risks and incidents.
- Past issues encountered with third parties in terms of contracts, performance, quality, etc.
- Any regulatory requirements/expectations relevant to the organization and the jurisdictions within which it operates.

Typical Engagement Planning Steps

- Gather information to understand the area or process under review.
- Conduct a preliminary risk assessment of the area or process under review.
- Form engagement objectives.
- Establish engagement scope.
- Allocate resources.
- Document the plan.
- Report the engagement results.

For detailed instructions on how to plan and scope an audit engagement, see IIA Practice Guide "Engagement Planning: Establishing Objectives and Scope."

Conduct a Preliminary Risk Assessment of the Area or Process Under Review

Because any single internal audit engagement cannot cover every risk, internal auditors assess the significance of the risks identified by management, during previous internal audit engagements, and audits or assessments of other internal or external entities or consultants as described in Standard 2050 – Coordination and Reliance.

Standard 2210 – Engagement Objectives states that objectives must be established for each engagement, and Standard 2210.A1 requires a preliminary assessment of the risks relevant to the activity under review. Internal auditors may interview relationship owners, business managers,

procurement managers, legal personnel, and other relevant personnel who have technical knowledge that can assist in identifying risks to the third-party risk management process.

To be clear, the internal audit activity is responsible for assessing the quality of management's third-party risk management framework and process to determine whether it is adequate in design and/or operation. Management's third-party risk management process should account for not only the financial, operational, and regulatory impact of third party risks, but also nonfinancial impacts, such as damage to the organization's reputation or relationships with customers. Even a small, contained information breach can have a damaging impact on an organization's reputation depending on the nature of the breach. Some risks may appear insignificant on their own but should be considered in the context of the organization's overall third-party risk management framework and process.

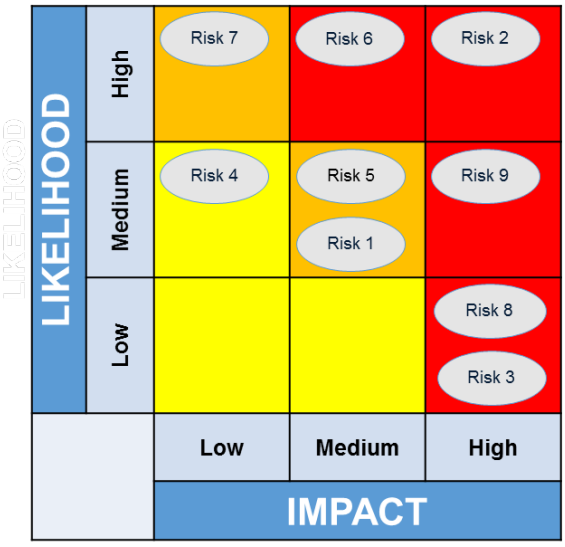
Internal audit activities vary in how they assess risk for their engagements. One effective way to perform and document an engagement-level risk assessment for a third-party engagement is to leverage any risk assessments management has done for third parties within a reasonable time frame. Collect the documents listed in the Due Diligence section of this guide and review them along with management's risk assessment documentation to ensure the risks as viewed by internal audit and management are (reasonably) the same.

Consider using a risk matrix listing the relevant inherent risks (e.g., risks that could exist if internal controls are not applied), expanding the matrix to include measurement of the risk exposure when including the effectiveness of relevant controls. A risk matrix may be created using a spreadsheet or similar document, with or without a software program. The format of the matrix may vary but typically includes a row for each risk and a column for each risk measure, such as impact and likelihood. Once the internal audit activity has assessed the level of risk exposure presented to the organization by its third-party risk management framework and process, the engagement risk matrix will result in a basic graph, such as the heat map shown in Figure 6.

If using heat maps and/or risk and control matrices in an assessment, include them in the engagement workpapers within the preliminary risk assessment, supporting the internal audit activity's decisions about risk significance and in conformance with Standard 2330 – Documenting Information.

Implementation Guide 2210 – Engagement Objectives also states, "During engagement planning, it is helpful for internal auditors to develop a planning memo, where they can document the objectives, scope, risk assessment, and prioritized areas for testing." The IIA Practice Guide "Engagement Planning: Establishing

Figure 6: Heat Map



Objectives and Scope" provides detailed information about building upon the risk assessment to develop the engagement objectives and scope. In addition, heat maps and risk and control matrices will lend support to the engagement results and conclusions.

Form Engagement Objectives

In accordance with Standard 2210 – Engagement Objectives, the overall objective of a third-party risk management audit typically is to provide independent assurance over the governance, policies, processes, and key controls that support the implementation, execution, and oversight of an organization's third-party risk management framework and process.

Objectives of Assurance Engagements

- Reflect risks to the business objectives of the area or process that were assessed as significant during the preliminary risk assessment (2210.A1).
- Consider the probability of significant errors, fraud, noncompliance, and other exposures (2210.A2).
- Identify appropriate evaluation criteria (2210.A3).

In a risk-based audit plan, the internal audit activity should aim (within a reasonable period of time) to perform engagements covering the organization's third-party risk management framework and associated processes along with specific third-party risks for functions and departments as needed. The internal audit activity also may perform engagements related to the third-party risk management processes in terms of individual elements, specific vendors, etc. Coverage of third-party risk management topics can be provided in one end-to-end audit or multiple audits, depending on how the organization has defined the coverage approach.

Internal auditors may approach an audit engagement covering third-party risk management in several ways including:

1. Audit the third-party risk management framework.
2. Audit the third-party risk management processes.
3. Audit a component of the third-party risk process.
4. Include third-party risk management in a process, product, or unit audit.

Depending on the approach taken, the objectives of the audit engagement will differ widely, but in general, the process of forming engagement objectives for a third-party risk management-focused internal audit should relate to the organization's current business objectives and strategies. Standard 2210.A3 offers three elements for use in constructing the evaluation criteria for engagements.

- Internal (e.g., policies and procedures of the organization).
- External (e.g., laws and regulations imposed by statutory bodies).
- Leading practices (e.g., industry and professional guidance).

These criteria are needed to determine whether third-party risk management related objectives and goals as determined by management and/or the board have been accomplished. Standard 2210.A3 points out: "Internal auditors must ascertain the extent to which management and/or the board has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, internal auditors must use such criteria in their evaluation."

Establish Engagement Scope

The chief audit executive (CAE), or internal auditors assigned by the CAE, should be involved in various meetings throughout the organization regarding third party risk management, which can help determine the internal audit activity's approach to the engagement scope, in conformance with Standard 2220 – Engagement Scope.[9]

Further, internal audit personnel may participate within third-party risk management committees for awareness of key vendor risks and issues, as well as knowledge of when new key vendors are engaged or terminated. This knowledge serves as a key input into internal audit's overall risk assessment process, which helps inform the annual audit plan. In some cases, internal audit may map vendors to business areas or auditable entities to assist in their risk assessment and audit coverage approach.

Audit Consideration

Consider including affiliate relationships or "internal third parties" within the organization's overall third-party risk management framework and process.

Certain affiliate relationships require interaction be at "arm's length," and may be enhanced by leveraging work performed by existing assurance providers.

Potential Scope Limitations

There are situations in which the third party manages data for many customers and cannot be persuaded to devise a method of extracting the data necessary for the contracting organization to exercise its right to audit without exposing the data of another customer. In this case, note the situation as a scope limitation. Implementation Guide 2220 – Engagement Scope states "Internal auditors generally consider and document any scope limitations, as well as any requests from the client or stakeholders for items to be included or excluded from the scope. If internal auditors encounter scope limitations, these must be reported in the final engagement communication."

[9] The *International Professional Practices Framework, 2017 Edition* glossary defines chief audit executive as "the role of a person in a senior position responsible for effectively managing the internal audit activity in accordance with the internal audit charter and the mandatory elements of the International Professional Practices Framework. The chief audit executive or others reporting to the chief audit executive will have appropriate professional certifications and qualifications. The specific job title and/or responsibilities of the chief audit executive may vary across organizations."

At a minimum, the scope of any internal audit engagement regarding third-party risk management should include confirming whether processes related to it reflect the principles in the third-party risk management framework, if the organization uses one.

Allocate Resources

To accurately and completely examine the third-party risk management framework and/or process, internal auditors should ensure they are independent and that the appropriate technical skill sets are employed. In conformance with Standard 2230 – Engagement Resource Allocation, the CAE should assess the skills of internal audit team members periodically to ensure that the internal audit activity has the appropriate skills to evaluate the third-party risk management process of the organization.

Auditing third-party risk management requires different skill sets from auditing traditional areas (e.g., financial statements). The CAE should be aware of this and engage experts where necessary. For example, an internal audit activity may collaborate with the cybersecurity team when performing procedures relevant to a third party that handles information sensitive to the organization including personally identifiable information for customers.

As noted in Standard 2050 – Coordination and Reliance, the CAE should carefully consider the competency, objectivity, and due professional care of any other assurance providers upon which the internal activity intends to rely. The CAE should clearly understand the scope, objectives, and results of their work, because the CAE retains the responsibility for ensuring adequate support exists for the conclusions and opinions reached by the internal audit activity. Standard 2050 is reinforced by Principle 4 – Competency in The IIA's Code of Ethics, which reads, "Internal auditors apply the knowledge, skills, and experience needed in the performance of internal audit services."

Audit Considerations

Some internal audit documentation and evaluation criteria may be covered by existing assurance providers. Examples include SOC reporting (reliance on external audit firms), third party regulator examinations, ISO certifications, etc. Internal audit should consider the reliability and relevance of this information if it is available.

In some industries, such as energy, many internal audit activities do not directly audit plants, drilling platforms, and other facilities. The environmental, health, and safety (EHS) organization may perform their own audits on which internal audit may rely.

Internal audit would still be responsible for reviewing the controls implemented within the EHS organization.

Document the Plan

During planning, internal auditors document information in engagement workpapers. This information becomes part of the engagement work program established to achieve the engagement objectives, as required by Standard 2240 – Engagement Work Program.

The process of establishing the engagement objectives and scope may produce any or all of the following workpapers:

- Process maps.
- Summary of interviews.
- Preliminary risk assessment (e.g., risk and control matrix and heat map).
- Rationale for decisions regarding which risks and which components of the organization's third party risk management framework and/or process to include in the engagement.

Testing and Evaluating Third-party Risk Management

Standards 2300 – Performing the Engagement and Standard 2320 – Analysis and Evaluation govern this element of an engagement. By whatever method the organization chooses to manage third-party risk, internal audit's responsibility is to assess the effectiveness of the third-party risk management framework and process. Essential criteria for evaluating the organization's third-party risk management framework and process would include comprehensiveness, relevancy, and testing "assumptions."

Differences in the Public Sector

In the public sector, third parties may not have an internal audit function. In this case, the internal audit activity should carefully consider when forming their recommendations whether management is or should be doing on-site visits and/or executing more rigorous due diligence and monitoring for those third parties.

Internal audit may also encounter this situation in other company structures (e.g., in Germany there are family-owned companies without internal audit departments).

Many internal audit activities have standard audit programs tailored to their geographical location, product, customers, services provided, and more. An important element for internal audit to consider when testing and evaluating third-party risk management is testing management's assumptions regarding each third party and the products/services it provides. The intent is to assure that the rationales for those assumptions are clearly defined (documented), that the assumptions are reasonable, and that the framework and process include arrangements to periodically reevaluate those assumptions.

On-site Audits

If not mandated by regulation, internal auditors may choose to do on-site reviews of third parties that meet one or more of the following criteria:

- Posing more compliance risk.
- Posing significant reputation risks (e.g., system vendors that would affect customers if they could not recover or ceased operations).
- Presenting issues identified in documentation reviews or by negative external news (e.g., bankruptcy).
- Anything posing a high risk.

Management must maintain appropriate oversight of the third party, inclusive of on-site reviews if deemed appropriate, given the risk exposure, criticality, and scope of services. Internal audit must not become the control for management for on-site reviews conducted at third-party locations. (See Appendix G. Testing and Evaluating Third-party Risk Management.)

Report the Engagement Results

Upon completion of thorough testing, analysis, and evaluation, internal auditors will have documented "sufficient, reliable, relevant, and useful information to support the engagement results and conclusions," in conformance with Standard 2330 – Documenting Information.

Guidance on the Audit Report

For more information, please see IIA Practice Guide, "Audit Reports: Communicating Assurance Engagement Results."

Internal auditors should follow standard reporting procedures for all third party risk management engagements as per Standard 2400 – Communicating Results. However, following Standard 2440 – Disseminating Results, management will receive a written report and the board should receive a copy. If no significant issues arose during an engagement and a satisfactory rating was determined, providing a summary report to the board or its delegates is typically acceptable.

Internal auditors should note that to conform to Standard 2410 – Criteria for Communicating and 2410.A1, the final communication of engagement results must include the engagement's objectives, scope, results, applicable conclusions, recommendations, and/or action plans. Further, according to The IIA's Code of Ethics, Principle 2 – Objectivity requires that "Internal auditors make a balanced assessment of all the relevant circumstances and are not unduly influenced by their own interests or by others in forming judgments." As a result, internal audit engagement reports should be thorough, balanced and of value to management in terms of managing the risks and controls relevant to the engagement.

Appendix A. Related IIA Standards and Guidance

The following IIA resources were referenced throughout this practice guide. For more information about applying the *International Standards for the Professional Practice of Internal Auditing*, please refer to The IIA's Implementation Guides.

Related IIA Standards
Standard 1210 – Proficiency
Standard 2050 – Coordination and Reliance
Standard 2200 – Engagement Planning
Standard 2201 – Planning Considerations
Standard 2210 – Engagement Objectives
Standard 2220 – Engagement Scope
Standard 2230 – Engagement Resource Allocation
Standard 2240 – Engagement Work Program
Standard 2300 – Performing the Engagement
Standard 2320 – Analysis and Evaluation
Standard 2330 – Documenting Information
Standard 2400 – Communicating Results
Standard 2410 – Criteria for Communicating
Standard 2440 – Disseminating Results

Related IIA Guidance
Practice Guide "Audit Reports: Communicating Assurance Engagement Results," 2016.
Practice Guide "Engagement Planning: Establishing Objectives and Scope," 2017.

Other Resources
IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control, 2013.

Appendix B. Evaluating a Third Party's Conduct and Ethical Values

Forming a view of a third party's inner workings regarding conduct and ethical values can be difficult given that the organization is not privy to the confidential information and opinions necessary to understand the third party's culture. This appendix offers one approach that management can apply as part of its third-party risk management framework, which is an evaluation using the Ten Principles of the United Nations (UN) Global Compact, representing fundamental responsibilities for organizations in the areas of human rights, labor, environment, and anti-corruption.

A Third-party Evaluation Using the 10 Principles of the UN Global Compact

Hypothetical example: ABC Consulting Company providing model validation services in the US, UK, and Australia

Principle	Contributing factors	Mitigating factors	Risk level
1. Businesses should support and respect the protection of internationally proclaimed human rights.	Vendor's website contains a statement supporting the UN Global Compact.	Vendor's offices are located in the U.S., U.K., and Australia, which all have a system of law and order that aim to protect human rights.	1
2. Businesses should make sure that they are not complicit in human rights abuses.	Consultants are deployed all over the world potentially in countries that restrict human rights.	Vendor has never been cited for human rights abuses. Vendor has a code of conduct and ethics program that aim to prevent them from deploying consultants to countries with known human rights issues. Staffing is regularly reviewed by managing partners.	1
3. Businesses should uphold the freedom of association and the effective recognition of the right to collective bargaining.	Vendor is not unionized and no record of their views on collective bargaining are known.	Vendor is located in countries with strict labor laws that aim to protect the worker, guarantee medical leave and vacation, and have a minimum wage.	1
4. Businesses should uphold the elimination of all forms of forced and compulsory labour.	N/A	Vendor performs a lucrative service and operates mostly in the U.S., U.K., and Australia where slavery is prohibited by law.	1

A Third-party Evaluation Using the 10 Principles of the UN Global Compact (continued)			
Principle	**Contributing factors**	**Mitigating factors**	**Risk level**
5. Businesses should uphold the effective abolition of child labour.	Vendor has made no statements concerning their views on child labor.	Vendor is located in countries with strict labor laws that aim to protect the worker, guarantee medical leave and vacation, and have a minimum wage. Vendor is located in countries where child labor is prohibited by law.	1
6. Businesses should uphold the elimination of discrimination in respect of employment and occupation.	Publicly available reports indicate that the vendor's workforce is predominantly male. Females comprise approximately 30% of the consultants employed at the vendor.	Vendor is located in countries with government agencies that aim to monitor and prosecute violations of employment discrimination laws.	1
7. Businesses should support a precautionary approach to environmental challenges.	Vendor's workforce travels a great deal (e.g., 5 days per week), which creates a large carbon footprint per consultant. Vendor is located in countries without strict environmental protection laws regarding recycling, efficient cars, and other protections.	Vendor has provided their statement of sustainability that outlines their commitment to paperless working, limiting long distance travel when possible, office recycling, and other initiatives taken by both the vendor and their parent company regarding environmental sustainability.	2
8. Businesses should undertake initiatives to promote greater environmental responsibility.	See above.	See above.	1
9. Businesses should encourage the development and diffusion of environmentally friendly technologies.	See above.	See above.	1
10. Businesses should work against corruption in all its forms, including extortion and bribery.	Vendor does business in countries known as problem areas for corruption, bribery, kidnapping, etc.	Vendor's code of conduct explicitly forbids employees to engage in bribery or other corrupt practices in accordance with the U.S. law, the Foreign Corrupt Practices Act.	2
		Total Risk Score	12
1–Low (10-17)	**2–Medium (18-23)**	**3–High (24-30)**	

Source: Adapted from the United Nations Global Compact, "The Ten Principles of the UN Global Compact." https://www.unglobalcompact.org/what-is-gc/mission/principles. Accessed on August 27, 2018.

Appendix C. Due Diligence Considerations

This table lists some key topics and questions an organization may ask to determine whether their selected third parties are appropriate and able to operate within the terms of the contract when negotiated. The list is neither exhaustive nor meant to be used as an engagement work program or checklist.

Table 1: Key Topics and Questions to Determine Eligibility of Potential Third-party Vendors

Ownership structure and background
■ What is the legal structure of the organization (a corporation, limited liability corporation, not-for-profit entity, etc.)?
■ Who owns the organization? Obtain details of the ownership.
Company performance and financial health
■ Is the company solvent? Obtain financial statements.
■ Is the company a likely candidate for a buyout or hostile takeover?
■ Is the company party to any lawsuits or subject to any fines or civil penalties?
Company location
■ Is the organization licensed to do business with the country/state in which its business and any other offices reside?
■ Is the company located in a geographical area far from your organization's location or in an area at-risk for any of the organization's red flags?
Business model and practices
■ Obtain a summary of the company's business strategies and direction for the next three years.
■ Why should the company be considered (or why was it considered) for a strategic alliance with the organization?
■ Does the company have a stated philosophy or mission statement that indicates they would be a "good match" for the organization?
References
■ How many clients does the company currently serve? How many are significant to the organization's operations (i.e., to what extent is the entity dependent on a few large customers)?
■ How many clients have terminated their relationship with the company in the last 12 months? Why?
■ Obtain a list of other clients in the organization's industry that are doing business with the company.
Service delivery capability, status, and effectiveness
■ What materials/services would be received as part of the service/product (analyses, bids, etc.)?
■ What training does the company provide for the service/product?
■ Is training provided by on-site qualified trainers or delivered electronically using qualified trainers?
Pricing and billing
■ How is the service/product currently priced?
■ Does the company expect this pricing structure to change? How often?
■ What is the company's billing process?

Table 2: Documentation That May Be Gathered to Assist in Determining Eligibility of Potential Third-party Vendors
Financials
■ Financial statements/annual reports.
Business continuity
■ Policies and/or procedures regarding granting, restricting, and terminating access to data. ■ Business continuity/disaster recovery plans and testing results. ■ Incident response procedures. ■ Insurance certificates.
Cybersecurity
■ Information stating where data is processed and stored and evidence of compliance with relevant regulations.
Contractual obligations
■ Letters/memoranda of understanding. ■ Nondisclosure agreements.
Ethics policies
■ Codes of conduct. ■ Relevant ethics policies including whistleblower policies and procedures.
Controls
■ Assurance Reports on Controls at a Service Organization as required by International Standards for Assurance Engagements (ISAE) No. 3402 for international organizations or by Statement on Standards for Attestation Engagements No. 18 (SSAE-18) for United States organizations.

Once these inquiries are completed and evaluated, the selected third-party vendor may be submitted along with the required reporting to senior management or the board for approval. That step may be delayed until a contract is negotiated as required by the organization's third-party risk management policy.

Appendix D. Considerations for Small Internal Audit Departments

Small organizations may not have departments dedicated to third-party risk management, procurement, or a similar function. The key is having at least one individual accountable for the third-party risk management processes to ensure the process is working as intended and that management is completing its due diligence and monitoring responsibilities.

Internal audit activities with limited resources can approach third-party risk management from the perspective of auditing the process, focusing on assessing the strength of management's risk assessments. In doing so, internal audit can review management's documentation, interview responsible officials, and select third parties to examine more closely to determine agreement with management's conclusions and assessments. Interviews with SMEs and walkthroughs of the contracting process may also be helpful on a sample basis.

For small organizations, internal audit should understand third-party risk management, the organization's business model, and the risks involved. Being limited to ticking checklist boxes to ensure proper paperwork exists and is filed properly leaves the organization open to the risks potentially presented by third-party relationships and negates the value internal audit can provide, especially in organizations with few resources.

Example

A small credit union hired a third party to implement a service that would allow members to sign in to the third-party website, enter their credit union account number and an account number from another banking institution to transfer funds. The third party would then initiate an electronic funds transfer to move money from the member's bank account to the credit union.

The credit union's project team assigned to evaluate the third party's contract ensured that the appropriate forms were submitted to complete the checklist of documents required by the credit union's vendor management program. In theory, the project team complied with the requirements.

However, the project team neglected to consult a subject matter expert from IT to review the contract's technical specifications. When the IT department was asked to grant the third party access to the credit union's network and core transaction system, they started asking questions. IT engineers at the credit union discovered the contract made no guarantee on the quality of the third party's cybersecurity protocols and had no provision on what might occur if the third party's systems were breached, potentially exposing member information. They discovered the contract also failed to specify whether the third party would retain the member's information on their systems or if that sensitive information would be permanently and verifiably deleted.

The contract had already been signed and the termination clause, which also had not been properly reviewed, included a provision that in the event the contract was terminated for any reason prior to a five-year term, the credit union would owe the vendor all licensing and operation fees due to them and an additional estimate of all revenue lost by the third party for not collecting their fees from the members who may have used their service.

The credit union learned an expensive lesson on using the resources they had to protect their members and themselves from unfavorable third party contract terms.

Appendix E. Contract Review Considerations

This section lists considerations for contract terms an organization may wish to use when negotiating and reviewing contracts. These lists are not exhaustive, not meant to be used as an engagement work program or checklist, and should not be construed as legal advice. Each third-party relationship and contract should be evaluated based on the organization's third-party risk management framework and/or processes.

Table 1: Contract Terms to Consider

Operational

- A statement that the third party is a valid enterprise operating in compliance with all applicable laws and regulations.
- A statement requiring the third party to immediately report any changes in its ownership or change in structure that would affect its risk profile.
- Arrangements if a third party is unable to operate due to unforeseeable circumstances beyond their control (e.g., weather events or geopolitical issues, also known as force majeure).
- Hold harmless clauses.
- Bank guarantees are valid up to the expiry date of the contract (this may be missed if the contract is automatically extended).

Monitoring, issue resolution, termination

- The third party's representation and warranty of the quality of their product or service.
- Penalties for breach of contract (e.g., failure to deliver products or services on time and of acceptable quality according to the SLA, also known as liquidated damages).
- Conditions allowing the third party to rectify issues related to quality, delivery, or other issues within certain time frames and conditions.
- Dispute resolution protocols.
- Customer complaints (e.g., the contract should define what constitutes a customer complaint and state who is empowered to make decisions according to specified criteria).
- Specific termination conditions and any costs associated with early termination, including the ability to terminate a third-party relationship due to change of control or management within the third-party organization among other reasons. Termination conditions should also outline the support requirements during the transition and the retention/return of data expectations.

Ethics/code of conduct

- A statement that the third party will abide by the contracting organization's third-party code of conduct, ethics standards, policies, procedures, and values.
  - This statement may be followed by a requirement that all employees of the third party who work on the contract be educated regarding the contracting organization's standards, culture, compliance requirements, etc., including a stipulation that employees certify their understanding in writing.
- Clauses regarding anti-corruption and anti-retaliation.

Technology

- Confidentiality and data protection/cybersecurity requirements, which may be stringent depending on the applicable regulations.
- Requirements to disclose data breaches within a certain period of time based on the time of detection.

Fourth parties

- Approval requirements should a third party engage subservice agents (fourth parties) to fulfill obligation.
- Fourth-party usage conditions or restrictions.

Table 2: Sample Contract Review Checklist		
Scope	**Yes**	**No**
The contract is effective for a stated period, not "auto-renewed." The vendor management policy prohibits "auto-renewed" contracts.	☐	☐
The contract states the method and requirements for renewal, and allows for negotiation of terms.	☐	☐
The contract states the third party will comply with all applicable laws, regulations, and regulatory guidance.	☐	☐
The contract states the service provider/vendor carries appropriate insurance coverage per the terms of the contract, and is obligated to provide proof of such coverage to the organization.	☐	☐
The contract provides for ongoing due diligence obligations of the organization under the vendor management policy, and requires the service provider/vendor to cooperate as applicable.	☐	☐
The contract explains the organization's rights regarding amendments or other changes, and are fully understood by management.	☐	☐
Cost and compensation	**Yes**	**No**
The contract states the fees to be paid, including fixed compensation, variable charges, and any fees to be paid for nonrecurring items or special requests.	☐	☐
The contract states the cost and responsibility for purchasing and maintaining equipment, hardware, software, or other items related to the product or service.	☐	☐
The contract identifies the party responsible for payment of legal or audit expenses.	☐	☐
The contract minimizes short-term incentives, and employs compensation structured to promote long-term performance in a safe and sound manner.	☐	☐
Performance standards	**Yes**	**No**
The contract lists the frequency, format, and specifications of the product or service to be provided, in a measurable standard.	☐	☐
The contract states other services to be provided, such as software support and maintenance, training of employees, and customer service.	☐	☐
The contract identifies which party will be responsible for delivering any required customer disclosures.	☐	☐
The contract states the terms related to any use of the organization's premises, equipment, or employees.	☐	☐
The contract prohibits the third party from subcontracting or using another party to meet its obligations with respect to the contract without first obtaining written permission from the organization.	☐	☐

Table 2: Sample Contract Review Checklist (continued)		
Reports	**Yes**	**No**
The contract specifies the type and frequency of management information reports to be received from the service provider/vendor.	☐	☐
The contract outlines routine reports, such as performance reports, audits, financial reports, security reports, exception reports, and business resumption testing reports, to be provided and that serve as notification of changes or problems that could affect the relationship or pose a risk to the organization.	☐	☐
Audit	**Yes**	**No**
The contract specifies the institution's right to audit the third party, including by engaging an independent auditor, as needed to monitor performance under the contract.	☐	☐
The contract ensures the third party's internal control environment as it relates to the service or product being provided is sufficiently audited.	☐	☐
The contract includes authorization for the appropriate federal and state regulatory agencies to have access to records as is necessary or appropriate to evaluate compliance with laws, rules, and regulations.	☐	☐
Confidentiality and security	**Yes**	**No**
The contract prohibits the service provider/vendor and its agents from using or disclosing data or information, except as necessary to perform the functions designated by the contract.	☐	☐
The contract specifies nonpublic personal information must be handled in accordance with applicable privacy laws and regulations.	☐	☐
The contract states that breaches in the security and confidentiality of information, including unauthorized intrusion, are required to be fully and promptly disclosed to the organization.	☐	☐
Customer complaints	**Yes**	**No**
The contract specifies which party has the duty to respond to any complaints received from customers of the organization.	☐	☐
The contract states that if the third party is responsible, a copy of the complaint and the resolution should be forwarded to the organization.	☐	☐
The contract provides for periodic summary reports detailing the status and resolution of complaints.	☐	☐
Business resumption and contingency plans	**Yes**	**No**
The contract provides for continuation of services in the event of an operational failure by the service provider/vendor, including man-made and natural disasters.	☐	☐
The contract specifies the service provider/vendor will provide appropriate protections for backing up information and maintaining disaster recovery procedures to secure the organization's data and information.	☐	☐
The contract specifies the service provider/vendor will provide results of their disaster recovery and contingency plan testing.	☐	☐

Table 2: Sample Contract Review Checklist (continued)		
Default and termination	**Yes**	**No**
The contract specifies what circumstances constitute default, identifies remedies, and allows for a reasonable opportunity to cure a default.	☐	☐
Termination rights under the contract are identified.	☐	☐
The contract states termination and notification requirements, with operating requirements and time frames for the orderly conversion to another entity.	☐	☐
The contract specifies the return of the organization's data, records, and/or other resources.	☐	☐
Dispute resolution	**Yes**	**No**
The contract specifies how disputes over contract terms and/or performance will be resolved.	☐	☐
The contract states the service/product will be provided during the resolution of a dispute.	☐	☐
Indemnification	**Yes**	**No**
The contract contains indemnification provisions requiring the third party to hold the organization harmless from liability as a result of the third party's own negligence, and vice versa. (NOTE: Indemnification clauses do not exempt the organization from regulatory corrective actions.)	☐	☐
Limits on liability	**Yes**	**No**
The chief financial officer has evaluated and substantiated that any liability limitation in the contract is reasonable compared to the amount of loss the organization would incur should the third party fail to adequately perform.	☐	☐
Approval and execution	**Yes**	**No**
The contract has signatures of both the organization representative and the service provider/vendor representative.	☐	☐
The original contract with both sets of signatures, either paper or electronic, has been sent to Compliance.	☐	☐
Requirements of foreign vendors	**Yes**	**No**
The contract has been reviewed by legal counsel.	☐	☐
The contract has been reviewed for risks associated with foreign vendors from the vendor management program (including: country, operations, compliance, strategic, and credit risks).	☐	☐

Source: Adapted from the Federal Deposit Insurance Corporation. "Guidance For Managing Third-Party Risk." https://www.fdic.gov/news/news/financial/2008/fil08044a.html. Last updated June 6, 2008.

Appendix F. Right to Audit Clause Illustration

Frequently, contracts will include a single paragraph that simply states a party's option of the right to audit the other party. Vendors can and do restrict an organization's ability to conduct an audit. This is why it is important for the contract to carefully document the organization's rights, and spell out expectations and responsibilities to avoid unnecessary constraints. The right to audit should not be a simple clause or statement in the contract. It should clearly state the conditions and criteria necessary to conduct a comprehensive audit under reasonable and acceptable conditions and practices.

The following list documents a set of condition statements that management may request to be included when drafting any right-to audit statement in a contract. Vendors should be willing to discuss these terms as long as the organization is firm that the contract will not be signed unless the vendor agrees to reasonable right-to-audit conditions.

This table uses the terms SOC 1, SOC 2 (SOC Type 1 and SOC Type II). SOC stands for Service Organization Controls. These terms reference reports accounting standards require third parties to produce, and auditors (both internal and external) should confirm management asks for and receives these reports to achieve a proper level of due diligence for significant third-party relationships. As of 2017, the American Institute for Certified Public Accountants (AICPA) replaced the Statement on Standards for Attestation Engagements No. 16 (SSAE-16) and SOC I reports with the SSAE-18. The SSAE-18 focuses on financial reporting controls.

SOC 2 reports still exist and are sometimes required in the United States by focus on a business's nonfinancial reporting controls as they relate to security, availability, processing integrity, confidentiality, and privacy of a system. The International Standards for Assurance Engagements (ISAE) No. 3402 report is the global equivalent. The terms SOC 1 and SOC 2 are used in the table to provide clarity regarding the difference between the two sets of information provided, which may be helpful to internal auditors who want to build questionnaires regarding this information.

For more information on the SSAE-16, SSAE-18, SOC 1 and SOC 2 reports, please refer to https://www.ssae-16.com/soc-1/ and https://www.aicpa.org/. For more information on the ISAE No. 3402 report, please refer to http://isae3402.com/ISAE3402_overview.html.

Examples of Condition Statements for a Right-to-Audit Statement

Audit notification

Sample condition statement	Purpose and considerations
Except in the case of surprise audits, as may be subsequently described, client agrees to provide vendor prior notice, not less than ____ but no more than ____ days' before commencing an onsite audit.	The required notification period should be stated. A common vendor assertion is to suggest that a 30, 60, or even 90 day notice period is required unless it is specifically spelled out. A "reasonably sufficient" notification term is not adequate. **NOTE:** If the company desires the right to perform surprise audits, that should be clearly noted and under what conditions a surprise audit is possible (see Right to Evaluate Vendor's IT Processes below).

Scope of work hours

Sample condition statement	Purpose and considerations
The client will be allowed to conduct the audit during normal business hours, and the vendor will provide appropriate access to facilities, staff, and records, and adequate workspace for an audit team of up to [#] auditors to include internet and utility connectivity and access during the audit period.	Hours of work should be clearly defined. If the auditors intend to conduct audit work during normal business hours, the contract should specify the time frame expected. Vendors may require this to avoid adverse effects on normal processing or operations. If an audit must be performed outside normal hours, such as evening or overnight hours, vendors may require the client to pay for staffing or supplies necessitated by work required outside normal operating hours.

Scope of location

Sample condition statement	Purpose and considerations
Any vendor location (including offshore locations) that is directly or indirectly within or related to the scope of products or services provided to the client may be subject to visit, and the conducting of audit procedures, to successfully accomplish the audit plan objectives.	The vendor may require that audits only be performed at a specific location, such as a headquarter office. If significant operation centers, data centers, or storage facilities are made unavailable, the audit can be impeded. Any location that can access, view, or manipulate the auditors' data must be within the scope of the right to audit. Even if "logically" restricted, if the capacity to access data is reasonably possible, auditors must be able to include such locations within the scope of audit rights.

Examples of Condition Statements for a Right-to-Audit Statement (continued)

Right to access documents, data, or use audit software

Sample condition statement	Purpose and considerations
While conducting the audit, the vendor will provide access to all client-related original documentation and data (or its legal equivalent), whether physical or logical, necessary to accomplish the audit objective. Client reserves the right to query its data by appropriate direct access to the data storage media upon which said data is contained.	During the audit, direct access to data may be necessary to verify or validate information and documents. If the vendor is able to isolate auditors from the "real" data, the audit is compromised. The right to access original documents and data within an application may be necessary to effectively accomplish the audit objectives. Some issues may arise depending on how the data is physically or logically segmented from the vendor's other client data they store and/or manage. **NOTE:** If a data extract procedure is necessary (due to security or privacy concerns), the procedure and extract script should be reviewed by a qualified and competent professional selected by the client and the procedure should be run under the supervision of the client. Such circumstances need to be clearly stated if so conditioned.
The client has the right to use general audit software and other reporting tools against the data files and/or databases that contain the client's data or data relating to the client.	Auditors may need to ensure that data provided is accurate and corroborated by sources. This may require use of specialized analytic software and direct queries to extract genuine data.

Right to evaluate vendor's financial and operational processes

Sample condition statement	Purpose and considerations
The client has the right to request and obtain current financial statements, whether audited by a firm of chartered or certified public accountants (CPAs) or not, and any associated audit reports, including letters with recommendations to management.	
If the vendor provides financial reporting services, the client has right to request and obtain a current and appropriate Service Organization Control (SOC) 1 (SOC 1) report issued by a CPA firm or other recognized professional source. SOC reports will be full Type II reports that include the vendor's description of control processes, and the independent auditor's evaluation of the design and operating effectiveness of controls.	Auditors must obtain a SOC Type II report to receive: ■ Description of the controls. ■ Auditor's evaluation of the design of the controls. ■ Auditor's evaluation of the effectiveness of the operation of those controls. A Type I report does not include testing of the operational effectiveness and therefore is not acceptable.
The client, using appropriate generally accepted and recognized auditing standards, has the right to evaluate the vendor's processes and practices relevant or relating to its products or services provided to/for the client under this contract.	

Examples of Condition Statements for a Right-to-Audit Statement (continued)

Right to evaluate vendor's IT processes

Sample condition statement	Purpose and considerations
The client has the right to request and obtain, at client's discretion, a current and appropriate Service Organization Control (SOC) report and/or other applicable and relevant independent assessment report(s) that encompasses the vendor's IT processes. SOC reports will be full Type II reports that include the vendor's description of control processes, and the independent auditor's evaluation of the design and operating effectiveness of controls.	SOC 1 reports are for financial reporting. SOC 2 reports cover IT processes and focus on one or more of American Institute of Certified Public Accountants (AICPA's) defined Trust Principles™: ■ Security. ■ Availability. ■ Confidentiality. ■ Processing Integrity. ■ Privacy. Other independent assessment reports such as PCI or ISO certifications may be appropriate but must be accepted at the organization's discretion.
In addition to receiving any independent assessment report, the client reserves the right to conduct relevant and applicable IT assessments above and beyond the SOC testing to assure that the client's information assets are properly protected. Areas that may be included in such testing include, but are not limited to vendor's: ■ Business continuity including disaster preparedness and recovery. ■ Ability for client to attend one of the vendor's recovery and readiness tests. ■ Backup, recovery, and data transfer procedures, including verification that backup media is readable and access to observe and verify off-site records/data management facility(s). ■ Security and privacy procedures and conditions including right to perform a security/privacy baseline assessment, periodic security/privacy test re-performance, and planned or surprise penetration testing.	The receipt and evaluation of an adequate and appropriate SOC report will likely suffice, but internal auditors must ensure they have a right to and can perform their own independent assessment of appropriate procedures and controls. Note that with the right to perform their own system and network penetration testing planned and surprise the vendor may justifiably necessitate limitations if vendor IT resources (databases, etc.) are shared with other clients. Limitations under these circumstances are appropriate, but should be documented in the contract. The organization should expect the vendor to make the same conditions effective if another client requested similar rights.

Right to include subcontractor or outsourced parties

Sample condition statement	Purpose and considerations
The vendor cannot subcontract or outsource any work or responsibilities for work performed under this contract without the client's prior written approval. If such approval is granted, the vendor must extend client's audit rights and conditions under this contract to each and every subcontractor or outsourced party that may perform services, or responsibilities under this contract.	Internal audit may need to extend the right to audit to all subcontractors or outsourced parties, which the vendor may delegate or assign its responsibilities and obligations to satisfy the contract. In addition, if allowed, internal auditors may need to warrant that the vendor passes these obligations and conditions to its partner organizations.

Source: Lance Johnson, L&H Johnson, LLC. Used by permission.

Appendix G. Testing and Evaluating Third-party Risk Management

Given the internal audit activity's role in providing independent assurance that the organization is managing risk in a way that is consistent with its risk appetite, any applicable regulatory requirements and the achievement of its objectives, the following tables comprise a framework for conducting an internal audit of third-party risk management. The internal auditor may need to tailor or create test steps for unique areas of an organization's policies and procedures. The internal auditor may also need to refer to audit programs for related areas (i.e., procurement, compliance, legal) to design a fully developed third-party risk management audit, especially if the audit is segmented as mentioned in this guide.

As illustrated in this guide, an internal audit engagement covering third-party risk management may be done using any, some, or all of these four approaches:

1. Audit the third-party risk management framework (e.g., risk appetite, governance, methodology). See Table 1.
2. Audit the third-party risk management process (e.g., procurement audit). See Table 2.
3. Audit a component of the third-party risk process (e.g., contracts audit).
4. Include third-party risk management in a process or product audit (e.g., a payroll audit would include evaluating the third-party risk management processes used for the third-party processing payroll).

Table 1: Audit the Third-party Risk Management Framework

Risk reporting

- Gather documentation including:
  - Charters, policies, and other mandate information for the governance entities responsible for establishing and overseeing the third-party risk management program.
  - Documentation of all phases of the third-party risk reporting process.
- Gain an understanding of the key risks identified as related to the organization's objectives.
- Determine whether third-party risk reporting is effective in communicating actual status of risk exposure in the organization (e.g., is it too complicated, is it too simple).
- Assess whether management has rated third-party risks in accordance with the organization's established risk assessment methodology.

Communication

- Follow third-party risk reporting in various areas to ascertain whether risk information is flowing uninhibited up, down, and across the organization.

Accountability

- Confirm third-party risk owners are held accountable for risk exposures in their sphere of authority.
- Confirm the board and senior management are held accountable regarding asking for and using third-party risk information in decision making.

Table 1: Audit the Third-party Risk Management Framework (continued)

Risk appetite

- Review the organization's risk appetite program for completeness and adequacy.
- Ensure it contains the necessary components:
  - Risk capacity: The maximum level of risk the organization can assume given its current level of resources, constraints, and its obligations.
  - Risk limits: The allocation of aggregate risk appetite limits to business lines, legal entities, specific risk categories, and other relevant granular levels.
  - Risk tolerance: Indicates how much variance the organization will accept around revenue and expenses, etc., given the parameters set for risk capacity and their associated risk limits.
- Review plans and processes to communicate the risk appetite to all employees.
- Ensure the plan covers the entire organization and is executed regularly.
- Ensure third-party contracts and service level agreements (SLAs) are consistent with the organization's risk appetite.
- Use surveys, interviews, or other methods to ascertain both employee participation in communication programs and their level of understanding regarding the organization's risk appetite.
- Internal auditors should confirm the existence of several components necessary for an organization to effectively articulate and enforce its risk appetite in a third-party relationship:
  - Risks are identified, assessed, and documented during third-party due diligence and updated at regular points throughout the relationship.
  - A vendor master file is in place and updated regularly.
  - Standard contracts are in use as a base that can be modified as required by each specific third-party relationship.
  - SLAs are matched with and relevant to the organization's operational objectives and expectations, including the business continuity plans of both the organization and the third-party provider.
  - A monitoring process exists that will flag issues concerning the third party as quickly as necessary given the third party's criticality to the organization.

Policies and procedures

- Verify that the policies and procedures are current and updated timely for any procedural changes.
- Confirm that any updates requested by the board during the annual review were properly made.
- Ensure the policies and procedures cover the entire third-party risk management process in detail. Specific areas of importance include:
  - Relationship to strategies and risk appetite.
  - Governance overview.
  - Risk limits and tolerances with their associated triggers and escalation protocols (walk through the process from the identification of a breach through resolution).
  - Roles and responsibilities.
  - Data considerations.
  - Regulatory requirements.

Risk assessment process

- Identify where and how often third-party risk assessments are conducted across the organization.
- Examine processes for risk identification, assessment, treatment, and monitoring/reporting for consistency.
- Review information obtained in the preliminary risk assessment to assess the impact and likelihood of third-party related risks occurring in the organization.

Table 2: Audit the Third-party Risk Management Process

Sourcing

- Confirm each third party presenting a high risk to the organization has a clearly defined and accountable relationship owner.
- Confirm from a sample of third-party relationships that the sourcing process for narrowing the number of third parties eligible for consideration was followed and documented properly according to the organization's third-party risk management policy and procedures.

Due diligence

- For a new relationship and/or a new engagement with an existing relationship, confirm management has gathered the appropriate due diligence information for the third party according to the level of risk the third party may present to the organization. Documentation may include:
  - Financial statements/annual reports.
  - Business continuity/disaster recovery plans and testing results.
  - Information stating where data is processed and stored.
  - Policies and/or procedures regarding granting, restricting, and terminating access to data.
  - Insurance certificates.
  - Letters of understanding.
  - Nondisclosure agreements.
  - Service level agreements.
  - Incident response procedures.
  - Codes of conduct.
  - Relevant ethics policies including whistleblower policies and procedures.
- Obtain management's risk assessment of the third party and confirm it conforms to the organization's required risk assessment process.
- Internal audit may also reperform one or more third-party risk assessment(s) and determine whether they agree with management's conclusions.

Contracting

- Confirm the organization's standard contract clauses are included in the third-party contract.
- Confirm personally identifiable information or other critical information is addressed properly in contracts.
- Confirm right to audit clause has been included, if appropriate.
- Confirm termination clauses in key third-party contracts meet the organization's expectations.
- Review SLAs; ensure they are being regularly monitored and are consistent with the organization's risk appetite.

Table 2: Audit the Third-party Risk Management Process (continued)

Monitoring

- Confirm high risk/critical third parties are monitored properly including having their information entered into the third-party management system.
- For a sample of ongoing third-party relationships, confirm management has continued to gather the appropriate due diligence information for the third party according to the level of risk the third party may present to the organization. Documentation may include:
  - Financial statements/annual reports.
  - Business continuity/disaster recovery plans and testing results.
  - Information stating where data is processed and stored.
  - Policies and/or procedures regarding granting, restricting, and terminating access to data.
  - Insurance certificates.
  - Letters of understanding.
  - Nondisclosure agreements.
  - Service level agreements.
  - Incident response procedures.
  - Codes of conduct.
  - Relevant ethics policies including whistleblower policies and procedures.
- Obtain management's risk assessment of the sampled third parties and confirm they conform to the organization's required risk assessment process.
- Ensure risk owners are performing and documenting monitoring activities in a timely manner and submitting the required documentation to the proper oversight bodies.

Issue resolution

- Confirm issues are appropriately escalated according to the organization's third-party risk management policy and procedures.
- Confirm any fees or compensation due to the organization from the third party per the contract terms have been collected (quality issues, down time, etc., may require the third party to reimburse the organization for the breach of contract terms).

Termination

- Obtain a sample of terminated third parties and ensure the contract terms were honored.
- Note any contract terminations that resulted in fees or other charges to the organization.
- Note any contracts that are auto-renew and discuss the risks of auto-renew contracts with management.

Appendix H. Sample Third-party Risks and Red Flags/Warning Signs

This table lists some of the main risk areas that internal auditors should consider when performing a third-party risk management engagement. The list is neither exhaustive nor meant to be used as an engagement work program or checklist.

Table 1: Sample Third-party Risks

Risk Category	Risks
Strategic	■ Not achieving the objectives of the relationship. ■ Reputational damage. ■ Loss of intellectual property.
Operational	■ Physical security. ■ Fourth parties. ■ Quality – failure to perform according to SLA. ■ Records retention pre- and post-termination. ■ Concentration of critical services to too few third parties. ■ Inadequate, unreliable, or untimely performance of risk assessments. ■ Failure to integrate SMEs into the due diligence and contracting process steps.
Human resources	■ Inadequate training. ■ Lack of personnel.
Financial	■ Cost overruns. ■ Failure to collect penalties. ■ Misuse of funds.
Legal/compliance	■ Corruption. ■ Conflict of interest. ■ Fraud. ■ Lawsuits. ■ Civil damages.
Technology	■ Business continuity and disaster recovery. ■ Failure to test compensating controls indicated as required by the third party. ■ Security, privacy, and confidentiality of information, especially sensitive or nonpublic information that is available to, accessed by, or maintained by the vendor.

Red Flags

The global enforcement climate is currently active on issues such as anti-corruption, privacy, and competition. Given this environment, there are red flags or warning signs that internal auditors may encounter during a third-party risk management engagement.

These red flags, among others, may increase risk exposure and indicate a closer look is necessary.

Table 2: Red Flags/Warning Signs

Category	Signs
Regional characteristics	■ Third parties are geographically remote from the organization. ■ Third parties work in different cultures with different customs, language, and expectations. ■ A representative for the third party has been referred to the organization by a government official. ■ The region, country, or industry in which the third party participates has a history of corruption.
Contracting and monitoring	■ The third party requests a contract that has little detail regarding the work being performed or service provided. ■ The third party rejects a right to audit clause in the contract. ■ Third parties are not familiar with the organization's rules or have no incentives to comply with those rules. ■ The third party utilizes shell companies in its corporate structure.
Financials	■ The third party or its representative is requesting or granted an unusually high commission. ■ The third party has been granted unusual payments or financial arrangements. ■ The third party is not transparent with its financial records. ■ The third party requests payment before the work is completed. ■ The third party requests to be paid in cash (undocumented or otherwise unaccounted for), or in a country other than where the work is actually performed.

Appendix I. Audit Considerations for Fourth Parties

Fourth-party risks can be difficult for organizations to evaluate. There are many unanswered questions as outsourcing becomes more common. One significant consideration is how far down the supply chain should an organization reach in terms of audits. Typically, organizations leave the main responsibility with their contracted third party. If that party identifies issues with product or services provided by the fourth party, the organization either assumes or has written into the contract that the contracted third party resolve the issue.

This approach often works in theory, but may not be adequate in the real world. Whether it is part of business continuity planning/disaster recovery or another exercise conducted along with the third party risk management processes, all third parties critical to an organization's operations should be evaluated as far down in the supply chain as necessary to provide management and the board with the knowledge necessary to effectively manage third party risk.

Example

In 2011, an earthquake followed by a tsunami and a nuclear crisis did severe damage to northeastern Japan. As a consequence, the supply of parts to the global automotive industry was interrupted indefinitely. The Japanese auto manufacturing industry runs (as do many manufacturing and retail industries) on a just-in-time delivery system that works best when parts are available exactly when they are needed. This delivery system is ideal for organizations that run lean and efficient production lines.

Toyota had several parts factories in the Tohoku region, which was severely affected by the tsunami. The company had to stop or significantly scale back production at select factories, and it was not known how long it would be impacted. The Tohoku region supplied Toyota with parts, but was also home to factories that produced sophisticated electronic components for luxury brands such as BMW.

Impact from factory shutdowns rippled throughout the global auto industry as a whole, with steelmakers impacted by the drop in demand for their product. Auto parts makers located outside Japan also faced a drop in demand for their products. Damage to shipping ports in northeastern Japan had negative effects on exports of select car models and specialty parts only made in Japan. These risk impacts continued affecting stock prices, market share, and earnings for approximately five years after the initial crisis.

Scenario-based analyses may help management and the board fully understand the impact of third- and fourth-party risks to their organizations. Internal auditors should be mindful of the global nature of business and pursue their third party internal audit activities to an appropriate level. This can help ensure the organization's real-world risk exposure is considered and that key risk indicators, escalation protocols, and other third party risk management processes are followed.

The problem becomes more complex when dealing with data, such as the personally identifiable of the organization's customers. Typically organizations do not allow third party subcontractors access to their systems directly, but what if the third party is passing data to the fourth party through direct connections to the organization's systems?

If the third party has outsourced its entire IT function, this will require the contracting organization's careful consideration. This type of arrangement may require the organization to connect directly with a fourth party. If the fourth party has not been correctly and thoroughly evaluated, there may be unidentified risk exposure to the organization. A helpful principle may be that the lower down the supply chain the vendor participates (third party → fourth party → fifth party → etc.), the more restricted their access to information becomes.

Appendix J. References and Additional Reading

References

Federal Deposit Insurance Corporation. "Guidance For Managing Third party Risk." Last updated June 6, 2008. https://www.fdic.gov/news/news/financial/2008/fil08044a.html.

The Institute of Internal Auditors, *International Professional Practices Framework, 2017 Edition* (Lake Mary, Fla.: Internal Audit Foundation, 2017).

United Nations Global Compact. "The Ten Principles of the UN Global Compact." Accessed on August 27, 2018. https://www.unglobalcompact.org/what-is-gc/mission/principles.

Additional Reading

A Security Manager's Guide to Vendor Risk Management. Bitsight Technologies, 2016. White paper PDF. https://info.bitsighttech.com/security-managers-guide-to-vrm.

Australian Prudential Regulatory Authority. *Prudential Standard CPS 231: Outsourcing*. (APRA, July 2017.) https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf.

Basel Committee on Banking Supervision. *The Joint Forum: Outsourcing in Financial Services*. (Basel, Switzerland: Bank for International Standards, 2005.) https://www.bis.org/publ/joint12.pdf.

Board of Governors of the Federal Reserve System. SR 13-1/CA 13-1. *Supplemental Policy Statement on the Internal Audit Function and Its Outsourcing.* Division of Banking Supervision and Regulation, January 23, 2013. www.federalreserve.gov/bankinforeg/srletters/sr1301.htm.

Board of Governors of the Federal Reserve System. SR 13-19/CA 13-21.*Guidance on Managing Outsourcing Risk*. Division of Banking Supervision and Regulation, Division of Consumer and Community Affairs, December 5, 2013. https://www.federalreserve.gov/supervisionreg/srletters/sr1319.htm.

Board of Governors of the Federal Reserve System. SR 16-14. *FFIEC Information Technology Examination Handbook — Information Security Booklet.* Division of Banking Supervision and Regulation, September 19, 2016. www.federalreserve.gov/bankinforeg/srletters/sr1614.htm.

Financial Stability Board. *Principles for an Effective Risk Appetite Framework*. (FSB, November 18, 2013.) http://www.fsb.org/wp-content/uploads/r_131118.pdf.

Institute of International Finance. *Implementing Robust Risk Appetite Frameworks to Strengthen Financial Institutions*. (IIF, June 17, 2011.) https://www.iif.com/file/7075/download?token=NOwe4NwK.

Monetary Authority of Singapore. *Guidelines on Outsourcing*. (MAS, July 27, 2016.) http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/Outsourcing%20Guidelines_Jul%202016.pdf.

Office of the Comptroller of the Currency. OCC Bulletin 2013-29. *Third party Relationships: Risk Management Guidance*. U.S. Department of the Treasury, October 30, 2013. https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

Office of the Comptroller of the Currency. OCC Bulletin 2017-7. *Third party Relationships: Supplemental Examination Procedures*. U.S. Department of the Treasury, January 24, 2017. https://www.occ.gov/news-issuances/bulletins/2017/bulletin-2017-7.html.

Office of the Superintendent of Financial Institutions. B-10. *Outsourcing of Business Activities, Functions and Processes.* Revised March 2009. http://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b10.aspx.

Otani, Yoko, Julie Williams, and Rachel Anderika. "Third-Party Risk Management – A Strategic Priority in Financial Innovation." *Promontory Sightlines in Focus* (September 20, 2016). http://www.promontory.com/uploadedFiles/Articles/Insights/160920_Sightlines_InFocus_TPRM.pdf.

Stephens, Randy. *2017 Ethics & Compliance Third Party Risk Management Benchmark Report*. NAVEX Global, 2017. PDF. https://www.navexglobal.com/en-us/resources/benchmarking-reports/2017-ethics-compliance-third-party-risk-management-benchmark-report?RCAssetNumber=2760.

Acknowledgements

Guidance Development Team

Mark Carawan, CIA, QIAL, United States (Chairman)
Tim Penrose, CIA, United States (Project Lead)
Brian Foster, CIA, United States
Rune Johannessen, CIA, CCSA, CRMA, Norway
Thomas Sanglier III, CIA, CRMA, United States
Stacey Schabel, United States
Teis Stokka, CIA, QIAL, CRMA, Norway

Global Guidance Contributors

Lance Johnson, CIA, CRMA, United States
Ahmed Al-Khabash, CIA, CCSA, Yemen
Cornelis Klumper, CIA, United States
Dana Lawrence, CIA, CFSA, CRMA, United States
Awad Elkarim Mohamed, CIA, QIAL, CCSA, CFSA, CGAP, CRMA, United Arab Emirates
Arunima Jasneet Nanda, India

IIA Global Standards and Guidance

Jeanette York, CCSA, Director (Project Lead)
Lisa Hirtzinger, CIA, QIAL, CCSA, CRMA, Vice President
Debi Roth, CIA, Managing Director
Anne Mercer, CIA, CFSA, Director
Eva Sweet, Director
Shelli Browning, Technical Editor
Lauressa Nelson, Technical Editor

The IIA would like to thank the following oversight bodies for their support: Financial Services Guidance Committee, Guidance Development Committee, Information Technology Guidance Committee, Public Sector Guidance Committee, Professional Guidance Advisory Council, International Internal Audit Standards Board, Professional Responsibility and Ethics Committee, and International Professional Practices Framework Oversight Council.

About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 190,000 members from more than 170 countries and territories. The association's global headquarters are in Lake Mary, Fla., USA. For more information, visit www.globaliia.org.

Disclaimer

Copyright

October 2018

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
www.theiia.org