



From Cybersecurity to IT Governance – Preparing Your 2014 Audit Plan

Assessing the Results of Protiviti's Third Annual IT Audit Benchmarking Survey

Powerful Insights. Proven Delivery.®

protiviti[®]
Risk & Business Consulting.
Internal Audit.

Table of Contents

- Introduction2**
- Top Technology Challenges Faced by Organizations 3**
- IT Audit in Relation to the Internal Audit Department.....6**
 - Existence of IT Audit Function and Leader6
 - Resourcing.....8
 - Reporting 10
 - Key Questions to Consider for Your Audit Plan 11
- Assessing IT Risks.....12**
 - Conducting an IT Audit Risk Assessment 12
 - Organizational Engagement/Involvement..... 13
 - Frameworks..... 15
 - Key Questions to Consider for Your Audit Plan 16
- Audit Plan17**
 - Focus of IT Audit Hours 17
 - IT Governance.....20
 - Key Questions to Consider for Your Audit Plan 21
- Skills and Capabilities22**
 - Gaps in IT Audit Plan22
 - Key Questions to Consider for Your Audit Plan.....23
- Methodology and Demographics.....24**
- About Protiviti.....26**

Introduction

Information technology challenges – from controls, security and infrastructure to global cyber threats – are top-of-mind for organizations today. Certainly, companies have become dependent on the continued availability, accuracy and confidentiality of their information and communications technologies. While it delivers significant benefits, technology has also enabled risks to be more prevalent in new and more subtle ways, and cybersecurity, for example, is now being discussed by virtually every board of directors. With growing government emphasis globally on fortifying cybersecurity measures and managing other IT risks, it is critical that companies have a strong IT security framework in place, along with a robust IT compliance and IT assurance function.

However, the results of our third annual IT Audit Benchmarking Survey show that organizations continue to leave themselves significant room for improvement in their IT audit programs and practices. To put it simply, a large percentage of organizations are not planning and instituting the IT audit coverage necessary to ensure an available, secure and efficient IT environment.

Key findings from our study show that:

Data security is of paramount concern – More than ever, there is greater scrutiny today on cybersecurity and threats from more sources than ever previously known. Many research studies, including Protiviti's annual IT Priorities survey, rank IT and data security at the top of the list of challenges.¹ Organizations should be looking to expand IT audits as one component of a broadening net of assurance to evaluate the design and operating effectiveness of management's security risk assessment, system of controls and monitoring of the environment.

Organizations are not gaining the audit coverage they need – Organizations do not have adequate IT audit resources, and these resources are not always a formal part of the audit group. By seemingly shortchanging themselves on the resources they devote to IT audit efforts, companies are limiting their ability to create transparency into how they adequately identify and manage their IT risks. Furthermore, limited IT audit resources become a significant problem when considering that nearly every function in organizations today, from accounting and finance to supply chains and sales, is technology-enabled.

There remain major shortcomings in IT audit risk assessments – Not enough companies are performing IT audit risk assessments on a regular basis, nor are they updating these assessments as frequently as they should. The likely result is that critical IT components and process areas supporting the business are not being reviewed sufficiently.

More organizations are implementing strong IT governance programs and practices – This is a positive development, particularly given the ranking of IT governance as a top IT challenge for organizations. The new COSO Internal Control – Integrated Framework emphasizes the importance of strong IT governance and controls, underscoring the dynamic nature of technology in business today.²

These findings and their implications should be considered as part of an organization's annual audit plan. We hope this report serves as a helpful guide and asset to internal audit functions, audit committees and boards of directors as they build their annual audit plans. We want to thank the more than 460 chief audit executives, IT audit directors, IT audit managers, and other auditing professionals who participated in our study. Upon request, we can provide more detailed breakdowns of the results by industry or company size.

Protiviti
November 2013

¹ 2013 IT Priorities Survey, Protiviti, 2013, www.protiviti.com/ITpriorities.

² For additional information, visit www.coso.org, or read Protiviti's guide, *The Updated COSO Internal Control Framework: Frequently Asked Questions*, available at www.protiviti.com.



Top Technology Challenges Faced by Organizations

We asked our survey participants, in a verbatim question, to name the top technology-related challenges that their organizations face. This year's list was a combination of new and repeat issues from 2012.

2013	2012
IT security: data security, cybersecurity and mobile security	Information security (including data privacy, storage and management)
IT governance	Cloud computing
Lack of successful ERP implementations, development and knowledge	Social media
Social media	Risk management and governance
Vendor management	Regulatory compliance
Cloud computing	Technology integration and upgradation
Emerging technology and infrastructure changes	Resource management
Big data and analytics	Infrastructure management
PCI compliance	Fraud monitoring
	Business continuity/disaster recovery

As audit plans are developed, these technology challenges (which we discuss below in further detail) should also be top-of-mind for internal audit. Executives have communicated these same challenges in other Protiviti surveys, including those in which we've polled board members and C-suite executives, thus it appears that management and auditors are in sync, which is a positive trend.³

³ For more information, read these Protiviti research reports:

- 2013 Internal Audit Capabilities and Needs Survey, www.protiviti.com/IASurvey.

- 2013 IT Priorities Survey, www.protiviti.com/ITpriorities.

- Executive Perspectives on Top Risks for 2013 (from North Carolina State University's ERM Initiative and Protiviti), www.protiviti.com/TopRisks.

IT security: data security, cybersecurity and mobile security

Protiviti's 2013 IT Security and Privacy Survey details the concerns organizations have when it comes to security (e.g., lack of key data policies, less-than-ideal data retention and storage, and being unprepared for crises).⁴ Earlier this year, the U.S. federal government formally acknowledged the importance of IT security by issuing an executive order calling for increased cybersecurity for the country's critical infrastructure. (Of note, virtually every top technology challenge identified by our respondents has a security component.) In addition, organizations are beginning to address recently released updates to the ISO/IEC 27001 and 27002 information security standards, which go into effect in 2015.⁵ Internal auditors should stay abreast of these developments and formulate plans to address IT security risk within the IT audit risk assessment process.

IT governance

The importance of IT governance is documented in IIA Standard 2110.A2. Of note, respondents to our 2012 IT Audit Benchmarking Survey reported that IT governance was not a priority for their organizations. It is both positive and understandable to find that it now ranks near the top of their list of challenges. At first glance, it can seem daunting to know specifically how to assess IT governance risk. A good starting point is to understand what governance is and how internal audit contributes to a strong governance structure. From there, auditors can ensure alignment between business objectives and IT operations and projects, and subsequently determine if this alignment is defined properly in the strategic plan.

Lack of successful ERP implementations, development and knowledge

As stated in Protiviti's white paper, *How to Select an ERP System*, the success or failure of an ERP implementation is not predicated on the characteristics of the software package.⁶ Frequently, failure ensues with the rush to select and implement a new ERP system. Internal audit can help organizations manage this risk by being brought in at the start of the project. Auditors can evaluate the system requirements, determine whether project management protocols are in place and operating, evaluate the governance of and involvement in the project by key stakeholders, and test internal controls that are designed into the process. This can help lead to higher success rates and achieve a level of automation that maximizes operational efficiency.

Social media

Not surprisingly, social media is on the minds of people globally regardless of industry, size of organization or position title. This is evident in the results of two Protiviti studies. Our 2013 IT Priorities Survey articulates how IT departments are investing significant time and resources to support social media. And participants in our 2013 Internal Audit Capabilities and Needs Survey clearly expressed the importance of auditing this dynamic communication medium.

Vendor management

Vendor management risk was also a key challenge that emerged from the results of our 2013 IT Priorities Survey. Complex outsourcing, offshoring and compliance requirements are increasing the importance of strong vendor management practices within organizations. With outsourcing and offshoring, the level of risk rises, which should grab the attention of internal auditors.

⁴ *Knowing How – and Where – Your Confidential Data Is Classified and Managed*, Protiviti, 2013, www.protiviti.com/ITsecuritysurvey.

⁵ For more information, read Protiviti's *IT Flash Report*, "Security Standards ISO/IEC 27001 and 27002 Have Been Revised: What Are the Significant Changes?," dated October 17, 2013, available at www.protiviti.com.

⁶ *How to Select an ERP System*, Protiviti, 2012, www.protiviti.com.

“[WE ARE] HIGHLY UNDERSTAFFED AND NOT READY FOR EMERGING RISKS. [OUR IT AUDIT RISK ASSESSMENT] IS DONE ON A GOOD-FAITH BASIS AND CONCENTRATES MORE ON INFRASTRUCTURE SECURITY.”

— AUDIT STAFF, MIDSIZE MEDIA COMPANY

Cloud computing

The allure and appeal of cloud computing has been well-documented. The cloud opens the door for IT but also comes with IT risks that must be managed. Because this is a path more organizations are taking, internal audit should examine how the organization is impacted from a security, privacy and continuity perspective.

Emerging technology and infrastructure changes

With the presence of social media, cloud computing and mobile devices, it makes sense that emerging technologies and infrastructure changes are top-of-mind for IT auditors. IT departments must invest time and energy to accommodate modern technology. In turn, auditors must incorporate into the audit plan the activities and time needed to assess how the pace of IT change is influencing the risks posed to the organization.

Big data and analytics

As data warehouses grow, bigger data must be classified and protected according to its classification. Participants in our 2013 IT Priorities Survey also identified this area as a top priority, and data analysis surfaced in our 2013 Internal Audit Capabilities and Needs Survey as an area requiring improvement. This is understandable as organizations continue to focus on how to control and classify data. Internal audit should play a key role in helping management assess and manage data-related risks.

PCI compliance

The Payment Card Industry Data Security Standard (PCI DSS) is maturing further and becoming more widely adopted across the globe. This priority goes hand-in-hand with respondents' concerns about IT security, virtualization and emerging technologies, as all have roles in the security of customer payment information. This challenge will become even greater for organizations as PCI DSS Version 3.0 is rolled out in 2014.⁷

⁷ For more information, read Protiviti's *IT Flash Report*, "Understanding PCI DSS Version 3.0 – Key Changes and New Requirements," dated November 8, 2013, available at www.protiviti.com.



IT Audit in Relation to the Internal Audit Department

Existence of IT Audit Function and Leader

This year's survey results are comparable to our 2012 study. While the relative stability in our findings is encouraging (i.e., no significant declines in the existence of an IT audit function), overall it is apparent that many organizations are still lacking this critical component of internal audit, especially small and midsize organizations that are clearly grappling with getting their IT audit functions in place.

In fact, there was a 14 percent year-over-year decrease in the number of small companies that have an IT audit function in place, which raises the question of whether these organizations are focusing enough on their IT risks.

Does an IT audit function exist within your internal audit function?

	2013		2012	
	Yes	No	Yes	No
Company Size (Annual Revenue)				
Greater than \$5 billion	90%	10%	91%	9%
\$1 billion - \$4.99 billion	74%	26%	77%	23%
\$100 million - \$999.99 million	60%	40%	61%	39%
Less than \$100 million	55%	45%	69%	31%
Region				
Americas	74%	26%	77%	23%
EMEA/APAC	70%	30%	73%	27%

Do you have a designated IT audit director (or equivalent position)?

	2013		2012	
	Yes	No	Yes	No
Company Size (Annual Revenue)				
Greater than \$5 billion	52%	48%	56%	44%
\$1 billion - \$4.99 billion	36%	64%	25%	75%
\$100 million - \$999.99 million	32%	68%	23%	77%
Less than \$100 million	27%	73%	31%	69%
Region				
Americas	40%	60%	34%	66%
EMEA/APAC	35%	65%	31%	69%

Given the high level of scrutiny on a broad array of IT issues and challenges today, it is remarkable to find that as many as 73 percent of organizations do not have an IT audit director in place or someone in an equivalent role whose primary focus is auditing technology risks. On the positive side, as expected, a greater percentage of larger companies have an IT audit director, and there is a notable year-over-year increase among organizations at the US\$100 million to US\$5 billion levels with an IT audit director, as well as among organizations in the EMEA/APAC regions.

Interestingly, when reviewing the findings for public companies (data not shown), the results are more positive, but not dramatically so. On average, across all revenue levels, there is just a 4 percent increase in the number of publicly held firms that have an IT audit director. This is a bit surprising given the increased inherent risk profile of public companies.

To whom within the organization does your IT audit director report?*

	Americas		EMEA/APAC	
	2013	2012	2013	2012
CAE	75%	73%	57%	69%
A director under CAE	10%	19%	29%	27%
CIO	5%	1%	11%	4%
Report through some other compliance function	10%	7%	3%	0%

*Respondents are those organizations that have a designated IT audit director (or equivalent position).

In organizations based in the Americas, three out of four organizations (75 percent) have a good structure in place, in that it is advisable to have the IT audit director report to an independent executive such as the CAE. This is very consistent with last year's results. However, as we've noted in our previous reports on this study, it is not advisable for the IT audit director to report into the CIO because independence and objectivity of assessments is lost. Even though the overall number of organizations with such a reporting structure is low, that number is still too high, and there was significant year-over-year growth among organizations that have this reporting relationship in place.

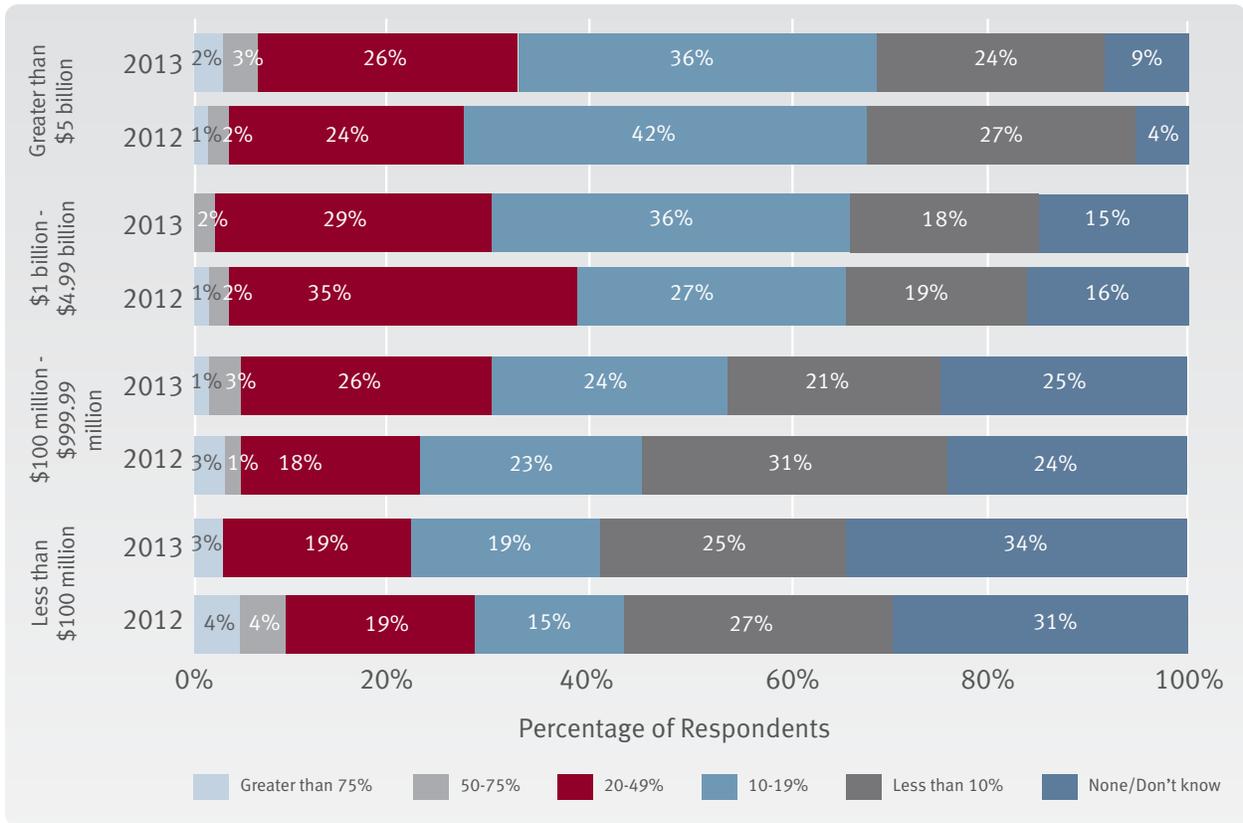
Does the IT audit director (or equivalent position) regularly attend the audit committee meetings?

	2013	2012
Yes	42%	27%
No	58%	73%

Here, the year-over-year growth is an encouraging development. The IT audit director’s regular presence in audit committee meetings is a positive sign that the organization is taking specific steps to audit its IT risks. In today’s technology-oriented business environment, it is more important than ever to have IT specialists engaged at the audit committee and board level, particularly given the inherent risk profile of IT.

Resourcing

What percentage of the internal audit department headcount is designated as IT audit?



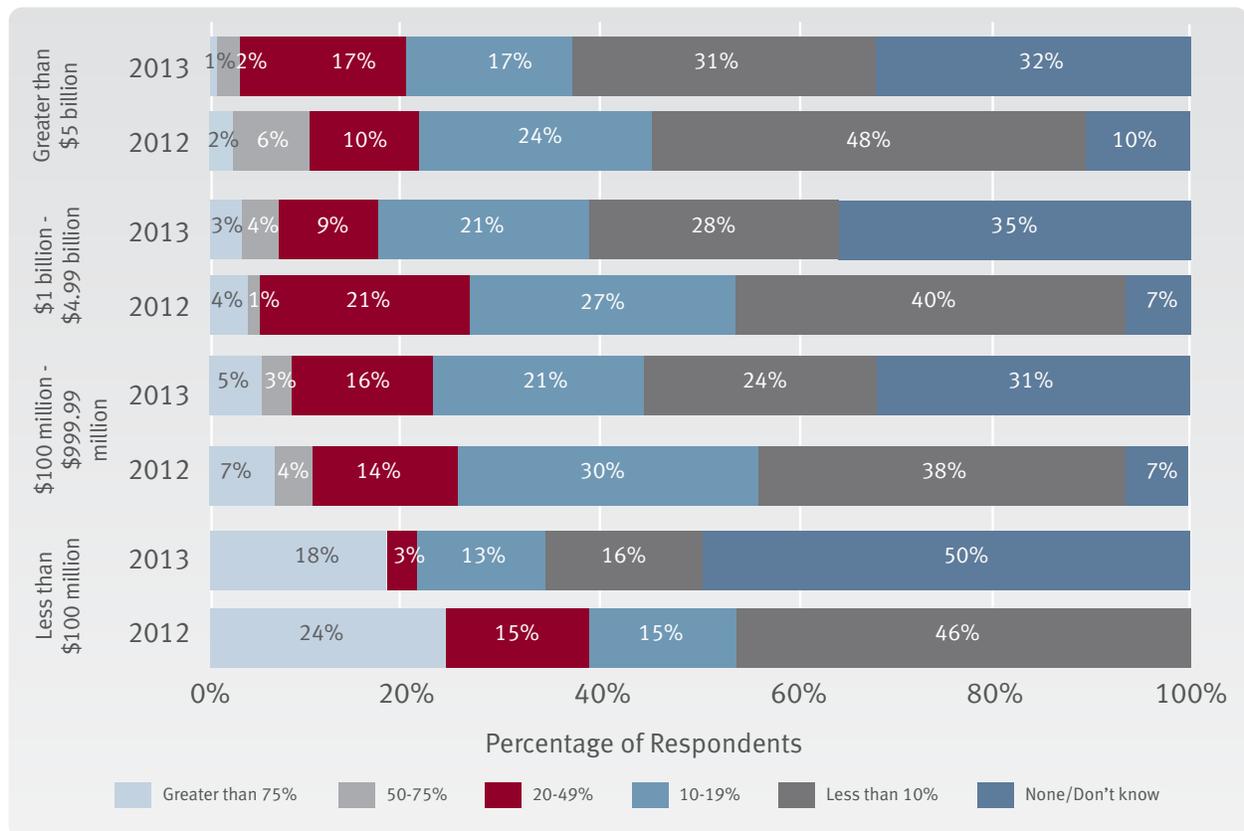
This year’s results continue to show that, in terms of IT audit skills, a large number of organizations may be understaffed. In fact, in several areas IT audit resource hours have decreased compared to last year. This is a concerning trend considering the pace at which IT risks are increasing.

Do you use outside resources to augment/provide your IT audit skill set?

	2013				2012			
	Yes, we use guest auditors	Yes, we outsource the IT audit function	Yes, we use co-source providers	Do not use outside resources	Yes, we use guest auditors	Yes, we outsource the IT audit function	Yes, we use co-source providers	Do not use outside resources
Company Size (Annual Revenue)								
Greater than \$5 billion	23%	7%	46%	37%	30%	3%	38%	42%
\$1 billion - \$4.99 billion	15%	12%	44%	36%	13%	8%	45%	43%
\$100 million - \$999.99 million	23%	20%	35%	31%	19%	13%	38%	34%
Less than \$100 million	19%	22%	19%	47%	12%	24%	20%	48%

As the results indicate, larger companies (US\$1 billion or greater in annual revenue) tend to co-source the IT audit function most often. However, similar to last year's findings, a substantial percentage of organizations do not use any outside resources. Given these findings along with those noted in the previous chart with regard to IT audit headcount, it appears the IT audit function is understaffed in many organizations. This is an indication that IT risks are not being addressed effectively in these organizations.

What is the percentage of outside IT audit resource hours used compared to total audit hours?



Please indicate the primary reasons your company uses outside resources to augment IT audit skills.

	2013	2012
In-house internal audit department lacks specific skill sets	48%	67%
Variable resource modeling	14%	21%
Different/outside perspectives	21%	28%
Lack of resources	42%	46%
Provides the opportunity for people to learn from the experiences of outside resources (e.g., knowledge transfer, etc.)	28%	38%

These findings may indicate improving economic conditions and increased hiring. Compared to last year's results, a lower percentage of organizations are using outside resources due to a lack of specific skill sets, variable resource modeling and overall lack of resources. Still, it is notable that nearly half of all companies bring in outside resources because they lack the necessary skills in house. It is likely that organizations are hiring more general IT auditors but are continuing to supplement their ranks, as needed, with technical experts who possess deep skills.

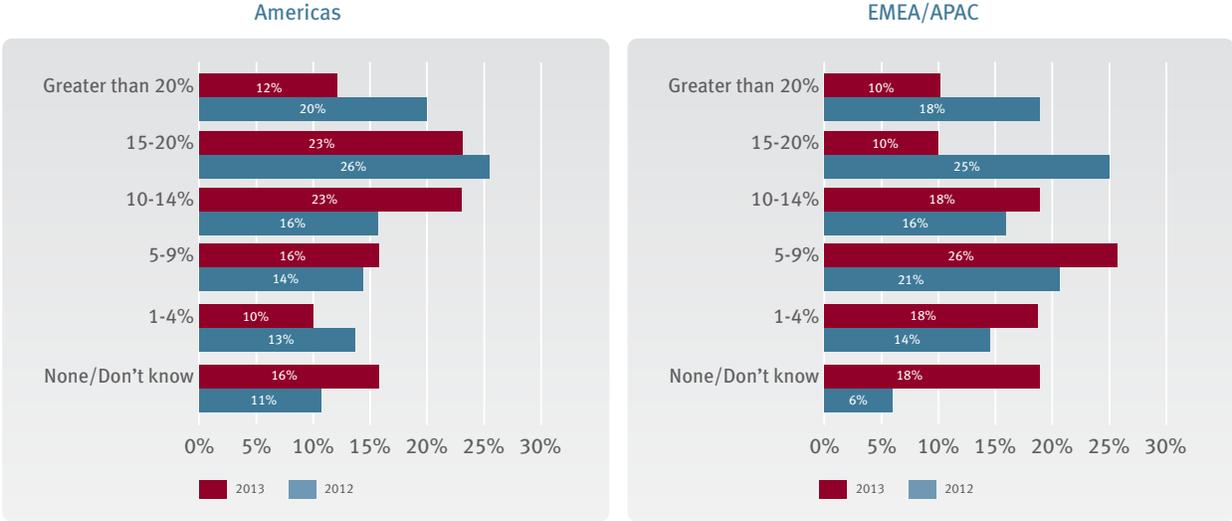
How are IT audit resources organized within your organization?

	2013				2012			
	Greater than \$5 billion	\$1 billion – \$4.99 billion	\$100 million – \$999.99 million	Less than \$100 million	Greater than \$5 billion	\$1 billion – \$4.99 billion	\$100 million – \$999.99 million	Less than \$100 million
Part of the internal audit department, not a separate function	53%	63%	62%	34%	56%	62%	61%	42%
Part of the internal audit department, but considered to be a separate function	37%	21%	13%	22%	30%	20%	17%	35%
Embedded in the organization as a separate audit function, e.g., line of business teams, process teams, etc.	5%	3%	3%	6%	8%	2%	8%	0%
No IT audit resources are available within the organization	5%	13%	22%	38%	6%	16%	14%	23%

Year-over-year results are comparable, which in one respect is troubling: In many companies, IT audit resources are not embedded within the internal audit department or are not available at all. This is a clear sign that a significant number of companies are not getting the IT audit coverage they need.

Reporting

Please indicate the number of IT audit reports issued as a percentage of the total reports issued by the internal audit department.



These results indicate that in a majority of organizations, less than 15 percent of internal audit reports are IT-focused, whereas the ideal percentage should be 20 percent or more. This suggests that organizations are not focusing enough on their IT risks.

Key Questions to Consider for Your Audit Plan

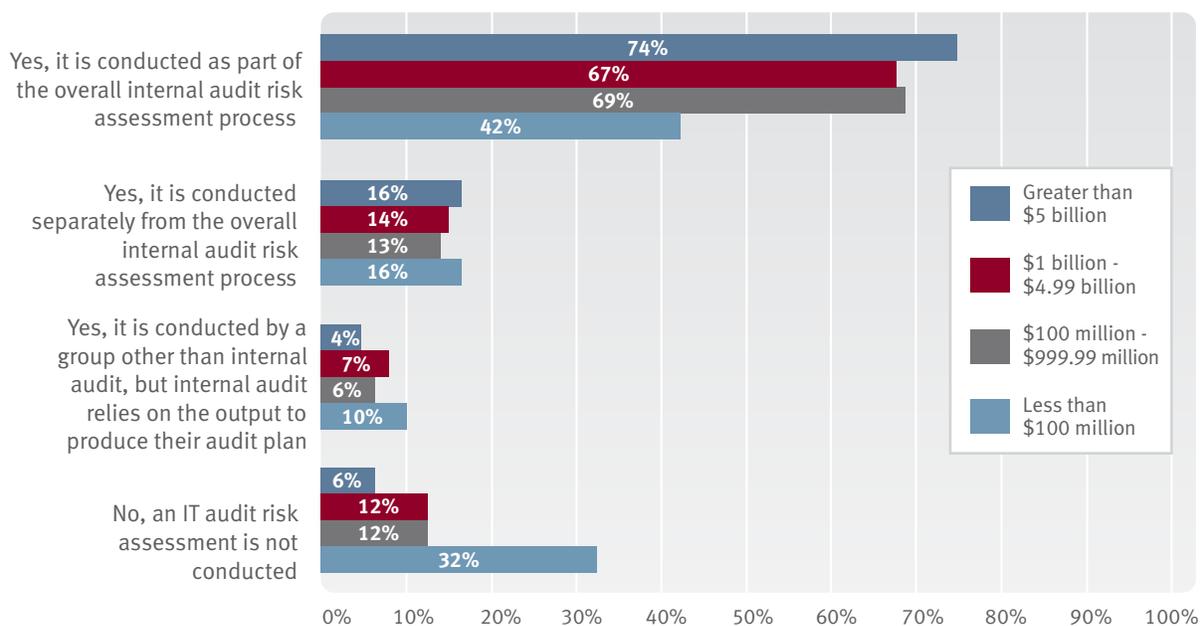
- Is our IT audit organization structured effectively relative to the size and composition of the organization?
- How do our IT audit costs compare to those of other comparable organizations (size, industry)?
- Can our IT audit function leverage new and emerging technology to meet established service levels and maximize audit efficiency?
- How do we staff our IT audits? Do we use specialists for auditing various technologies (e.g., applications versus infrastructure technologies)? If not, why?
- Have we considered outsourcing or offshoring as options for increasing our IT audit activities? Have we established a clear strategy and approach with regard to outsourcing/offshoring these activities?
- What processes do we have in place to evaluate and select a third-party IT audit service provider? Who is involved with these processes?
- How do we measure performance within our IT audit function? Has our internal audit department established quantifiable metrics and/or key performance indicators (KPIs)? How is this information being communicated to our top management?
- Have we documented our organization’s IT audit areas of responsibility?
- Has our IT audit function benchmarked itself against industry best practices?
- Do we review our IT audit work papers for quality and accuracy?



Assessing IT Risks

Conducting an IT Audit Risk Assessment

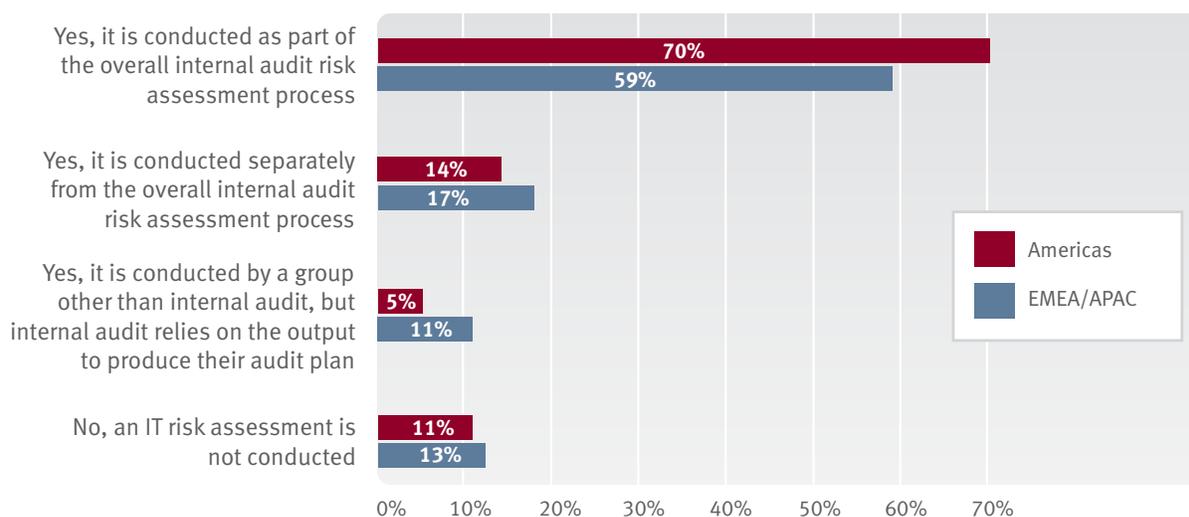
Does your organization conduct an IT audit risk assessment?



Mature internal audit functions are pushing their efforts to conduct fully integrated risk assessments that include IT risks. We expect that as the focus on strong enterprise risk management (ERM) continues to grow, more organizations will begin to have their IT audit risk assessments conducted by a function or third party other than internal audit, but IT audit will rely on these assessments to produce their annual audit plans. Such an approach is emphasized by COSO.

COSO has commented that one of the specific reasons for the update to its 1992 framework was to more directly address technology. To that end, one of the 17 principles (Principle 11) directs an organization to have IT general controls to support the achievement of objectives. This would entail the security, change and operational controls common in many SOX programs today, but may also include end user computing, reporting and other controls that are specific to that objective. In any case, starting with the objectives to be achieved and then determining if there are underlying technology components of the organization that are critical to the achievement of those objectives will lead to IT areas that need to be evaluated as part of an audit plan.

Results by Region



Organizational Engagement/Involvement

Indicate the level of involvement of each of the following individuals/groups in your organization's IT audit risk assessment process.⁷

	Significant		Moderate		Minimal		None	
	2013	2012	2013	2012	2013	2012	2013	2012
Americas								
Audit committee	13%	3%	25%	20%	36%	46%	26%	31%
Executive management (e.g., CIO)	34%	31%	43%	43%	20%	22%	3%	4%
Management and/or process owners	36%	32%	47%	45%	14%	19%	3%	4%
Line of business executives	18%	16%	42%	40%	29%	34%	11%	10%
Company IT organization representatives	43%	49%	40%	37%	13%	13%	4%	1%
Internal audit/IT audit	64%	72%	21%	18%	4%	6%	11%	4%
Risk management (separate from internal audit)	20%	15%	56%	24%	18%	24%	6%	37%
External auditor	8%	8%	31%	20%	35%	38%	26%	34%
Third-party service provider	7%	6%	17%	9%	21%	22%	55%	63%

⁷ Respondents are those organizations that conduct IT audit risk assessments as noted in answers to the previous question.

	Significant		Moderate		Minimal		None	
	2013	2012	2013	2012	2013	2012	2013	2012
EMEA/APAC								
Audit committee	16%	14%	29%	32%	28%	35%	27%	19%
Executive management (e.g., CIO)	22%	36%	47%	43%	28%	20%	3%	1%
Management and/or process owners	28%	39%	57%	44%	12%	16%	3%	1%
Line of business executives	24%	25%	40%	45%	28%	23%	8%	7%
Company IT organization representatives	35%	46%	39%	38%	18%	12%	8%	4%
Internal audit/IT audit	62%	59%	29%	22%	2%	12%	7%	7%
Risk management (separate from internal audit)	38%	32%	34%	36%	7%	14%	21%	18%
External auditor	9%	6%	24%	29%	40%	43%	27%	22%
Third-party service provider	3%	7%	21%	19%	31%	25%	45%	49%

A few observations based on these results:

- In the Americas, the audit committee appears to be more involved in the IT audit risk assessment process (comparing the year-over-year results), which is good to see. This also ensures the overall board of directors has an adequate level of involvement.
- Also in the Americas, the involvement of the external auditor is increasing. Note that last year, 28 percent were significantly or moderately involved in this process. This year the response increased to 39 percent.
- Line-of-business executives should have much greater involvement in the IT audit risk assessment process. Note there is more involvement among these executives within EMEA/APAC organizations.
- Not surprisingly, the risk management function appears to be involving itself more in the IT audit risk assessment process.

Frequency with which IT audit risk assessment is updated:

	2013	2012
Continually	8%	7%
Monthly	2%	1%
Quarterly	10%	13%
Semi-annually	10%	8%
Annually	65%	65%
Less than annually	4%	5%
Never	1%	1%

This year's results are similar to those from 2012. Overall, the fact that 70 percent of organizations appear to update their IT audit risk assessment only on an annual basis, or less than annual basis, is a poor trend. Most mature internal audit functions perform these assessments more frequently. And given the speed of technology innovation and change, it continues to be surprising to see in our study that the number of organizations doing these assessments on a quarterly or monthly basis is not higher. However, it is possible that some organizations perform more frequent ad hoc or informal updates to their IT audit risk assessments and change their audit plans accordingly. Over time, we expect to see the percentage of organizations conducting IT audit risk assessments on a quarterly or more frequent basis to increase.

Frameworks

On which of the following accepted industry frameworks is the IT audit risk assessment based?

	2013	2012
COBIT	62%	63%
COSO	52%	46%
SOGP	2%	0%
ISO	16%	19%
Other	8%	7%
None	13%	14%

Here, it is positive to see organizations employing a range of frameworks. In our experience, many internal audit functions utilize a combination of frameworks for their IT audit risk assessments.

Industry Frameworks

COBIT – ISACA’s globally accepted framework provides an end-to-end business view of the governance of enterprise IT that reflects the central role of information and technology in creating value for enterprises.

COSO Internal Control – Integrated Framework – This framework, produced as part of a landmark report from the Committee on Sponsoring Organizations of the Treadway Commission (COSO), establishes a common definition of internal control that serves the needs of different parties for assessing and improving their control systems. It provides principles-based guidance for designing and implementing effective internal controls. Earlier this year, COSO released its long-awaited update to its Internal Control – Integrated Framework. Developed over a two-and-a-half-year period, COSO’s new framework and related illustrative documents are intended to help organizations in their efforts to adapt to the increasing complexity and pace of change, to mitigate risks to the achievement of objectives, and to provide reliable information to support sound decision-making.

ISO – The International Organization for Standardization is the world’s largest developer of voluntary International Standards. International Standards give state-of-the-art specifications for products, services and good practice, helping to make industry more efficient and effective. Developed through global consensus, they help to break down barriers to international trade.

Standard of Good Practice (SOGP) for Information Security – From the Information Security Forum, this is a business-focused, practical and comprehensive guide for identifying and managing information security risks in an organization.

“IT AUDIT IS AN INTEGRAL PART OF THE INTERNAL AUDIT FUNCTION AND VALUED AS A PARTNER BY [OUR] IT ORGANIZATION.”

— VICE PRESIDENT OF IT AUDIT, LARGE CONSUMER PRODUCTS COMPANY

Key Questions to Consider for Your Audit Plan

- Does our internal audit function perform an effective IT audit risk assessment on at least an annual basis? Should we conduct this assessment more frequently? Are knowledgeable specialists in infrastructure technologies, application systems and IT processes involved in the assessment?
- Does our IT audit risk assessment consider the specific technological architecture and configuration employed by our organization?
- Have we reviewed, in detail, the recently released 2013 COSO Internal Control – Integrated Framework? Do we understand the increased emphasis on IT governance and strong IT controls, and have we addressed this adequately in our audit plan?
- How do we quantify our IT audit risks? What industry benchmarks and best practices do we use to support these estimates?
- Is our IT audit department collaborating effectively with other areas of our business to manage shifting priorities or changes in the regulatory landscape?
- Does our IT audit team have a clear understanding of our company’s short- and long-term IT objectives? Are the IT audit department’s priorities and activities aligned with these objectives?
- Does our IT audit team have visibility into major events we have planned in the near- or long-term, such as a merger or acquisition, initial public offering, divestiture or business expansion?
- Is our audit department aware of the degree to which our organization’s IT environment changes every year?
- Have we implemented any IT control frameworks or standards? If so, which ones? If not, have we established security and control baselines internally? If not, has our CAE recommended the implementation of an IT control framework and security and control baselines as part of the audit of IT governance and management?
- Does our IT audit risk assessment process coordinate with, and consider the results of, other risk assessment dimensions, such as financial, operational, compliance and geography?



Audit Plan

Focus of IT Audit Hours

Which activities are included within the responsibility of IT audit?

	2013	2012
IT general controls	85%	92%
IT process auditing, e.g., security, privacy, etc.	81%	85%
Application auditing	77%	82%
IT infrastructure auditing	70%	75%
IT compliance testing	69%	75%
Pre- and post-implementation auditing	58%	65%
Integrated auditing	54%	53%
IT Sarbanes-Oxley testing	53%	-
Data analytics	48%	49%
External audit support	40%	-
Consultative activities	39%	50%
Maintaining internal control framework documentation	38%	-
Continuous auditing	26%	30%
Vendor audits	24%	-
Other	3%	6%

“[OUR] CURRENT AUDIT PLAN IS SOX- AND COMPLIANCE-HEAVY DUE TO THE SMALL NUMBER OF EMPLOYEES. IT AUDIT BEYOND SOX CONTINUES TO BE AN AREA OF POTENTIAL EXPANSION.”

— AUDIT MANAGER, MIDSIZE MANUFACTURING COMPANY

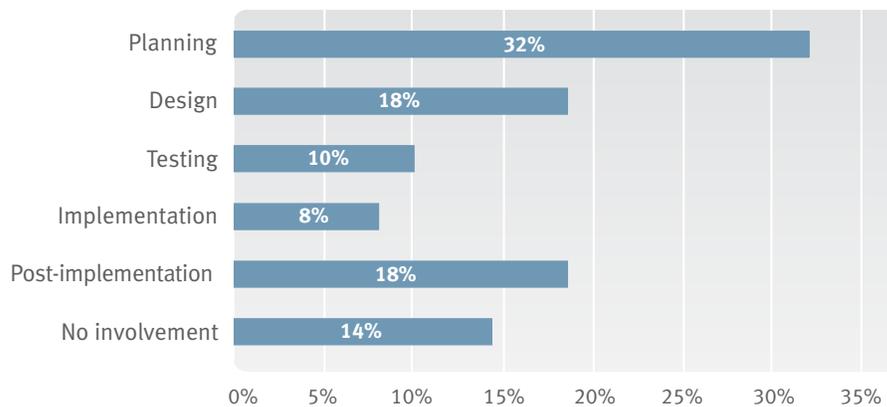
What level of involvement does IT audit have in significant technology projects?

	Significant	Moderate	Minimal	None
Company Size (Annual Revenue)				
Greater than \$5 billion	22%	46%	25%	7%
\$1 billion - \$4.99 billion	12%	45%	31%	12%
\$100 million - \$999.99 million	9%	35%	43%	13%
Less than \$100 million	7%	30%	41%	22%

Across the board (in terms of company size), there are many organizations in which IT audit has minimal or no involvement in significant technology projects. Even among large companies, one in three either involve IT audit minimally or do not have the function involved. With the continued upswing in the use of third-party IT services, solutions and platforms (e.g., cloud-based servers and applications), IT audit should be engaged in major technology projects more often.

That said, for those organizations that do involve IT audit in significant technology projects, it is good to see them doing so early. IT audit engagement during the planning and design stages allows the proper level of timely independent challenge along with guidance on risk management and control design. On the other hand, for the 18 percent of organizations that involve IT audit in the post-implementation stage, they may be too late to identify and/or address major project risks and issues before having to undertake costly fixes.

When does IT audit become involved in significant technology projects?



What percentage of time does the IT audit function spend on assurance, compliance and consulting activities?

Results by Company Size

	Greater than 75%	50 - 75%	25 - 49%	15 - 24%	1 - 14%	None/Don't know
Greater than \$5 billion						
Assurance	23%	33%	21%	8%	5%	10%
Compliance	3%	17%	24%	32%	13%	11%
Consulting	1%	5%	15%	26%	37%	16%
\$1 billion - \$4.99 billion						
Assurance	16%	26%	22%	13%	10%	13%
Compliance	7%	15%	26%	25%	13%	14%
Consulting	1%	7%	9%	25%	37%	21%
\$100 million - \$999.99 million						
Assurance	14%	26%	22%	10%	12%	16%
Compliance	8%	14%	29%	22%	13%	14%
Consulting	1%	4%	12%	21%	39%	23%
Less than \$100 million						
Assurance	11%	26%	19%	7%	11%	26%
Compliance	0%	11%	33%	11%	19%	26%
Consulting	0%	11%	7%	26%	22%	34%

Results by Region

	Greater than 75%	50 - 75%	25 - 49%	15 - 24%	1 - 14%	None/Don't know
Americas						
Assurance	14%	28%	23%	11%	9%	15%
Compliance	6%	16%	27%	25%	13%	13%
Consulting	1%	5%	12%	23%	39%	20%
EMEA/APAC						
Assurance	35%	29%	13%	5%	8%	10%
Compliance	5%	11%	27%	24%	16%	17%
Consulting	0%	8%	8%	27%	26%	31%

IT Governance

Has your IT audit activity completed an evaluation and assessment of your organization's IT governance process, in accordance with IIA Standard 2110.A2?

	2013		2012	
	Yes	No	Yes	No
Company Size (Annual Revenue)				
Greater than \$5 billion	48%	52%	45%	55%
\$1 billion - \$4.99 billion	44%	56%	23%	77%
\$100 million - \$999.99 million	29%	71%	22%	78%
Less than \$100 million	30%	70%	14%	86%

	2013		2012	
	Yes	No	Yes	No
Region				
Americas	40%	60%	28%	72%
EMEA/APAC	40%	60%	26%	74%

The results show year-over-year increases across the board among organizations that are meeting the requirements of The IIA's IT governance standard, which is good to see. Of note, IT governance may be covered as part of broader governance reviews in some organizations, so it's possible the percentage of organizations that have adequately evaluated and assessed their IT governance processes is even higher.

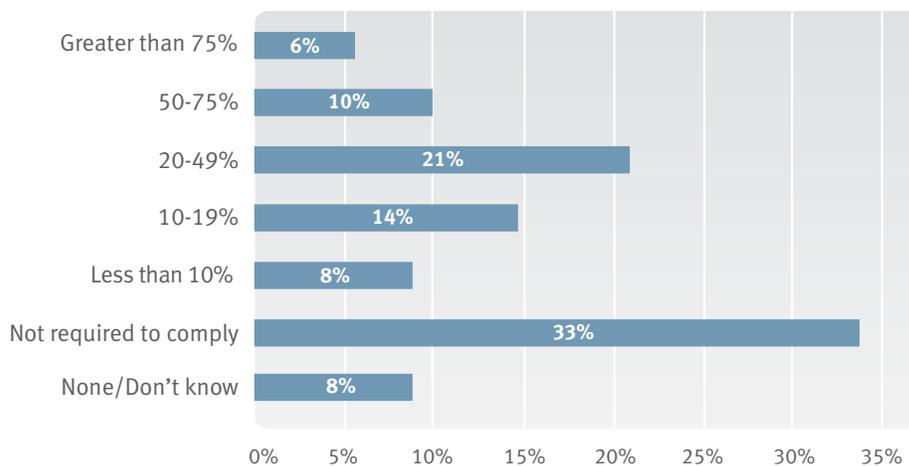
Please indicate whether you intend to complete an evaluation and assessment of your organization's IT governance process.⁸

	2013			2012		
	Yes, within the next year	Yes, but not within the next year	No plans to conduct such a review	Yes, within the next year	Yes, but not within the next year	No plans to conduct such a review
Company Size (Annual Revenue)						
Greater than \$5 billion	35%	32%	33%	29%	15%	56%
\$1 billion - \$4.99 billion	28%	28%	44%	31%	30%	39%
\$100 million - \$999.99 million	33%	32%	35%	23%	28%	49%
Less than \$100 million	42%	32%	26%	33%	39%	28%

⁸ Respondents are those organizations that have not completed an evaluation and assessment of the organization's IT governance process in accordance with IIA Standard 2110.A2.

	2013			2012		
	Yes, within the next year	Yes, but not within the next year	No plans to conduct such a review	Yes, within the next year	Yes, but not within the next year	No plans to conduct such a review
Region						
Americas	30%	32%	38%	25%	31%	44%
EMEA/APAC	46%	27%	27%	32%	18%	50%

In your most recently completed year of Sarbanes-Oxley compliance, what percentage of your organization's IT audit hours were associated with SOX-related activities?



Key Questions to Consider for Your Audit Plan

- In our activity mix, how much time are we spending on assurance and compliance compared with consulting? Should we seek to change that mix and provide more consultative guidance?
- How often is our IT audit plan reviewed? What processes do we have in place to maintain it?
- How is our IT audit plan addressing demands for faster performance in our organization?
- What process does IT audit have to ensure its practices align with our business expectations?
- How can our CAE and other IT audit leaders be more integrated into the planning and other activities of our business units and departments?
- Does the IT audit universe plan for audits at each layer of our IT environment? If not, why not? Are there special circumstances that apply, or is the IT audit plan suboptimal?
- How do we estimate our budgets for IT audits? Do we gather enough information on the front end of the audit to support an accurate estimation? Is the specific configuration of technology considered?
- How are our IT audit procedures defined? Do we develop them internally for our organization's specific environment, or are marketplace checklists used?
- Do we use any tools to accelerate IT audits (e.g., testing accelerators or facilitators)? If not, why not? If so, has our IT management tested and approved them?
- Is our audit strategic plan supported by individual tactical operating plans that take into account our IT audit requirements and deliverables?



Skills and Capabilities

Gaps in IT Audit Plan

Are there specific areas of your current IT audit plan that you are not able to address sufficiently due to lack of resources/skills?

	2013		2012	
	Yes	No	Yes	No
Company Size (Annual Revenue)				
Greater than \$5 billion	28%	72%	33%	67%
\$1 billion - \$4.99 billion	36%	64%	45%	55%
\$100 million - \$999.99 million	30%	70%	36%	64%
Less than \$100 million	31%	69%	40%	60%

There is a positive downward trend in organizations reporting they lack the resources and/or skills to address specific areas of their IT audit plans. Still, we would expect more large companies (US\$1 billion or more in annual revenue) to have the necessary resources in place, either through their own internal audit department or through co-sourcing. And the 69-70 percent “No” response among smaller companies is a bit surprising considering that a significant number of them lack an IT audit function (see page 5).

Are there specific areas of your current IT audit plan that you are not able to address sufficiently due to lack of software tools?

	2013		2012	
	Yes	No	Yes	No
Company Size (Annual Revenue)				
Greater than \$5 billion	9%	91%	15%	85%
\$1 billion - \$4.99 billion	14%	86%	19%	81%
\$100 million - \$999.99 million	15%	85%	24%	76%
Less than \$100 million	12%	88%	25%	75%

These results are highly encouraging in that they show more organizations are obtaining the software tools they need to perform IT audits effectively as part of their audit plans.

“THERE IS A NEED TO BUILD ROBUST IT AUDITING SKILLS IN OUR INTERNAL AUDIT DEPARTMENT.”

— AUDIT MANAGER, MIDSIZE SERVICES ORGANIZATION

Are IT audits conducted by individuals who are full-time internal audit professionals in the internal audit department and who focus on IT audit projects?

	2013		2012	
	Yes	No	Yes	No
Company Size (Annual Revenue)				
Greater than \$5 billion	81%	19%	92%	8%
\$1 billion - \$4.99 billion	73%	27%	75%	25%
\$100 million - \$999.99 million	52%	48%	57%	43%
Less than \$100 million	58%	42%	65%	35%

The results for larger companies are good, though it is interesting to see an 11 percent year-over-year drop in the “Yes” responses among the largest organizations.

In assigning audit staff to conduct IT auditing activities, organizations, regardless of size, should be sure to distinguish between IT audit generalists and specialists (either internal or third parties) who have more in-depth and relevant knowledge of critical IT issues such as cybersecurity, IT governance, cloud-based activities, data security and privacy, and mobile device usage, among many others.

Key Questions to Consider for Your Audit Plan

- With regard to our IT infrastructure and existing management tools, has our IT audit team identified opportunities for greater efficiencies and cost savings?
- Can a better understanding and improvement in IT audit processes help our audit staff add more value and improve its effectiveness?
- Have we established a training strategy for our IT auditors? Does this strategy consider all layers of our IT environment?
- Does our organization offer adequate training for IT audit staff in technical as well as interpersonal and communication skills to enable them to work more effectively with various departments?
- Have we observed interactions between our IT audit professionals and management that might have been handled more effectively from a communication standpoint?
- What sort of leadership training do we offer to IT audit personnel?

Methodology and Demographics

More than 460 respondents participated in Protiviti's third annual *IT Audit Benchmarking Survey*, which was conducted in the first and second quarters of 2013. The survey consisted of a series of questions grouped into five categories:

- Top Technology Challenges
- IT Audit in Relation to the Internal Audit Department
- Assessing IT Risks
- Audit Plan
- Skills and Capabilities

Survey participants also were asked to provide demographic information about the nature, size and location of their businesses, and their titles or positions within the internal audit department. All demographic information was provided voluntarily by respondents and not all participants provided data for every demographic question.

Sources of Respondents

- **Web-based survey at KnowledgeLeader®** – Electronic surveys were made available online to KnowledgeLeader (www.knowledgeleader.com) subscribers, including those with trial subscriptions. KnowledgeLeader is a subscription-based Protiviti website designed to assist internal audit professionals with finding information, tools and best practices they can use to improve the efficiency and quality of their work.
- **Electronic surveys** – Surveys also were forwarded and provided to other internal audit professionals who expressed an interest in participating.

Position

Chief Audit Executive (or equivalent)	22%
IT Audit Director	6%
Audit Director	10%
IT Audit Manager	17%
Audit Manager	15%
Audit Staff	20%
Other	10%

Size of Organization (by Gross Annual Revenue)

\$20 billion or greater	13%
\$10 billion - \$19.99 billion	7%
\$5 billion - \$9.99 billion	11%
\$1 billion - \$4.99 billion	31%
\$500 million - \$999.99 million	15%
\$100 million - \$499.99 million	16%
Less than \$100 million	7%

Industry

Financial Services	21%
Manufacturing	11%
Government/Education/Not-for-profit	10%
Insurance	9%
Energy	6%
Healthcare Provider	6%
Retail	5%
Telecommunications	4%
Utility	4%
Healthcare Payer	3%
Technology	3%
Distribution	2%
Hospitality	2%
Services	2%
Other	12%

Type of Organization

Public	50%
Private	26%
Not-for-profit	12%
Government	11%
Other	1%

Company Location

North America	84%
Europe	6%
Asia/Pacific	4%
Middle East	4%
Africa	2%

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit. Through our network of more than 70 offices in over 20 countries, we have served more than 35 percent of FORTUNE 1000® and FORTUNE Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

About Our IT Internal Audit Services

Protiviti's IT internal audit services help organizations understand their key technology risks and how well they are mitigating and controlling those risks. We also provide insight into the threats inherent in today's highly complex technologies. Protiviti provides a wide range of services for IT internal audit outsourcing and co-sourcing. The Protiviti methodology, which is both COSO- and COBIT-based, facilitates an overall IT internal audit management team (either Protiviti-led, client-led, or in combination) with the execution of individual projects by subject-matter experts in each IT audit area.

Other Thought Leadership from Protiviti

Visit www.protiviti.com to obtain copies of these and other thought leadership materials from Protiviti.

- *Using High Value IT Audits to Add Value and Evaluate Key Risks and Controls*
- Powerful Insights (Protiviti's podcast series)
 - IT Audit – Assessing and Managing Risks Effectively within the IT Environment
 - Social Media Use in Companies – Managing the Risks Effectively
 - Technology-enabled Audits – Increasing Productivity and Delivering More Timely and Reliable Results
 - Internal Audit Quality Assessment Reviews – Required as Well as Beneficial
 - Sarbanes-Oxley Compliance: Where U.S.-Listed Companies Stand Today
 - The Benefits of Outsourcing the Internal Audit Function
- *2013 Internal Audit Capabilities and Needs Survey*
- *Testing the Reporting Process – Validating Critical Information*
- *Guide to Internal Audit: Frequently Asked Questions about Developing and Maintaining an Effective Internal Audit Function* (Second Edition)
- *Building Value in Your SOX Compliance Program: Highlights from Protiviti's 2013 Sarbanes-Oxley Compliance Survey*
- *Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements* (Fourth Edition)
- *Guide to the Sarbanes-Oxley Act: IT Risks and Controls* (Second Edition)
- *Internal Auditing Around the World* (Volumes 1-9)

KnowledgeLeader[®] is a subscription-based website that provides information, tools, templates and resources to help internal auditors, risk managers and compliance professionals save time, stay up to date and manage business risk more effectively. The content is focused on business risk, technology risk and internal audit. The tools and resources available on KnowledgeLeader include:

- **Audit Programs** – A wide variety of sample internal audit and IT function audit work programs are available on KnowledgeLeader. These work programs, along with the other tools listed below, are all provided in downloadable versions so they can be repurposed for use in your organization.
- **Checklists, Guides and Other Tools** – More than 1,000 checklists, guides and other tools are available on KnowledgeLeader. They include questionnaires, best practices, templates, charters and more for managing risk, conducting internal audits and leading an internal audit department.
- **Policies and Procedures** – KnowledgeLeader provides more than 300 sample policies to help in reviewing, updating or creating company policies and procedures.
- **Articles and Other Publications** – Informative articles, survey reports, newsletters and booklets produced by Protiviti and other parties (including *Compliance Week* and Auerbach) about business and technology risks, internal audit and finance.
- **Performer Profiles** – Interviews with internal audit executives who share their tips, techniques and best practices for managing risk and running the internal audit function.

Key topics covered by KnowledgeLeader:

- Audit Committee and Board
- Business Continuity Management
- Control Self-Assessment
- Corporate Governance
- COSO
- Fraud and Ethics
- IFRS
- Internal Audit
- IT Audit
- IT Governance
- Sarbanes-Oxley

KnowledgeLeader also has an expanding library of methodologies and models – including the robust Protiviti Risk ModelSM, a process-oriented version of the Capability Maturity Model, the Six Elements of Infrastructure Model, and the Sarbanes-Oxley 404 Service Delivery Model.

Furthermore, with a KnowledgeLeader membership, you will have access to AuditNet Premium Content; discounted certification exam preparation material from ExamMatrix; discounted MicroMash CPE Courses to maintain professional certification requirements; audit, accounting and technology standards and organizations; and certification and training organizations, among other information.

To learn more, sign up for a complimentary 30-day trial by visiting www.knowledgeleader.com. Protiviti clients and alumni, and members of The IIA, ISACA and AHIA, are eligible for a subscription discount. Additional discounts are provided to groups of five or more.

KnowledgeLeader members have the option of upgrading to KLplusSM. KLplus is the combined offering of KnowledgeLeader's standard subscription service plus online CPE courses and risk briefs. The courses are a collection of interactive, Internet-based training courses offering a rich source of knowledge on internal audit and business and technology risk management topics that are current and relevant to your business needs.

Protiviti Internal Audit and Financial Controls Practice – Contact Information

Brian Christensen
Executive Vice President – Global Internal Audit
+1.602.273.8020
brian.christensen@protiviti.com

David Brand
Managing Director
Leader – IT Audit Practice
+1.312.476.6401
david.brand@protiviti.com

UNITED STATES

Central Region

Michael Thor
+1.312.476.6400
michael.thor@protiviti.com

Eastern Region

James Armetta
+1.212.399.8606
james.armetta@protiviti.com

Western Region

Jonathan Bronson
+1.213.327.1308
jonathan.bronson@protiviti.com

Anthony Samer
+1.415.402.3627
anthony.samer@protiviti.com

AUSTRALIA

Ewen Ferguson
+61.2.8220.9500
ewen.ferguson@protiviti.com.au

CANADA

Marc Poirier
+1.514.871.2348
marc.poirier@protiviti.com

CHINA

Michael Pang
(852) 2238.0499
michael.pang@protiviti.com

GERMANY

Thorsten Ruetze
+49.69.96.37.68.142
thorsten.ruetze@protiviti.de

JAPAN

Yasumi Taniguchi
+81.3.5219.6600
yasumi.taniguchi@protiviti.jp

SINGAPORE

Ivan Leong
+65.6220.6066
ivan.leong@protiviti.com

UNITED KINGDOM

Mark Peters
+44.207.389.0413
mark.peters@protiviti.co.uk

THE AMERICAS

UNITED STATES

Alexandria	Kansas City	Salt Lake City
Atlanta	Los Angeles	San Francisco
Baltimore	Milwaukee	San Jose
Boston	Minneapolis	Seattle
Charlotte	New York	Stamford
Chicago	Orlando	St. Louis
Cincinnati	Philadelphia	Tampa
Cleveland	Phoenix	Washington, D.C.
Dallas	Pittsburgh	Winchester
Denver	Portland	Woodbridge
Fort Lauderdale	Richmond	
Houston	Sacramento	

ARGENTINA*

Buenos Aires

CHILE*

Santiago

BRAZIL*

Rio de Janeiro
São Paulo

MEXICO*

Mexico City
Monterrey

PERU*

Lima

VENEZUELA*

Caracas

CANADA

Kitchener-Waterloo
Toronto

ASIA-PACIFIC

AUSTRALIA

Brisbane
Canberra
Melbourne
Perth
Sydney

INDIA

Bangalore
Mumbai
New Delhi

INDONESIA**

Jakarta

CHINA

Beijing
Hong Kong
Shanghai
Shenzhen

JAPAN

Osaka
Tokyo

SINGAPORE

Singapore

SOUTH KOREA

Seoul

EUROPE/MIDDLE EAST/AFRICA

FRANCE

Paris

ITALY

Milan
Rome
Turin

THE NETHERLANDS

Amsterdam

GERMANY

Frankfurt
Munich

UNITED KINGDOM

London

BAHRAIN*

Manama

QATAR*

Doha

KUWAIT*

Kuwait City

UNITED ARAB EMIRATES*

Abu Dhabi
Dubai

OMAN*

Muscat

SOUTH AFRICA*

Johannesburg

* Protiviti Member Firm
** Protiviti Alliance Member