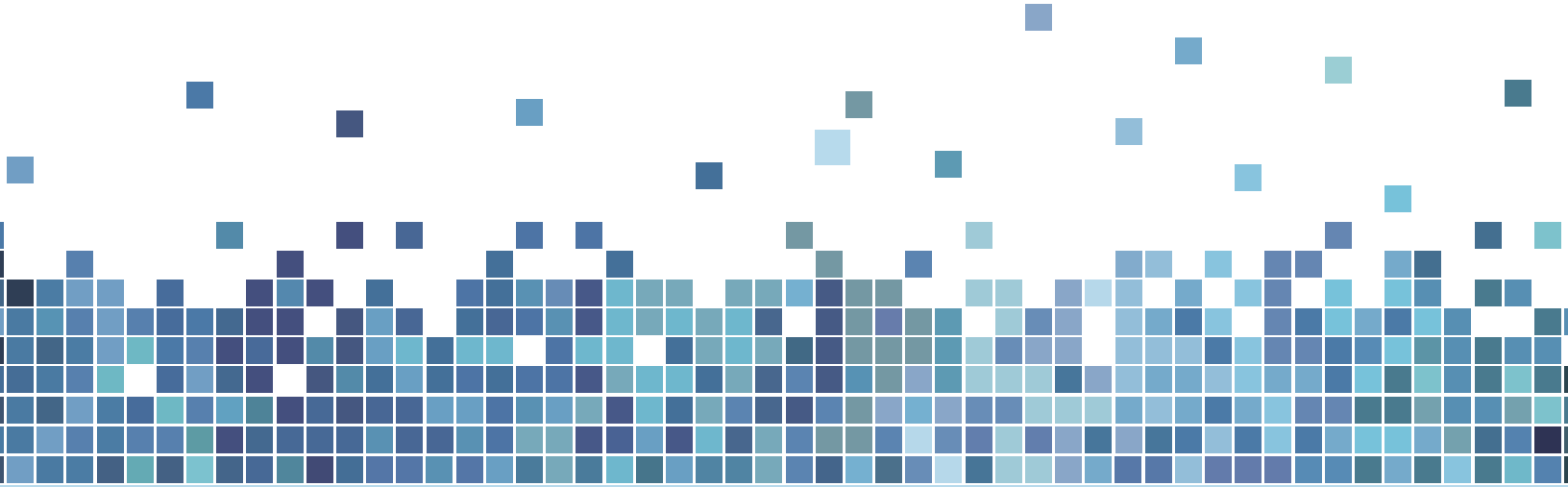
IIARF RESEARCH REPORT

Closing the Gaps in Third-Party Risk Management

Defining a Larger Role for Internal Audit



Crowe Horwath®

The Institute of Internal Auditors Research Foundation

Copyright © 2013 by The Institute of Internal Auditors Research Foundation (IIARF). All rights reserved.

Published by The Institute of Internal Auditors Research Foundation, 247 Maitland Avenue, Altamonte Springs, Florida, 32701-4201. (www.theiia.org/research)

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form by any means—electronic, mechanical, photocopying, recording, or otherwise—without prior written permission of the publisher. Requests to the publisher for permission should be sent electronically to: bookstore@theiia.org with the subject line "reprint permission request."

Limit of Liability: The IIARF publishes this document for informational and educational purposes and is not a substitute for legal or accounting advice. The IIARF does not provide such advice and makes no warranty as to any legal or accounting results through its publication of this document. When legal or accounting issues arise, professional assistance should be sought and retained.

The Institute of Internal Auditors' (IIA's) International Professional Practices Framework (IPPF) comprises the full range of existing and developing practice guidance for the profession. The IPPF provides guidance to internal auditors globally and paves the way to world-class internal auditing.

The IIA and The IIARF work in partnership with researchers from around the globe who conduct valuable studies on critical issues affecting today's business world. Much of the content presented in their final reports is a result of IIARF-funded research and prepared as a service to The IIARF and the internal audit profession. Expressed opinions, interpretations, or points of view represent a consensus of the researchers and do not necessarily reflect or represent the official position or policies of The IIA or The IIARF.

eISBN-13: 978-0-89413-816-4

18 17 16 15 14 13 1 2 3 4 5 6 7 8 9

CONTENTS

About the Author 5

About the Research Sponsors 5

Executive Summary 6

1 Introduction. 7

2 The Business Case for Investing in Third-Party Risk Management. 7

3 Research Methodology. 9

4 Trends in the Use of Third Parties. 9

5 Third-Party Risk Management Concerns 11

6 The Role of Internal Audit in Third-Party Risk Management 13

7 Who Owns Third-Party Risk? 17

8 Looking Ahead 19

Appendix A: A Third-Party Risk Management Capability Maturity Model. 21

Appendix B: Survey Respondent Demographics 23

Notes 25

LIST OF EXHIBITS

Exhibit 4.1. Use of Third Parties 10

Exhibit 4.2. Types of Third Parties Used 10

Exhibit 5.1. Third-Party Issues of Greatest Concern 12

Exhibit 6.1. Internal Audit Resources Spent on Third-Party Risks 13

Exhibit 6.2. Third-Party Use Compared to Internal Audit Resources Spent on Third-Party Risk 14

Exhibit 6.3. Bar Chart of Third-Party Use Compared to Internal Audit Resources Spent on Third-Party Risk. 14

Exhibit 6.4. Internal Audit Involvement in Decisions to Create Third-Party Relationships 15

Exhibit 6.5. Factors Considered When Selecting or Renewing Third-Party Relationships 16

Exhibit 6.6. Normal Practice Related to Third Parties. 17

Exhibit 7.1. Responsibility for Third-Party Risks. 18

Exhibit A.1. Third-Party Risk Management Capability Maturity Model 22

Exhibit B.1. Annual Revenue of Survey Respondents' Organizations (Non-Financial Services), USD. 23

Exhibit B.2. Total Assets of Survey Respondents' Organizations (Financial Services), USD. 23

Exhibit B.3. Number of Employees (FTEs) of Survey Respondents' Organizations 24

Exhibit B.4. Number of FTEs in the Respondents' Internal Audit Functions 24

ABOUT THE AUTHOR

Rick Warren is a principal with Crowe Horwath LLP and managing principal of the firm's Atlanta office. He is a director of the Stans Foundation and The Buckhead Coalition and the audit committee chair of the Atlanta Chapter of The Institute of Internal Auditors (IIA). He also has served as a member of The IIA's Atlanta Chapter Board of Governors.

Having spent most of his career advising corporate clients on risk management, governance, and internal control matters, Rick leads the Crowe third-party risk management service offering and is a frequent speaker on the topic of managing risks in the extended enterprise. He can be reached at 404.442.1606 or rick.warren@crowehorwath.com.

ABOUT THE RESEARCH SPONSORS

Crowe Horwath LLP (www.crowehorwath.com) is one of the largest public accounting and consulting firms in the United States. Under its core purpose of "Building Value with Values®," Crowe uses its deep industry expertise to provide audit services to public and private entities while also helping clients reach their goals with tax, advisory, risk, and performance services. With a total of more than 3,000 personnel, Crowe and its subsidiaries have offices coast to coast. The firm is recognized by many organizations as one of the country's best places to work. Crowe serves clients worldwide as an independent member of Crowe Horwath International, one of the largest global accounting networks in the world, consisting of more than 150 independent accounting and advisory services firms in more than 100 countries around the world.

Crowe Risk Consulting provides internal audit and risk consulting services to organizations around the world. Widely recognized as a thought leader on risk consulting topics, Crowe Risk Consulting dedicates significant resources to developing perspectives and research on risk and governance matters. Crowe is a Principal Partner of The IIA and has donated time and materials to The Institute of Internal Auditors Research Foundation (IIARF) to produce this report.

The Institute of Internal Auditors Research Foundation (www.theiia.org/research) is a not-for-profit corporation whose mission is to shape, advance, and expand knowledge of internal auditing by providing relevant research and educational products to the profession globally.

Since 1975 The IIARF has been building a comprehensive, credible, and accessible repository of practitioner-reviewed content for the internal audit profession. The books and reports published by The IIARF provide forward-thinking research, current best practices, and insight into emerging issues.

To support academic development of the internal audit profession, The IIARF also provides grants and awards for research by students and academic leaders. Finally, every five years The IIARF conducts the Global Internal Audit Survey, which is the world's largest survey of internal auditors (collecting approximately 13,000 responses from more than 100 countries). This data source is used for ongoing research and benchmarking.

EXECUTIVE SUMMARY

Third-party relationships are growing in importance for all types of organizations in all industries. Helping to assess the risks and the controls associated with an organization's relationships with third parties—service providers, distributors, partners, and others—would seem to be a natural role for an internal audit department.

In view of this emerging risk, The Institute of Internal Auditors Research Foundation (IIARF) and Crowe Horwath LLP conducted a study to assess the level of involvement of internal audit in assessing third-party relationships. One goal of the study was to identify the approaches and tools used by organizations and internal audit departments in relation to third-party risk.

A major component of this study was a cross-industry survey of 164 chief audit executives (CAEs) predominantly at organizations in North America. The survey was supplemented by additional research and individual interviews with a number of CAEs.

One overarching conclusion to be drawn from the study is that many large organizations are concerned about their vulnerability to third-party risk. And, despite what would seem to be an obvious role for internal audit in assessing risks and controls associated with third-party relationships, a surprisingly large number of organizations report limited use of internal audit resources in this effort.

The study revealed that more than 65% of the internal audit executives who responded to the survey described their organizations' reliance on third parties as either "significant" or "extensive." An overwhelming majority (82%) said they devote less than 20% of their internal audit resources to assessing third-party risks.

This relative lack of internal audit involvement does not necessarily reflect a lack of concern. More than three-quarters (78%) of the CAE respondents said they had either "some concern" or "high concern" about difficulties with monitoring third parties' risk management practices.

It could be argued that the vulnerabilities the survey revealed are due in large measure to an underlying issue that the survey also addressed: the lack of consensus in the business community about who has clear ownership of third-party risk. When the respondents were asked who has the primary day-to-day responsibility for evaluating and overseeing third-party risk in their organizations, the answers varied widely.

As follow-up interviews with CAEs indicated, the internal audit function must consider expanding its role in assessing third-party risks and controls. With such relationships growing more common—and more complex—third-party risk is clearly a critical factor for all enterprises.

1. INTRODUCTION

Internal auditors are charged with helping their organizations evaluate their capabilities and internal controls. Executives today are demanding more from the internal audit function than ever before in the way of risk identification, assurance, performance improvement ideas, and ways to enhance organizations' abilities to comply with expanding regulations.

The risk profile of most organizations has changed over the past decade. Today, most organizations must deal with fast-paced changes in technology, increased customer expectations, and new and stricter regulations—and do all this in an increasingly global business environment.

Using third parties, which make up a growing network of service providers, often enables organizations to adapt to these changes. Third parties are pervasive in most business models today. Rapid expansion of the supply web, globalization, and regulations further complicate the topic of third-party risk. In addition, relationships and reputation now make up significant portions of the valuation of an organization and its brand.

As third-party risk issues become increasingly problematic for organizations, internal audit departments are also more focused on third-party risks. This report helps to shed light on where the profession is focusing its third-party risk efforts and where internal audit is creating value for its business. This research also yields important perspectives on how internal auditors can play a role in identifying and assessing risk management activities related to third parties.

2. THE BUSINESS CASE FOR INVESTING IN THIRD-PARTY RISK MANAGEMENT

Twenty years ago, the concept of vendor risk management was relatively limited to very large organizations and was focused primarily on the supply chain. Today, organizations of all sizes can take the brunt of the impact from adverse actions of their third-party relationships, resulting in significant impact on their shareholder value. These exposures include:

- **Disruptions.** Supply disruptions have consistently increased since the first supply chain study was performed by the Business Continuity Institute in 2009. These are some findings of a more recent study:
  - Seventy-three percent of respondents experienced at least one disruption in their supply chain in the previous 12 months.
  - Thirty-nine percent of disruptions originated below the immediate tier-one supplier.
  - More than 52% reported the main cause of disruption was IT or telecommunication outages, and 48% reported the main cause as weather.

- Failure of outsourcing suppliers was noted as one of the top three causes of disruption.
- Twenty-one percent of respondents suffered more than €1 million in costs for a single incident.[1]

- **Regulations.** Regulatory impact is an often-cited concern for CEOs today. One of the regulations behind this concern is the Foreign Corrupt Practices Act of 1977 (FCPA). Other anti-corruption regulations around the world augment the concern. The resulting investigations are becoming significant events for many organizations.
  - Investigations resulting in enforcement action for bribery result in significant costs, averaging 5.1% of the market capitalization of the business being investigated. These costs are even higher when fraud is involved.[2]
- **Data Breaches.** Third parties are often key contributors to data breaches. Data also shows that breach remediation costs increase when the breach was caused by third parties or required quick notification of data breach victims, regulators, and others. Below are highlights from a recent study related to breaches that occurred in 2012:
  - In the United States, 41% of breaches were caused by a malicious or criminal attack, 33% by a human error, and 26% by a system error.
  - The average number of breached records per incident in the United States was 28,765.
  - The average total cost per incident to the organization in the United States was $5.4 million, excluding fines.
  - The average breach cost per record was approximately $188. This number varied, depending on the industry.[3]
- **Reputation Damage.** Today's brand is increasingly tied to the collective acts of an organization and its suppliers or service providers. Customers are demanding more of the organizations from which they make purchases. The flow of information results in an almost instant reaction, and the resulting effects of adverse events can be significant.
  - There is an 80% chance of an organization sustaining a loss of at least 20% of its shareholder value (over and above the market) in any month over a five-year period.[4]
  - Reputation equity can sometimes even exceed the book value of an organization and has become an important driver of shareholder value.[5]

3. RESEARCH METHODOLOGY

The major component of this study was a cross-industry survey of 164 CAEs at organizations headquartered in the United States and Canada. The data was gathered in the first quarter of 2013.

Survey participants included members of The IIA's Audit Executive Center, IIA members in general, and contacts made through Crowe business relationships. The industries in which they were employed represented a broad cross-section of the economy, along with a small sample of governmental agencies and not-for-profit organizations.

A sizable portion of the respondents (30%) worked in the financial services sector, and another 9% were in the insurance industry. In instances in which this weighting might have affected the responses to certain survey questions, the responses from financial and non-financial industry respondents are broken out. These instances are noted, as appropriate, in this report.

Other industry sectors with sizable representation among the respondents included manufacturing (10% of respondents), health services (7%), and technology (6%).

The survey population represented organizations of all sizes, with annual revenues ranging from less than $10 million to $10 billion or more. (For financial institutions, respondents were asked to report either the annual revenue or the asset range of their organization, whichever was larger.) By far, the largest group of organizations was in the $1 billion to $10 billion range.

In addition to being asked to provide their size in terms of financial metrics, respondents were asked to describe their organizations in terms of the size of their workforce. Again, medium-size organizations were the most widely represented. The largest group of organizations reported that their workforces ranged in size from 1,001 to 5,000 full-time-equivalent (FTE) employees.

The survey population was composed almost exclusively of high-level executives. More than eight out of 10 (82%) of the individual respondents identified themselves as their organization's "chief audit executive," which was defined as "the most senior auditing officer for the organization with ultimate responsibility for the entire internal auditing function." Another 12% identified with the title "director of audit," which was described as someone who is "authorized to direct a broad, comprehensive program of internal auditing…reporting to the chief audit executive or equivalent." Fewer than 7% described themselves as "audit manager" or another title.

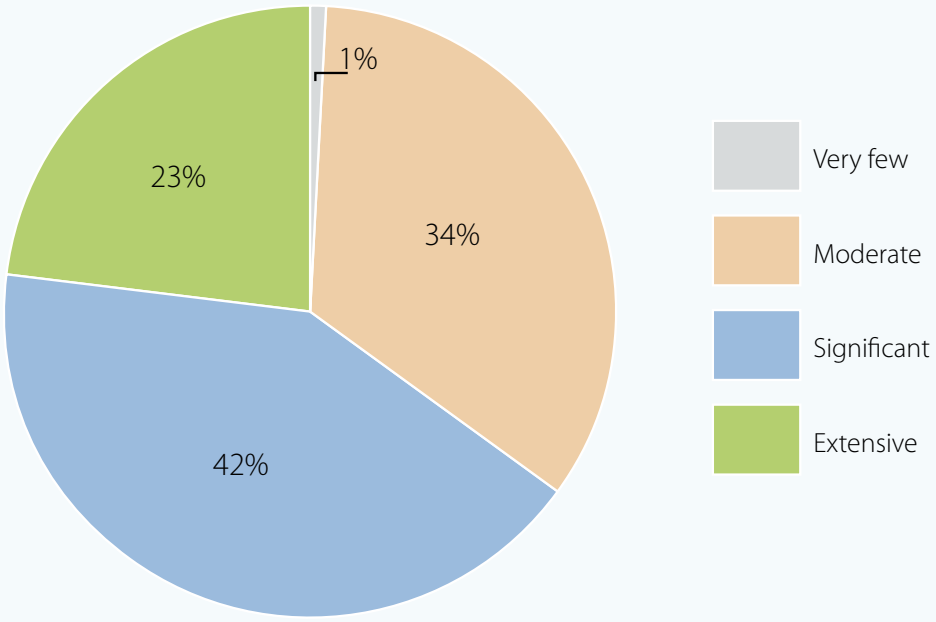
To supplement the survey findings, additional research sources were consulted and are cited in this report where applicable. Please note that the survey data is deemed to be generally representative of the profession, but formal sampling procedures were not used.

4. TRENDS IN THE USE OF THIRD PARTIES

The 2013 survey of internal audit executives by The IIARF and Crowe leaves no doubt about the importance of third-party relationships to today's businesses. More than 65% of the survey respondents described their organizations' reliance on third parties as either "significant" or "extensive." Only one-third described their use of third parties as "moderate," and barely 1% said that their business model uses "very few" third parties (see exhibit 4.1).

Exhibit 4.1. Use of Third Parties

How would you describe use of third parties in your organization?

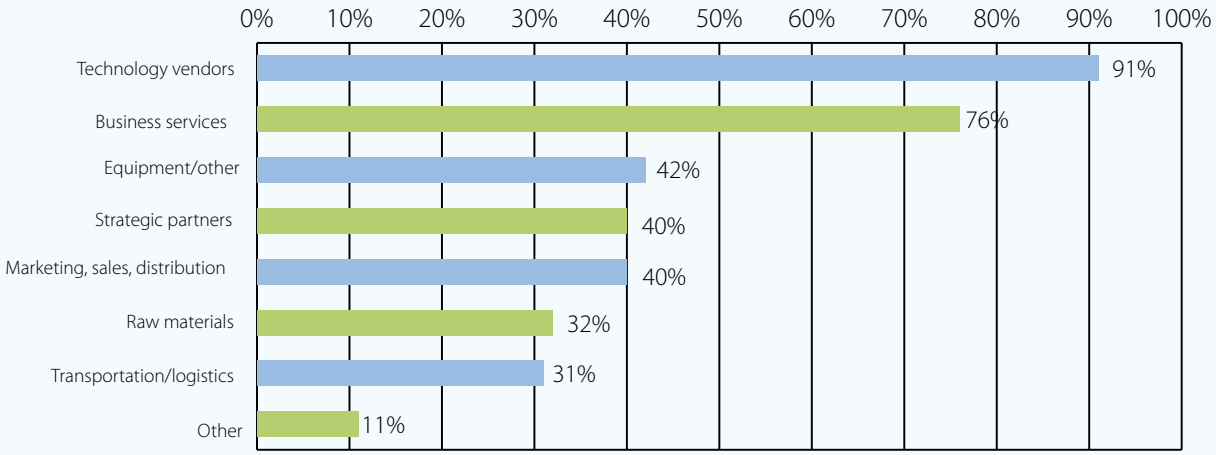


(Question 1)

When asked which types of third parties they used, more than 90% of the survey respondents reported using third-party technology vendors. Three-quarters (76%) said they use third-party providers for high-level business services such as auditing, banking, legal services, and advertising. A sizable number of respondents also reported significant roles for strategic partners such as joint-venture partners or marketing, sales, and distribution-channel partners (see exhibit 4.2).

Exhibit 4.2. Types of Third Parties Used

Which types of third parties are significant in your business model?



(Question 2)

These survey findings are consistent with other recent research about the role of third parties in today's businesses. For example, in a 2012 executive survey conducted for Crowe by CFO Research Services, only 5% of respondents said they "rarely or never" worked or interacted with third parties. A large majority (61%) said they interacted with third parties regularly.[6]

What's more, 40% of the respondents to the CFO Research Services survey said they expected to increase the use of domestically based third parties in the future, while 37% expected to increase the use of internationally based third parties.

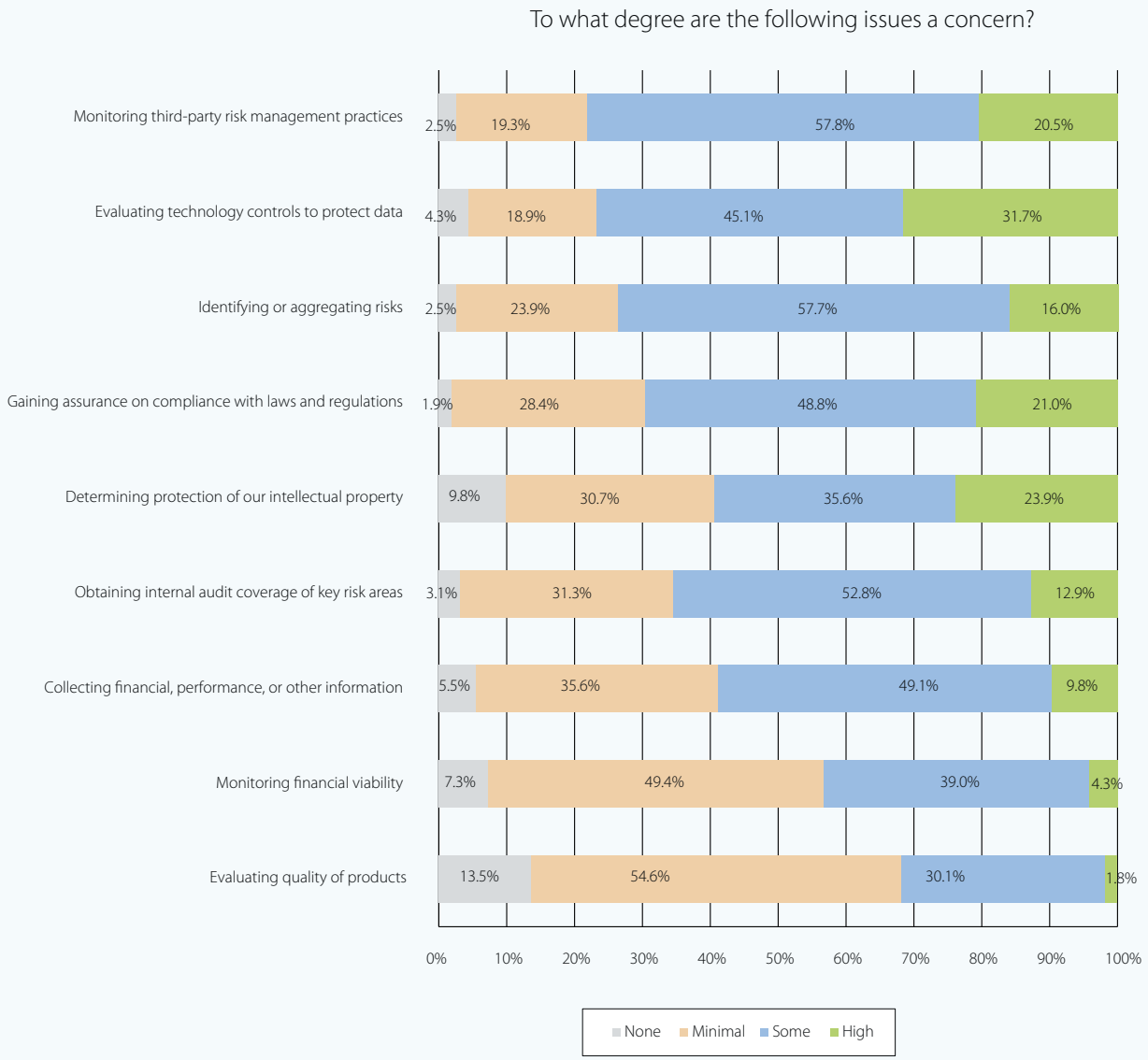
5. THIRD-PARTY RISK MANAGEMENT CONCERNS

In view of the growing role of third parties in many organizations' business models, it is not surprising that the survey respondents expressed significant concern about risk management issues associated with their third-party relationships. More than three-quarters (78%) of respondents said they had either "some concern" or "high concern" about difficulties with monitoring third parties' risk management practices.

Respondents expressed particularly high levels of concern about their ability to evaluate third parties' technology controls for protecting the respondents' organizational data. Almost 77% of respondents said they had either "some" or "high" concern about this issue, including 32% who rated their concern as "high." This was the largest proportion of "high" concern among all the issues raised in this question.

Difficulty with determining how well third parties protect their intellectual property and difficulty with confirming third parties' compliance with laws and regulations were also of "some" or "high" concern to nearly 70% of the executives. On the other hand, more than two-thirds (68%) of the respondents expressed either minimal or no concern about their organizations' ability to evaluate the quality of third-party suppliers' products (see exhibit 5.1).

Exhibit 5.1. Third-Party Issues of Greatest Concern



(Question 4)

The relatively high number of participants from the financial services industry apparently had little effect on the survey results related to this survey question (see exhibit 5.1). Generally speaking, the financial services executives' responses did not vary by more than a few points from those of the overall survey population.

Other contemporary research provides additional insights into the nature of third-party risk. For example, in the CFO Research Services study cited earlier, 97% of survey respondents indicated at least one aspect of their third-party risk management process needed improvement. The largest group (38%) said that improving visibility into the full range of third-party risk exposures was one of their top three priorities.[7]

6. THE ROLE OF INTERNAL AUDIT IN THIRD-PARTY RISK MANAGEMENT

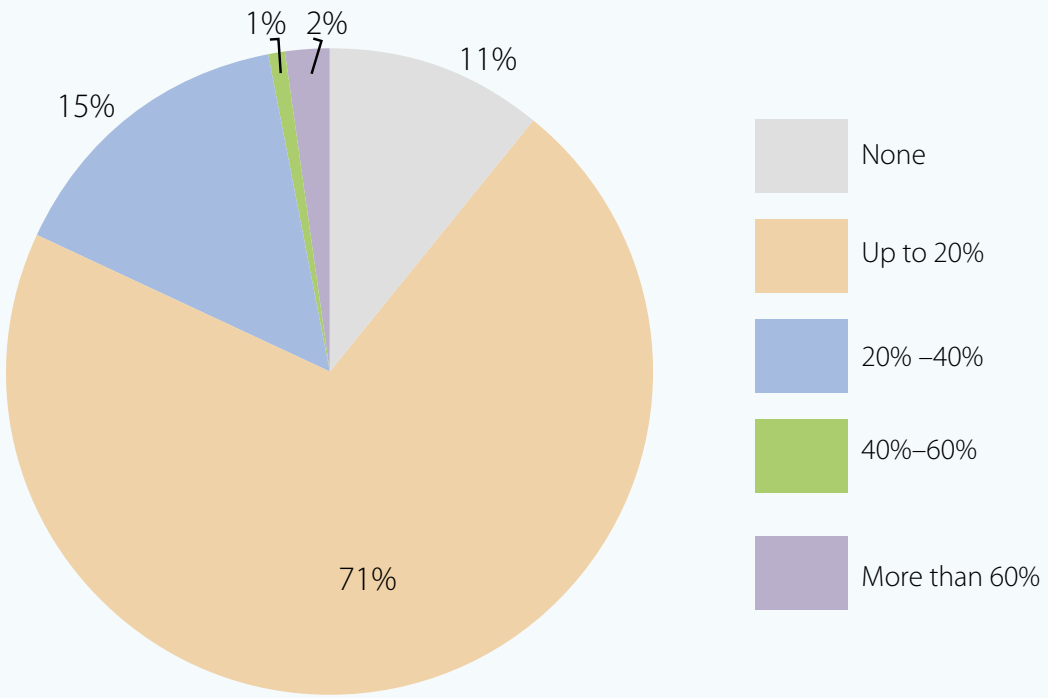
Despite the major role that third parties of all kinds now play in their businesses—and despite their concerns about third-party risk management issues—only a small portion of the surveyed executives said their organizations devote a significant portion of their internal audit resources to auditing third-party relationships.

PUTTING RESOURCES WHERE THE RISK IS

An overwhelming majority—almost 82%—devote less than 20% of their internal audit resources to assessing third-party risks, including 11% who devote no resources at all to this area. Three percent devote more than 40% of their internal audit resources to third-party risk (see exhibit 6.1).

Exhibit 6.1. Internal Audit Resources Spent on Third-Party Risks

What percentage of your organization's internal audit resources (internal and external service providers) is spent on auditing third-party risks?



(Question 3)

The allocation of internal audit effort to third-party risk issues for organizations reporting significant reliance on third parties was almost the same as the allocation of those who indicated that their organization's use of third parties was moderate or it used very few. Twenty-four percent of organizations

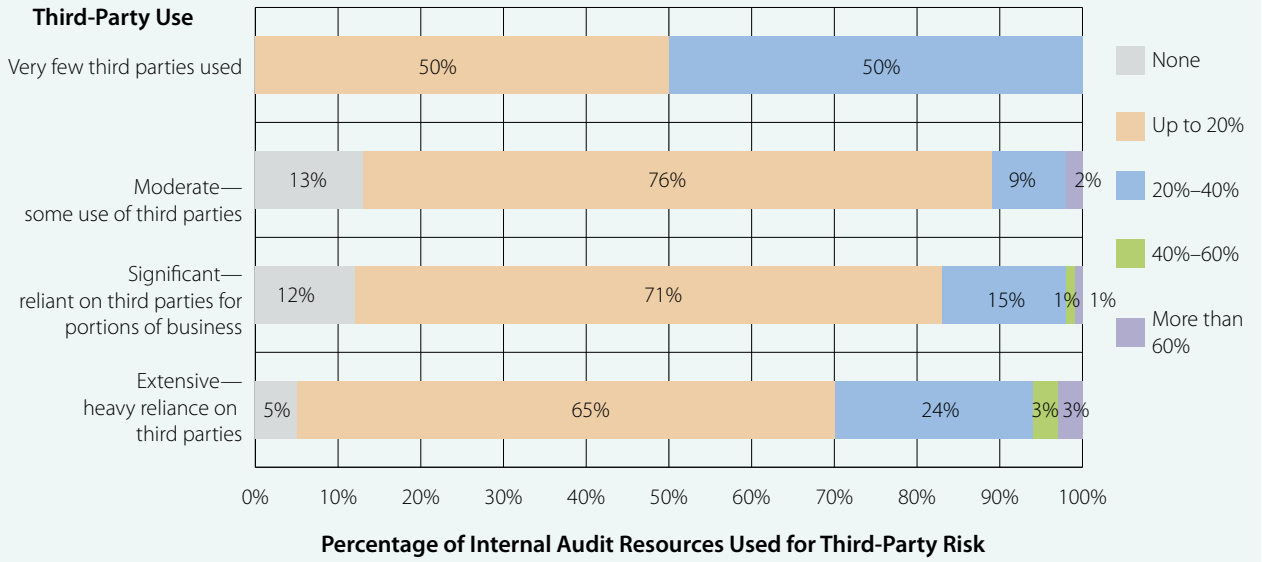
reporting that they rely heavily on third parties spent between 20% and 40% of their internal audit effort on third-party risks (see exhibits 6.2 and 6.3).

Exhibit 6.2. Third-Party Use Compared to Internal Audit Resources Spent on Third-Party Risk

Internal Audit Resources Spent on Third-Party Risk	Use of Third Parties			
	Extensive (heavy reliance) n = 37	Significant (reliant for portions of business) n = 69	Moderate (some use) n = 55	Very Few Third Parties Used n = 2
None	5%	12%	13%	0%
Up to 20%	65%	71%	76%	50%
20%–40%	24%	15%	9%	50%
40%–60%	3%	1%	0%	0%
More than 60%	3%	1%	2%	0%
Subtotals	100%	100%	100%	100%

(Questions 4 and 15)

Exhibit 6.3. Bar Chart of Third-Party Use Compared to Internal Audit Resources Spent on Third-Party Risk



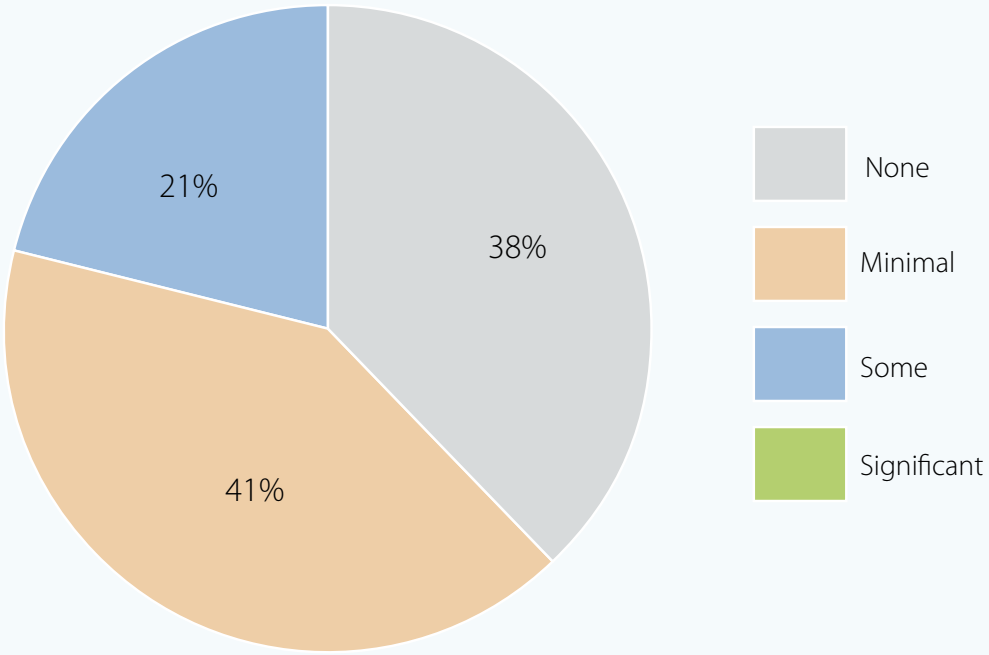
(Questions 4 and 15)

INTERNAL AUDIT'S INVOLVEMENT IN THE DECISION MAKING FOR THIRD-PARTY RELATIONSHIPS

The majority of internal audit executives indicated that their departments have little involvement in the decision to establish or renew third-party relationships. About 41% described their involvement as "minimal," and 38% said they had no role at all (see exhibit 6.4). While internal audit should not be making decisions about whether or not to create third-party relationships, internal audit could offer significant value by educating and advising decision-makers on the potential risks.

Exhibit 6.4. Internal Audit Involvement in Decisions to Create Third-Party Relationships

What is the level of involvement of internal audit in the decision-making process for the creation of a third-party relationship at your organization?



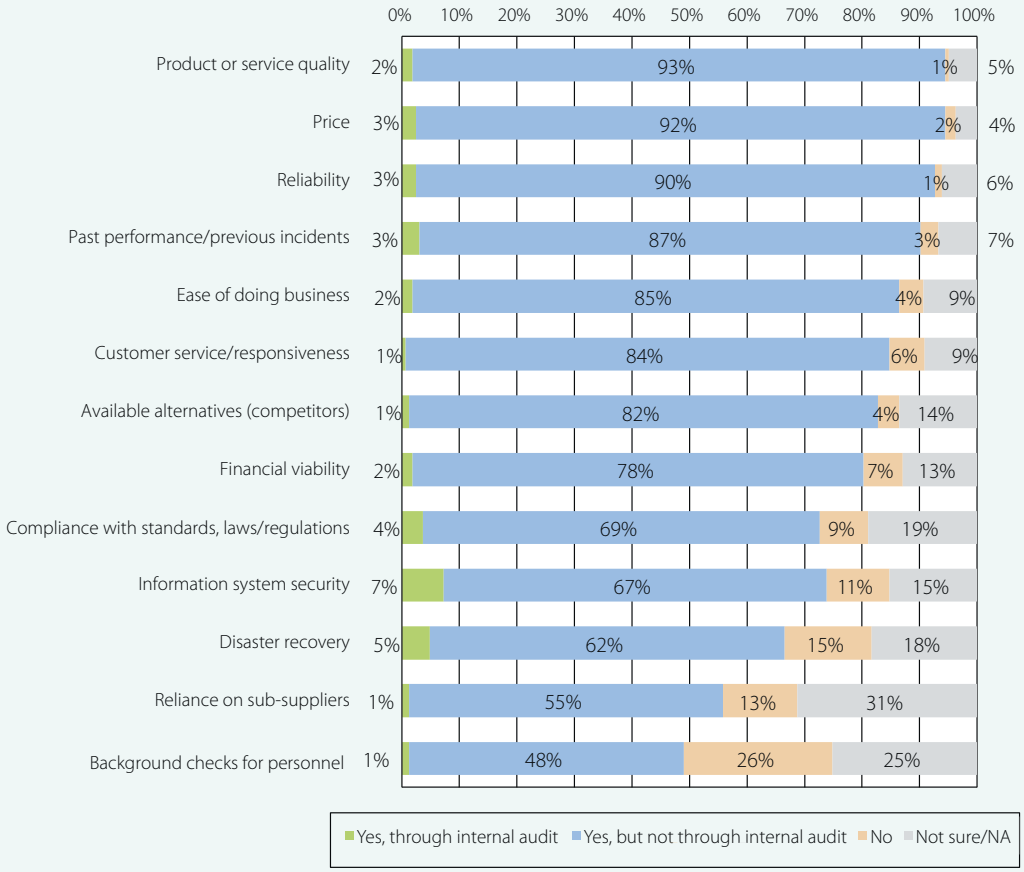
(Question 6)

PREVALENCE OF THIRD-PARTY CONTROLS AND RISK MANAGEMENT ACTIVITIES

The limited involvement of internal audit in assessing risks associated with new third-party relationships is reflected in other survey responses. For example, when asked if their organizations considered a third party's ability to comply with standards, laws, and regulations before contracting with them, more than a quarter (28%) answered either "no" or "not sure." In addition, more than a third answered "no" or "not sure" when asked if their organizations considered third parties' disaster recovery capabilities (see exhibit 6.5).

Exhibit 6.5. Factors Considered When Selecting or Renewing Third-Party Relationships

When selection or renewing a third-party relationship, what factors does your organization consider and by what means?



(Question 9)

Moreover, even after a contract with a third party is signed, the survey indicates that internal audit plays only a secondary role in most aspects of risk management. The survey participants were asked about their organizations' practices as they relate to a range of basic risk management functions. According to the survey responses, internal audit generally plays a leading role in only one of these functions—evaluating reports required by Statement of Standards for Attestation Engagement No. 16 (SSAE 16)/SOC reports. Thirty-seven percent of the respondents cited internal audit as the primary actor in this activity (see exhibit 6.6).

Thirty-two percent said internal audit was responsible for periodically auditing or obtaining assurance related to compliance with agreements, but an even larger number (36%) said primary responsibility for this task resided elsewhere in their organizations. Surprisingly, 25% of the respondents said their organizations do not audit compliance with agreements at all.

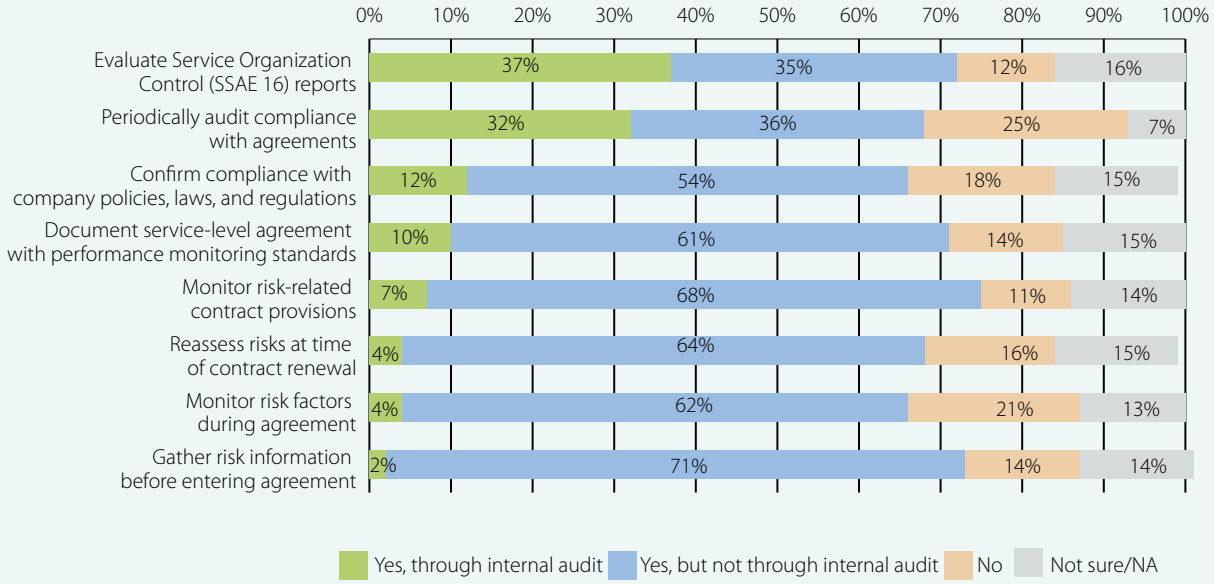
The only other areas in which a significant number of respondents attributed responsibility to internal audit were (1) confirming compliance with organizational policies, laws, and regulations; and (2) verifying the existence of a service-level agreement with performance monitoring standards. In both

of these instances, however, a far larger proportion of respondents assigned responsibility for these activities to departments other than internal audit.

The important role that internal audit should play in managing third-party risk has also been the subject of significant commentary in professional circles. For example, a recent article in *Compliance Week* notes that organizations "often fail to proactively account for issues that can occur throughout the relationship cycle. Because there are many different types of third parties, each managed by a distinct department…internal audit with its understanding of company operations is in an excellent position to consolidate the process."

The article goes on to note that "internal audit's expertise can assist in examining and developing relationship criteria in order to judge the level of compliance measures and oversight that is required." The author concludes, "Managing third-party risk is becoming a critical success factor for all enterprises. Internal audit should be looked to as a resource to help build a vendor risk management program."[8]

Exhibit 6.6. Normal Practice Related to Third Parties



(Question 8)

7. WHO OWNS THIRD-PARTY RISK?

It could be argued that the vulnerabilities discussed in the preceding pages stem in large measure from a more fundamental issue that appears to be common among many of the survey respondents: a lack of clarity and consistency about who is ultimately responsible for managing third-party risk. Or, to put it more simply, "Who owns the risk?"

When asked who has the primary day-to-day responsibility for evaluating and overseeing third-party risk in their organizations, the answers varied widely. While the individual "business unit or functional leadership" was the most frequent response, it was far from a consensus choice, cited by only 32% of respondents. Other frequent responses were "corporate leadership" and "the procurement function."

Significantly, only 6% affixed the ownership of third-party risk to a centralized enterprise-wide risk function (see exhibit 7.1).

Exhibit 7.1. Responsibility for Third-Party Risks

Who has primary day-to-day responsibility for evaluating and overseeing third-party risk?

Organizational Area	All Respondents n = 164	Financial Sector n = 47
Business unit/functional leadership	32%	40%
Individual business unit or operational managers	20%	9%
Decentralized risk management in the business unit	14%	17%
Not clearly defined	12%	4%
Procurement	7%	0%
Centralized, enterprise-wide risk management	6%	17%
Other	5%	9%
Corporate leadership	4%	4%
Don't know	1%	0%
Internal audit	0%	0%
Total	100%	100%

(Question 10)

In this area, the responses from participants in the more heavily regulated financial services industry varied somewhat from the overall population. For example, more than 40% of financial services executives said primary day-to-day responsibility for third-party risk belongs to the business unit or functional leadership, compared to about 32% of the overall population who responded this way (see exhibit 7.1).

On the other hand, only 9% of financial industry respondents assigned responsibility to individual managers at the business unit or operational level, compared to 20% of the overall population. It seems reasonable to assume that such variations generally reflect the more highly regulated nature of the financial services industry, which in turn has led many institutions to develop relatively more mature third-party risk management programs.

"Who owns the risk?" is a question that also arises in other research studies, with results that are somewhat comparable. For example, in the 2012 CFO Research Services study cited earlier, survey respondents were close to equally divided on the question of who has primary, day-to-day responsibility for evaluating and managing third-party risk. Forty-six percent chose responses that indicated a centralized responsibility, while 45% of the responses indicated a decentralized responsibility.[9]

8. LOOKING AHEAD

So that the broadest possible range of insights could be gathered, survey respondents were given the opportunity to offer additional, unprompted comments. These comments are extremely useful in providing indications of the direction the profession might go in the next few years.

For example, one survey respondent noted, "Our CIO has primary responsibility. However, we are migrating that to business unit managers to ensure they take responsibility for their vendors." Another noted, "This is a new area in our company that is now finally getting visibility."

The role of internal audit in monitoring risk in general—and contract compliance in particular—was described by one survey participant, who wrote, "Our internal audit group facilitates (an) ongoing risk-based review process to help ensure the program is functioning and to assist business unit management with assistance. We also work with our IT security manager who is involved with assessing IT risk associated with vendors as well."

Another went into greater detail: "Concessionaires are required at their own expense to provide a certification of gross receipts (as defined in their agreement) by an independent CPA firm. However, internal audit more often than not finds additional recoveries. Interest is charged on such amounts due to us."

Yet another respondent described a more technology-driven approach to the issue: "We have a software application that helps us track vendor relationships. It offers a risk assessment for due diligence when entering into a vendor relationship and for periodic assessments of the vendor relationship. The software tracks contract renewals and also tracks the frequency of the periodic assessments. Internal audit reviews the vendor relationship during audits of each business unit." The situation was summed up concisely by another participant who wrote, "There is no consistent approach across the board for all third parties."

INTERNAL AUDIT'S ROLE

Roles and expectations vary with each audit committee and management team. That said, the data suggests that in many organizations there is a bigger, more important role that internal audit departments can play. The business case for this role has to be built on the skills of the team (risk management, risk aggregation, controls, inspection audit and assurance, and process improvement).

Following are nine areas where internal audit might be able to provide significant value:

1. Assist management with identifying the third-party risk universe and risk ranking.
2. Identify, quantify, and assess the risks to the organization that arise out of third-party relationships.
3. Identify or evaluate management's understanding of how third parties comply with regulations or policies that should be in place.
4. Evaluate the third-party risk management activities in place at the organization and the relative maturity of the third-party risk management program related to the risk exposures in the organization.

5. Compare third-party risk management approaches to those used in the organization's enterprise risk management (ERM) program.
6. Determine the adequacy and effectiveness of assurance activities.
7. Perform testing for compliance with agreements and regulations or policies.
8. Confirm service-level agreements are being met.
9. Identify process improvements for third-party interactions.

Each of these areas provides an opportunity for the internal audit function to provide an objective point of view on how well third-party risks are being managed. And each may have a different level of interest or importance, depending on the nature of the organization's unique risks and external relationships.

CONCLUSION: EVALUATING THIRD-PARTY RISK MATURITY

The data suggests that there are opportunities for improvement in managing third-party risks. As organizations look to improve their capabilities, often the first place to start is understanding where the organization is today so that strategies can be developed to move to a more mature process (if required). Appendix A provides a third-party risk maturity model tool to help organizations with this evaluation. Regardless of the levels of maturity, third-party risk management activities should be clearly tied to the overall risk management program of the organization.

APPENDIX A: A THIRD-PARTY RISK MANAGEMENT CAPABILITY MATURITY MODEL

One useful method for assessing an organization's risk management capabilities is through the use of a conventionally structured capability maturity model.[10] The tool allows an organization to perform an objective assessment of risk management methods and processes and can help the organization define its goals for the future.

The attributes that are assessed range from overall program breadth and strategy for third-party risk to more specific features such as governance, assessment methods, and communication.

Using a variation of the Third-Party Risk Management Capability Maturity Model as shown on the following page can be helpful at the third-party risk management program level, by third-party category, business unit, and the like because not all third parties or business processes require the same level of maturity.

Exhibit A.1. Third-Party Risk Management Capability Maturity Model

Third-Party Risk Program Component	Initial	Repeatable	Defined	Managed	Optimizing
Governance and Organization	• Minimal coordination • Little to no governance or oversight • Lacking standards and methods	• Limited senior management commitment to standard practices related to third parties • Organizational awareness that controls are needed around third-party risk	• Policies are established • There is a formal organization for managing the risks of third parties (committee, central group, executive leader, etc.) • Defined escalation processes • Meaningful board involvement for high-risk areas	• Risk management activities are embedded in operational processes • Third-party risk is quantitatively managed across business functions • Monitoring is performed at the business unit and enterprise level	• Third parties are continually evaluated through the organization • Resources allocated as needed to address third-party objectives or emerging risks • High level of cross-functional coordination in monitoring risks
Risk Identification and Assessment	• Activities are not linked to the organization's ERM framework • Differing tolerances and risk assessment levels • Limited perspective of risk levels across the organization	• Specific activities are in place to assess risk, although they may differ across the organization	• Periodic reporting and oversight of risk management activities • Formal methods for aggregating and monitoring risk profiles of third parties are in place • There is a common approach at the enterprise level with consistent risk ratings • Processes for managing third-party risks are incorporated in standard business processes	• Internal benchmarking/metrics are available to evaluate and monitor key third parties and related risk areas	• Advanced indicators of red flags • Benchmarking with peers as needed • Calculated risk taking or reduction activities • Risk factors embedded into decision making on overall third-party relationship
Assurance Activities	• Little or no assurance on third-party risk matters • Differing assurance approaches across the organization	• Prescribed assurance activities are in place for key third parties, although the approach may not be consistent	• Formal enterprise approach to identifying and assessing third parties, based on risk	• Trends are monitored and improvements addressed across the third-party portfolio • Periodic assurance activities tied to risk levels and tolerances	• Real-time monitoring or automation of compliance activities • Assurance and ultimately reliance on the third party's own risk management activities

APPENDIX B: SURVEY RESPONDENT DEMOGRAPHICS

Exhibit B.1. Annual Revenue of Survey Respondents' Organizations (Non-Financial Services), USD

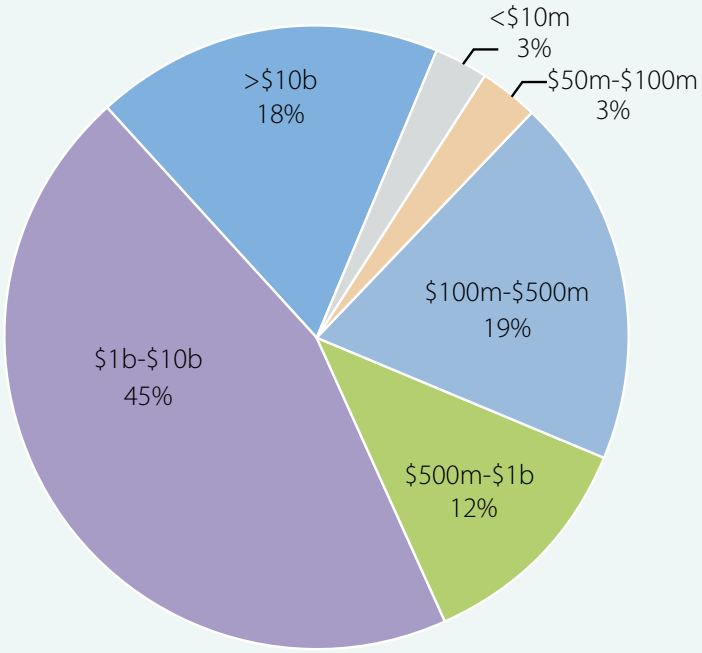


Exhibit B.2. Total Assets of Survey Respondents' Organizations (Financial Services), USD

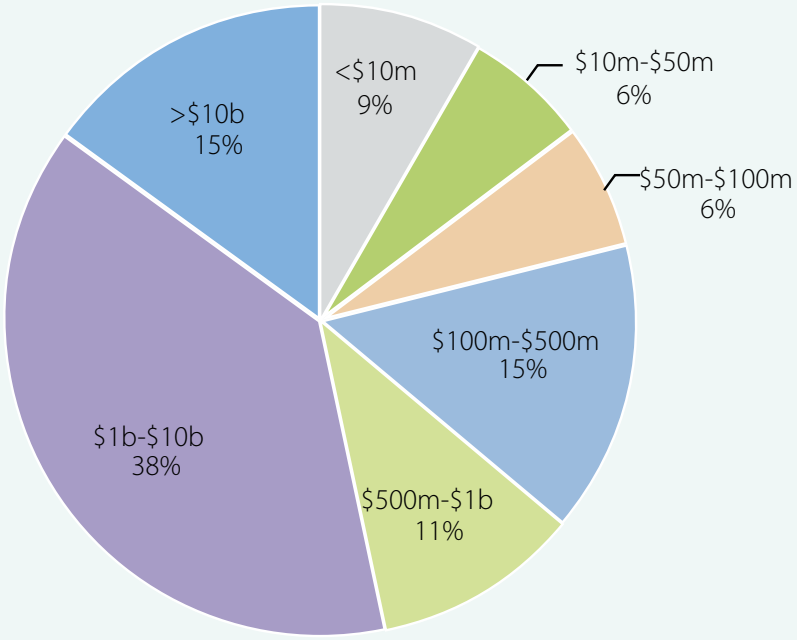


Exhibit B.3. Number of Employees (FTEs) of Survey Respondents' Organizations

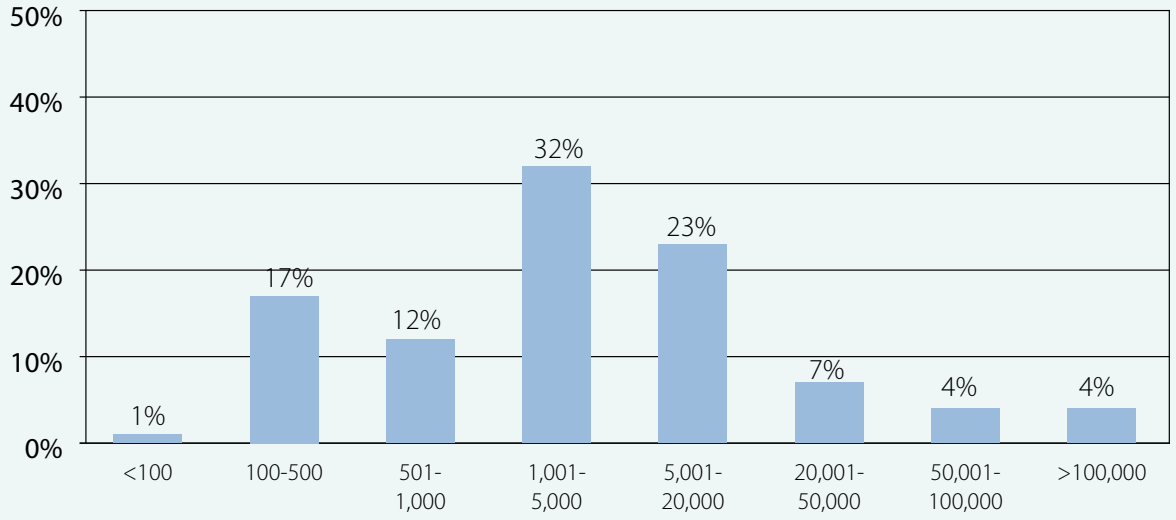
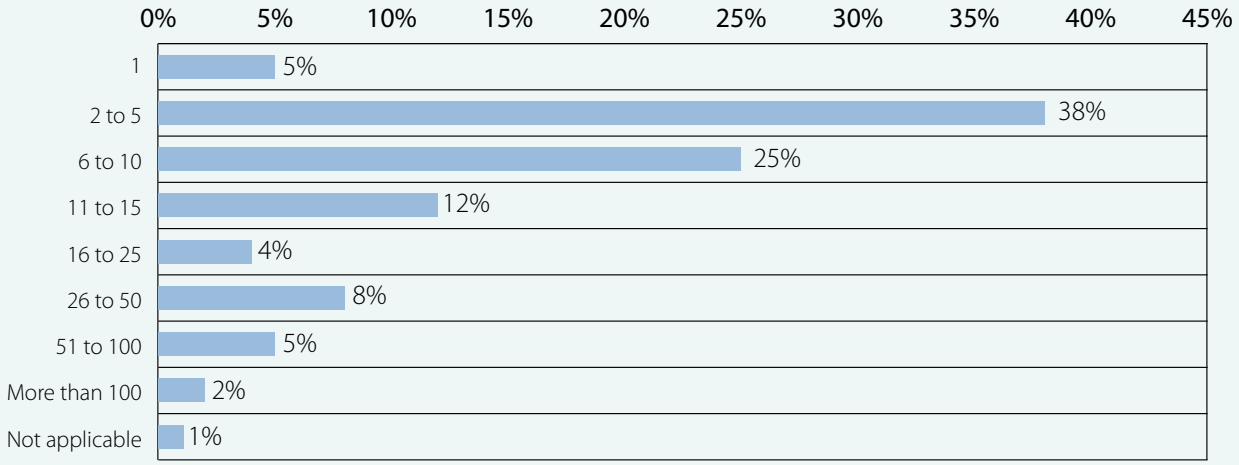
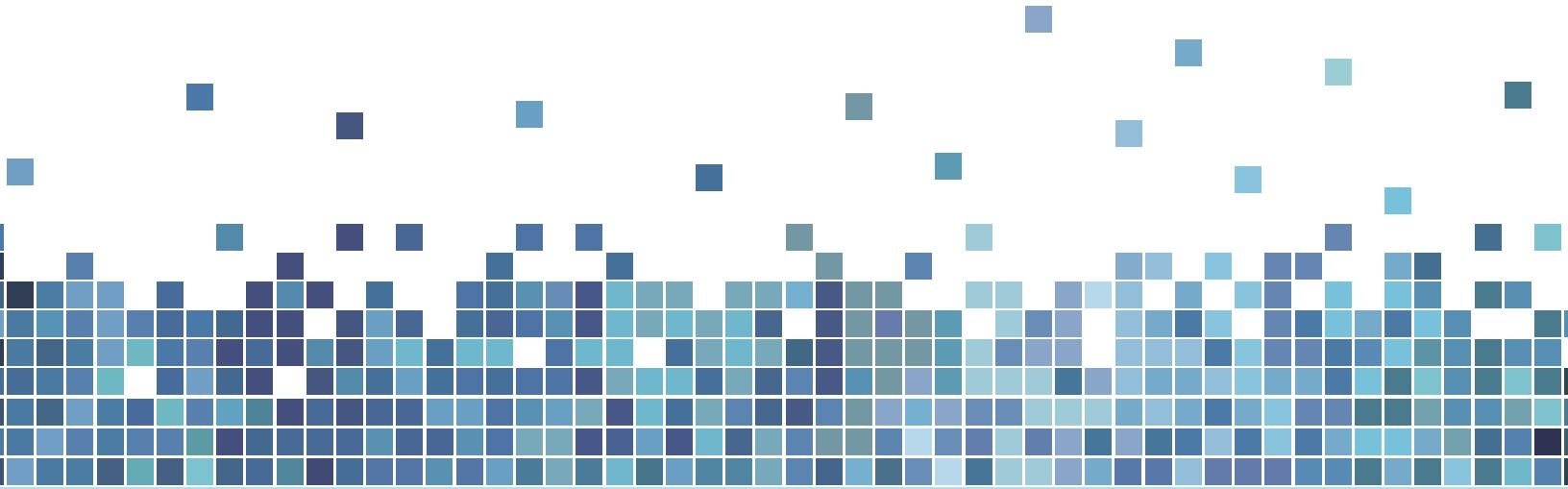


Exhibit B.4. Number of FTEs in the Respondents' Internal Audit Functions



NOTES

1. "Supply Chain Resilience 2012," November 2012, Business Continuity Institute, http://www.thebci.org/index.php/supply-chain-resilience-survey-2012.
2. Jonathan M. Karpoff, D. Scott Lee, and Gerald S. Martin, "The Economics of Foreign Bribery: Evidence from FCPA Enforcement Actions," July 29, 2013, available at SSRN: http://ssrn.com/abstract=1573222 or http://dx.doi.org/10.2139/ssrn.1573222
3. "2013 Cost of Data Breach Study: Global Analysis," research sponsored by Symantec, May 2013, Ponemon Institute, https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf
4. "Oxford Metrica Reputation Review 2012," a joint project of Oxford Metrica and Aon, http://www.aon.com/attachments/risk-services/Aon-OM-Reputation-Review-2012.pdf
5. Ibid.
6. "Working Well Together: Managing Third-Party Risk in a More Integrated World," April 2012 research study by CFO Research Services and Crowe Horwath LLP, p. 4, http://www.crowehorwath.com/ContentDetails.aspx?id=4473
7. Ibid, p. 11.
8. Jose Tabuena, "Internal Audit's Role in Managing Third-Party Risks," *Compliance Week*, March 12, 2013, http://www.complianceweek.com/pages/login.aspx?returl=/internal-audits-role-in-managing-third-party-risks/e/283019/&pagetypeid=28&articleid=283019&accesslevel=2&expireddays=0&accessAndPrice=0
9. "Working Well Together," p. 14.
10. The Capability Maturity Model was developed by Carnegie Mellon University to define the level of maturity in a process.



The Institute of Internal Auditors
Research Foundation

www.theiia.org/research