2012 Internal Audit
Capabilities and Needs Survey

protiviti®
Risk & Business Consulting.
Internal Audit.

Powerful Insights. Proven Delivery.®

Introduction

"TECHNOLOGY IS CRUCIAL TO ADMINISTERING AND MANAGING THE AUDIT PROCESS FROM THE BEGINNING TO THE END. WITHOUT TECHNOLOGY, THE RELIABILITY AND CONSISTENT ADHERENCE TO STANDARDS WOULD BE DIFFICULT, IF NOT IMPOSSIBLE."

Chief audit executive, nonprofit organization

Technology continues to be a key enabler and catalyst in business today, helping companies achieve greater efficiencies, productivity and profitability. At every turn, from the supply chain and production floor to back-office administration and even the C-suite, technology is a pervasive and, far more often than not, indispensable asset. Further, new technologies, including but not limited to mobile platforms and the "cloud," already are demonstrating the potential to take businesses to even higher levels of performance.

Without question, technological advancement in virtually every organization is creating a wealth of new challenges, along with opportunities, for chief audit executives (CAEs) and internal audit professionals. Not only must they enhance their knowledge and understanding of new technologies and how they support the business, but they also must leverage them to perform internal audit activities with greater effectiveness and efficiency.

It is for this reason that Protiviti focused the latest edition of its *Internal Audit Capabilities and Needs Survey* on technology, both in a special section dedicated to the use of technology in the audit process, and in the introduction of numerous new technology-related competencies in other sections of the survey.

More than 800 respondents participated in this year's study, including CAEs along with internal audit directors, managers and staff. These professionals answered close to 200 questions in the study's three standard categories – **General Technical Knowledge, Audit Process Knowledge**, and **Personal Skills and Capabilities** – and a new section, **Use of Technology in Auditing Business Process Controls**.

As we detail in the following pages, new technologies and managing risks related to them are major themes in this year's findings. Among the highlights:

1. **Social media and cloud computing are top concerns** – Internal audit executives and professionals recognize they must have superior knowledge and understanding of these areas and their inherent risks, and how their organizations are leveraging as well as controlling them, in order to perform their jobs at a high level and add value to the organizations they serve.

2. **There is significant potential for improvement via technology-enabled auditing** – Based on the survey's results, internal audit appears to be behind other departments in terms of using technology. Many internal audit functions are not using software tools to administer their audit processes, and among those that are, most are not leveraging these tools to their fullest extent.

3. **IT asset management, along with vendor negotiation and set-up, are top-of-mind priorities** – With regard to leveraging technology to audit business process controls, internal auditors see significant room for improvement.

4. **A surprisingly large number of organizations are not leveraging technology as part of their fraud prevention, detection and monitoring efforts** – Many are relying on simple databases and describe the availability of electronic data as less than optimal. The survey results clearly show that not enough companies are using technology in a proactive manner to prevent fraud, abuse, corruption and even bribery.

5. **CAATs, continuous auditing and continuous monitoring continue to garner attention** – As in previous years of the study, most respondents recognize the need to improve in these areas, suggesting the profession will continue to move more toward these approaches and techniques, which cover all or a large population of transactions rather than very limited sample sizes.

6. **Networking effectively and developing strong outside contacts are prized skills** – This is an indicator of the value internal audit executives and professionals see not only in developing best practices, but in learning from other high-performing organizations. While there are ever-increasing amounts of data and information available on the Web, connections, conversations and relationships with peers may prove to be the most efficient and valuable.

The internal audit executives and professionals who participated in our survey represent virtually all industry sectors. The largest segments are from financial services, healthcare and manufacturing. Half are with publicly traded companies, the others being from private, government and nonprofit organizations. (Please note that, upon request, we can provide customized reports based on the results of respondents from specific groups – industry, company size, etc.)

We continue to be very appreciative of the time invested in this study by all of the respondents, as well as the positive feedback we receive from the market about the survey findings and our insights. We are confident the results of our 2012 survey will again be of interest to board members, chief executive officers, chief financial officers and chief information officers, along with the internal audit community. Based on feedback from these audiences, we will continue to update this annual study to reflect changes in the business and regulatory environments, as well as emerging trends affecting internal audit functions and professionals.

Finally, we want to express our appreciation to The Institute of Internal Auditors for continuing to be an outstanding global leader and advocate for our profession.

Protiviti
March 2012

Use of Technology in Auditing Business Process Controls

Key Findings – 2012

- In this new category to the survey, IT asset management is considered a top priority, as is vendor negotiation and set-up.
- Not surprisingly, there is a need to increase the use of technology to audit areas that are more prone to fraud and security breaches – such as access controls, expense management and purchase orders.

Table 1: Overall Results, Use of Technology in Auditing Business Process Controls

"Need to Increase Use of Technology" Rank	Areas Evaluated by Respondents	Degree of Technology Use (5-pt. scale)
1	IT asset management	2.9
2	Vendor negotiation and set-up	2.7
3 (tie)	Access controls	3.3
3 (tie)	Cash receipts/applications	2.9
4 (tie)	Supplier management	2.8
4 (tie)	Travel and entertainment	2.9
5 (tie)	Purchasing/purchase orders	3.1
5 (tie)	Data/telecom costs	2.8
5 (tie)	HR records management	2.8
5 (tie)	Accounts receivable	3.0

Overall Findings

Respondents were asked to assess, on a scale of one to five, the degree to which their organizations use technology to audit 36 business process controls, with one indicating no use and five representing extensive use. For each area, they were then asked to indicate whether they believe their level of technology use is adequate or needs to be increased, taking into account the circumstances of their organization and industry. (For the business process controls under consideration, see page 5.) Figure 1 depicts a comparison of "Need to Increase Use of Technology" versus "Degree of Technology Use" ratings.

The results above suggest there continue to be significant concerns about 1) the proliferation of technology and how employees throughout the organization are leveraging a variety of desktop and mobile devices as part of their day-to-day duties, and 2) the potential for fraud in the organization.

Considering the proliferation of new technologies in organizations today, it is incumbent upon the IT organization to keep careful track of devices, tools, software and other technologies that have been deployed throughout the organization to potentially thousands of employees. It is incumbent upon the internal audit function to audit and test controls related to the policies for these tools and devices, including security and privacy, change control, and data integrity. As any organization knows, there is significant cost associated with IT assets, from which a return on investment (ROI) is needed. Physical security is important; it's easy for "little" things to disappear. Even a relatively small percentage of

"loss" in terms of hardware or, more importantly, data and other intellectual property could result in significant financial losses and, in the event of a security or data breach, potentially devastating effects in terms of regulatory noncompliance and reputation loss.

In terms of fraud, CAEs and internal audit professionals clearly are looking to do a better job of capitalizing on technology-enabled auditing to monitor controls over areas more prone to fraudulent activity, such as access controls, suppliers, capital expenditures, and travel and entertainment expenses, among others. The high "Need to Increase Use of Technology" rankings for auditing business processes such as purchasing and purchase orders, as well as cash receipts, are further indicators of ongoing fraud-related concerns among internal auditors and their organizations, and the power and leverage of using technology to assist them.

Vendor negotiation and set-up ties into these concerns as well. Creating vendors for actual use in the company's ERP system in itself is a key transaction that makes those vendors "go live" and allows for disbursements of funds to those organizations, albeit with the requirement of various approvals. Upon set-up, payments can be made – but it is possible that certain payments could be unauthorized or even fraudulent.

Organizations also are mindful of the fact that extending to any third parties, vendors or otherwise, access to key systems and controls creates fraud- and security-related risks that must be managed carefully. In addition to these concerns, internal audit must work with department heads and business owners to ensure vendor relationships are set up in compliance with organizational standards, as well as applicable laws and regulations.

Key Questions to Consider:

- Is the internal audit function partnering effectively with the CIO and IT department to assure that IT assets are managed and controlled appropriately? Are you aware of any gaps in the IT asset management process that should be addressed? Does the audit team have relevant and appropriate experience to handle technical matters?

- Is there a sufficient process in place to assess the security policies and practices of vendors that work with your organization? Does the organization have confidence that vendors' access controls and privacy standards exceed or are on par with its own? Are vendor access controls terminated when vendor relationships end?

- Does the internal audit function have appropriate technology tools to audit effectively business processes such as expense management, purchase orders, suppliers and accounts receivable, among other areas?

- How are internal auditors leveraging technology to prevent, detect, monitor and investigate fraud?

- Have all significant classes of mobile devices been considered?

Figure 1: Use of Technology in Auditing Business Process Controls – Perceptual Map

Number	Business Process Controls	Number	Business Process Controls
1	IT asset management	19	Time and expense reporting
2	Vendor negotiation and set-up	20	Time off/vacation tracking
3	Access controls	21	Facilities leases/improvements
4	Cash receipts/applications	22	Electronic data interchange (EDI) analysis
5	Supplier management	23	Validation of employment
6	Travel and entertainment	24	Credit memo process
7	Purchasing/purchase orders	25	Capital/operating leases
8	Data/telecom costs	26	Physical security/building access
9	HR records management	27	Obsolete/expired inventory
10	Accounts receivable	28	Construction analysis
11	Revenue recognition	29	Inventory valuation
12	Billing	30	Intercompany/interbusiness unit sales and transfer pricing
13	Fixed asset control	31	Inventory master control
14	Receiving	32	Book and physical inventory differences
15	Compensation and benefits management	33	Sales contract timing
16	Accounts payable/cash disbursements	34	Call center/customer service
17	Credit collection/bad debt	35	Royalties
18	Cash management segregation of duties	36	Warranty repair

FOCUS ON CHIEF AUDIT EXECUTIVES

Table 2: CAE Results, Use of Technology in Auditing Business Process Controls

"Need to Increase Use of Technology" Rank	Areas Evaluated by Respondents	Degree of Technology Use (5-pt. scale)
1	IT asset management	2.8
2 (tie)	Cash receipts/applications	2.8
	Supplier management	2.6
3	Purchasing/purchase orders	3.0
4	Access controls	3.2
5 (tie)	Accounts receivable	2.9
	Revenue recognition	2.7
	Data/telecom costs	2.7

Key Questions for CAEs:

- Are you confident in your organization's processes for managing and controlling IT assets? Are you confident in the level of accuracy in the results?

- In what areas is the organization currently most vulnerable to potential fraud? How are these areas being addressed? Are you using technology effectively to prevent, detect, monitor and investigate fraud?

- Are you satisfied with the technology tools the internal audit function currently is employing to perform auditing activities? Is the internal audit function leveraging these tools to their fullest extent?

Special Section: How Internal Auditors Are Using Technology

In addition to the standard Capabilities and Needs Survey instrument, respondents were asked a series of questions related specifically to how their organizations are leveraging technology as part of various internal audit and organizational processes.

Among the notable findings:

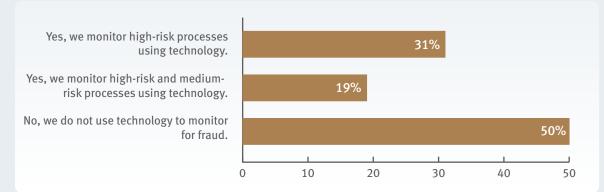**Using Technology to Administrate the Audit Process**

- More than one out of three organizations – 35 percent – are **not** utilizing any sort of software application to administrate their audit processes. Among those that are using one, 37 percent are using basic word processing or spreadsheet software to do so (more than any other tools). Of those that are not using any software application, just one in four plan to implement one within the next 12 months. Interestingly, while more large companies tend to use a software application as part of their audit processes, nearly one in five (18 percent) do not.

- Most respondents – 87 percent – noted that the tool they use delivers significant or moderate value to the audit process. However, these applications appear to be used more for basic activities such as work paper and report storage, audit plan documentation, and report writing rather than more advanced tasks such as self-assessment activities and risk and compliance project integration.

Commentary: It is surprising that internal audit's use of technology is not keeping pace with the business. Most companies are using advanced technology tools in so many parts of their businesses, yet many internal audit respondents say they are not leveraging such tools.

Using Technology to Prevent, Detect, Monitor and Investigate Fraud

- Just 17 percent of respondents, on average, believe their organizations are highly effective at preventing, detecting and monitoring fraud. The numbers are better with regard to investigating fraud, with 31 percent reporting they are highly effective in this area.

- Surprisingly, 60 percent of organizations do not leverage data analysis or technology-enabled audits to help prevent fraud. The percentages are somewhat better when it comes to detecting, monitoring and investigating fraud, with more than half of all organizations leveraging these processes.

- Only one in five organizations utilize results from their fraud risk assessments to, with the aid of technology, monitor high-risk and medium-risk processes. Of note, these results are relatively consistent across company size.

Do you utilize results from your organization's fraud risk assessment to identify business processes that need to be monitored for fraud?

- Yes, we monitor high-risk processes using technology. — 31%
- Yes, we monitor high-risk and medium-risk processes using technology. — 19%
- No, we do not use technology to monitor for fraud. — 50%

- On average, 20 percent of respondents reported that limited or poor accessibility of electronic data within their organizations hinders their efforts to prevent, detect, monitor and investigate fraud. In addition, 81 percent noted that electronic data in their organizations is either "moderately" or "partially" accessible, with just 17 percent saying it was "very" accessible.

Commentary: Here again, the underutilization of technology is surprising. Clearly, there is an opportunity to improve the use of technology as a best practice as part of fraud prevention activities. Preventive and detective tools and computer techniques are utilized in leading-edge internal audit organizations to assist line functions in managing fraud-related risk.
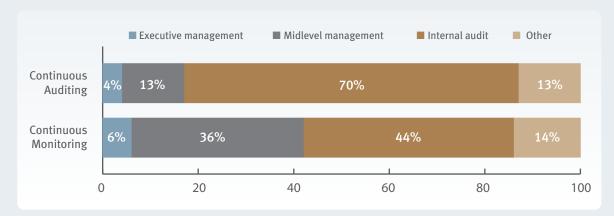
Using Technology in the Control Testing Process

- In 28 percent of organizations, technology is used in the control testing process less than 10 percent of the time or not at all. Only one in three organizations conduct internal audits in which technology is used in the control testing process more than half of the time.

Commentary: There are significant opportunities to use technology more as part of internal audit activities and specifically in the control testing process. These are surprising results that show technology continues to be underutilized significantly by internal audit functions. Leading-edge internal audit shops are increasingly relying upon technology – including advanced data analytics and tools – to test large data sets versus sampling techniques previously employed.

Continuous Auditing and Continuous Monitoring

- There is strong belief among internal audit executives and professionals (85 percent of respondents) that continuous auditing and continuous monitoring applications, techniques, scripts, etc., should be transferred to management and business process owners.

- Despite this belief, there is relatively limited involvement to date in these areas – in 60 percent of organizations, management and business process owners have no involvement in continuous audit-ing. The same holds true in 45 percent of companies with regard to continuous monitoring. For either process, management and business process owners have significant involvement in less than 10 percent of organizations.

- In a positive trend, while internal audit utilizes continuous auditing and continuous monitoring the most in organizations, in more than one in three organizations (36 percent), midlevel management is utilizing continuous monitoring processes and techniques.

Who utilizes continuous auditing and continuous monitoring the most in your organization?

	Executive management	Midlevel management	Internal audit	Other
Continuous Auditing	4%	13%	70%	13%
Continuous Monitoring	6%	36%	44%	14%

General Technical Knowledge

Key Findings – 2012

- Social media applications and cloud computing – new additions to the survey – rank as the top areas in need of improvement.
- Fraud is a prevalent theme in the survey findings and a key priority for internal auditors.

Table 3: Overall Results, General Technical Knowledge

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1	Social media applications	2.6
2	Cloud computing	2.6
3	GTAG 13 – Fraud Prevention and Detection in an Automated World	2.9
4	Fraud risk management	3.3
5	GTAG 16 – Data Analysis Technologies	2.9

Overall Findings

Respondents were asked to assess, on a scale of one to five, their competency in 57 areas of technical knowledge important to internal audit, with one being the lowest level of competency and five being the highest. For each area, they were then asked to indicate whether they believe their level of knowledge is adequate or requires improvement, taking into account the circumstances of their organization and industry. (For the areas of knowledge under consideration, see pages 10-11.) Figure 2 depicts a comparison of "Need to Improve" versus "Competency" ratings in a General Technical Knowledge landscape.

Like virtually every other department and function in organizations today, the rise of cloud computing and, in particular, the meteoric increase in the use of social media applications are having major effects on internal auditing activities. Why? First of all, both cloud computing and social media applications are relatively new. As with any new process or activity that introduces significant elements of change, social media applications and cloud computing create substantial new risks that internal audit must – in partnership with executive management and business owners – identify, assess, monitor and mitigate appropriately.

Secondly, and perhaps even more important, these technologies are in most cases being used organization-wide, from human resources and IT to sales, marketing and legal. As a result, there are many potential risks that have been introduced throughout the enterprise. Just some of these include, for cloud computing, the security policies and protocols of cloud computing vendors, access to data that may be regulated or subject to legal guidelines, and business continuity contingencies in the event of an interruption.

With regard to social media, there are numerous security, privacy, legal and reputation risks to consider. It is incumbent upon the internal audit function to work with management, the board of directors, department leaders and business process owners to develop clear social media use policies and standards, and to ensure there is ongoing compliance with these standards throughout the organization. More broadly, internal audit should partner with these executive and leadership groups to assess the risks of the organization's social media capabilities, and ensure that this risk profile fits the corporate culture and overall control environment.
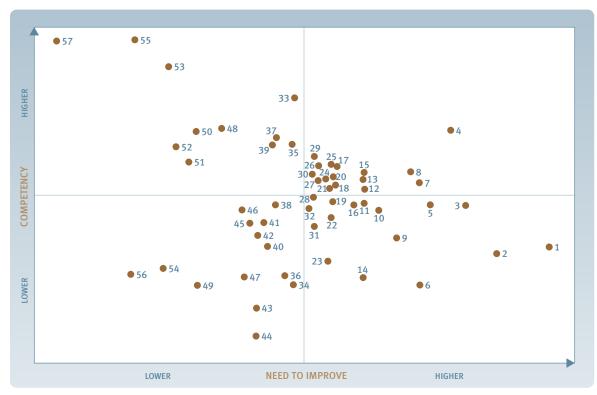
Figure 2: General Technical Knowledge – Perceptual Map

Number	General Technical Knowledge	Number	General Technical Knowledge
1	Social media applications	14	ISO 27000 (information security)
2	Cloud computing	15	IT governance
3	GTAG 13 – Fraud Prevention and Detection in an Automated World	16	GTAG 14 – Auditing User-developed Applications
4	Fraud risk management	17	IIA Practice Guide – Auditing the Control Environment
5	GTAG 16 – Data Analysis Technologies	18	GTAG 5 – Managing and Auditing Privacy Risks
6	ISO 31000 (risk management)	19	COBIT
7	IIA Practice Guide – Assessing the Adequacy of Risk Management	20	GTAG 9 – Identity and Access Management
8	IIA Practice Guide – Measuring Internal Audit Effectiveness and Efficiency	21	GTAG 12 – Auditing IT Projects
9	International Financial Reporting Standards (IFRS)	22	IIA Practice Guide – Assisting Small Internal Audit Activities in Implementing the International Standards for the Professional Practice of Internal Auditing
10	The Guide to the Assessment of IT Risk (GAIT)	23	Six Sigma
11	GTAG 6 – Managing and Auditing IT Vulnerabilities	24	GTAG 11 – Developing the IT Audit Plan
12	GTAG 15 – Information Security Governance	25	GTAG 2 – Change and Patch Management Controls
13	GTAG 3 – Continuous Auditing	26	GTAG 1 – Understanding IT Controls

Number	General Technical Knowledge	Number	General Technical Knowledge
27	GTAG 4 – Management of IT Auditing	43	Extensible business reporting language (XBRL)
28	GTAG 7 – IT Outsourcing	44	ISO 14000 (environmental management)
29	GTAG 10 – Business Continuity Management	45	Fair value accounting
30	GTAG 8 – Auditing Application Controls	46	FASB Accounting Standards Codification™
31	Reporting on Controls at a Service Organization – SSAE 16/AU 324 (replaces SAS 70)	47	Tax laws (in your applicable region/country)
32	IIA Practice Advisory 2050-3 – Relying on the Work of Other Assurance Providers	48	Corporate governance standards (or local country equivalent)
33	COSO Enterprise Risk Management Framework	49	Revenue arrangements with multiple deliverables (EITF 08-1 (ASU 2009-13))
34	ISO 9000 (quality management and quality assurance)	50	U.S. GAAP (or local country equivalent)
35	Recently enacted IIA Standards (effective January 1, 2009) – Functional Reporting Interpretation (Standard 1110)	51	Foreign Corrupt Practices Act (FCPA)
36	Evaluating executive compensation risk of Regulation S-K	52	AU Section 322 – The Auditor's Consideration of the Internal Audit Function in an Audit of Financial Statements
37	Recently enacted IIA Standard (effective January 1, 2009) – Audit Opinions and Conclusions (Standards 2010.A2 and 2410.A1)	53	COSO Internal Control Framework
38	Board risk oversight (SEC Item 407(h) of Regulation S-K)	54	Stock-based compensation
39	Recently enacted IIA Standard (effective January 1, 2009) – Overall Opinions (Standard 2450)	55	International Standards for the Professional Practice of Internal Auditing (IIA Standards)
40	IIA Practice Advisory 1312-3 – Independence of External Assessment Team in the Private Sector	56	UK Bribery Act
41	Country-specific ERM framework	57	Sarbanes-Oxley (Sections 301, 302, and 404)
42	IIA Practice Advisory 1312-4 – Independence of the External Assessment Team in the Public Sector		

Key Questions to Consider

- Is your organization deploying cloud solutions? If so, does internal audit have a clear understanding of the associated risks and how they should be managed?

- Does the company monitor technology innovations and the risks associated with new technology, including mobile technology and devices?

- Has your organization conducted an assessment of potential risks related to the use by employees of social media applications? Does the organization have a social media policy? Is internal audit engaged in ensuring compliance with this policy? Are automated technologies being employed to monitor employee and company social media activities?

- Are you keeping apprised of current and relevant GTAG standards?

Three-Year Trends

Table 4: Overall Results, General Technical Knowledge – Three-Year Comparison

Rank	2012	2011	2010
1	Social media applications	IFRS	GAIT
		GTAG 13 – Fraud Prevention and Detection in an Automated World	
2	Cloud computing	ISO 31000 (risk management)	IFRS
3	GTAG 13 – Fraud Prevention and Detection in an Automated World	Penalties in Administrative Proceedings (Dodd-Frank Act §929P)	XBRL
4	Fraud risk management	Six Sigma	ISO 27000
5	GTAG 16 – Data Analysis Technologies	Hedging by Employees and Directors (Dodd-Frank Act §955)	COBIT
		GTAG 15 – Information Security Governance	

"I BELIEVE THAT CONTINUOUS CONTROL MONITORING BY MANAGEMENT IS BECOMING A NECESSARY STEP TO PREVENT, DETECT AND MONITOR FOR FRAUD. MANAGEMENT IS RESPONSIBLE FOR PREVENTING, DETECTING AND MONITORING FOR FRAUD ON A DAY-TO-DAY BASIS. INTERNAL AUDIT CAN DEVELOP A PROGRAM BUT THEN IT SHOULD BE TRANSFERRED TO MANAGEMENT."

Chief audit executive, services company

FOCUS ON RESULTS BY COMPANY SIZE

Social media applications rank as a top priority for companies regardless of size, a further indicator that currently – though not surprisingly – there is a lack of control in this area.

Interestingly, while both social media applications and cloud computing rank as top priorities for small and midsize companies, cloud computing is absent from the top "Need to Improve" areas for large organizations, suggesting that, in terms of risk assessment and management, they have cloud computing covered. This is not a surprise considering that most of these companies have large IT shops.

Table 5: Company Size Results, General Technical Knowledge

Rank	Small ‹ $1B	Midsize $1B-9B*	Large ≥ $10B
1	Social media applications	Social media applications	Social media applications
2	Cloud computing	Cloud computing	ISO 31000 (risk management)
3	GTAG 13 – Fraud Prevention and Detection in an Automated World	GTAG 13 – Fraud Prevention and Detection in an Automated World	Evaluating executive compensation risk of Regulation S-K
3	GTAG 16 – Data Analysis Technologies	GTAG 13 – Fraud Prevention and Detection in an Automated World	Fraud risk management
4	The Guide to the Assessment of IT Risk (GAIT)	Fraud risk management	Country-specific enterprise risk management framework
5	Fraud risk management	ISO 31000 (risk management)	ISO 9000 (quality management and quality assurance)
5	IT governance	GTAG 16 – Data Analysis Technologies	Board risk oversight (SEC Item 407(h) of Regulation S-K)
5	IIA Practice Guide – Assessing the Adequacy of Risk Management	IIA Practice Guide – Assessing the Adequacy of Risk Management	Board risk oversight (SEC Item 407(h) of Regulation S-K)
5	IIA Practice Guide – Measuring Internal Audit Effectiveness and Efficiency	IIA Practice Guide – Assessing the Adequacy of Risk Management	Board risk oversight (SEC Item 407(h) of Regulation S-K)

* Upon request, Protiviti can provide additional reporting in this broad category.

FOCUS ON CHIEF AUDIT EXECUTIVES

The response from CAEs largely mirrors the overall results, with social media applications and cloud computing ranking as high "Need to Improve" areas and, thus, top priorities for these executives.

Table 6: CAE Results, General Technical Knowledge

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1	Social media applications	2.6
2	Cloud computing	2.7
3	GTAG 13 – Fraud Prevention and Detection in an Automated World	3.1
4	GTAG 16 – Data Analysis Technologies	3.0
5	International Financial Reporting Standards (IFRS)	2.9

Key Questions for CAEs:

• Do your C-level executives know the potential technology risks that your organization faces, specifically those related to the deployment and/or use of newer technologies?

• Are the expectations of C-suite and business unit executives with regard to IT consistent with how technology is managed?

• Are you completing a more specific IT risk assessment in formulating your overall audit plan?

• Have you identified and assessed the risks associated with social media usage by employees and the company?

• Is your internal audit department collaborating effectively with the business to manage shifting priorities or changes in the regulatory landscape, including but not limited to IFRS, FCPA and Dodd-Frank?

Table 7: CAE Results, General Technical Knowledge – Three-Year Comparison

Rank	2012	2011	2010
1	Social media applications	IFRS	GAIT
2	Cloud computing	GTAG 13 – Fraud Prevention and Detection in an Automated World	XBRL
3	GTAG 13 – Fraud Prevention and Detection in an Automated World	Penalties in Administrative Proceedings (Dodd-Frank Act §929P)	IFRS
		Hedging by Employees and Directors (Dodd-Frank Act §955)	
4	GTAG 16 – Data Analysis Technologies	GTAG 14 – Auditing User-developed Applications	COBIT
		GTAG 15 – Information Security Governance	
5	International Financial Reporting Standards (IFRS)	GTAG 3 – Continuous Auditing	ISO 27000
		GTAG 12 – Auditing IT Projects	

"TECHNOLOGY IS ONE ASPECT ONLY [OF PREVENTING, DETECTING AND INVESTIGATING FOR FRAUD]. THERE NEEDS TO BE AN INTEGRAL CULTURE WITHIN THE ORGANIZATION TO DETECT AND PREVENT FRAUD."

Chief audit executive, government agency

Audit Process Knowledge

Key Findings – 2012

- Consistent with findings from previous years of the study, continuous auditing and CAATs are top priorities for internal auditors.
- Continuous monitoring, a new addition to this year's survey, also ranks among the top "Need To Improve" competencies.

Table 8: Overall Results, Audit Process Knowledge

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1	Continuous auditing	3.3
2	Computer-assisted audit tools (CAATs)	3.0
3	Continuous monitoring	3.3
4	Data analysis tools – data manipulation	3.3
5	Data analysis tools – statistical analysis	3.3

Overall Findings

Respondents were asked to assess, on a scale of one to five, their competency in 52 areas of audit process knowledge, with one being the lowest level of competency and five being the highest. For each area, they were then asked to indicate whether they believe their level of knowledge is adequate or requires improvement, taking into account the circumstances of their organization and industry. (For the areas of knowledge under consideration, see pages 18-19.) Figure 3 depicts a comparison of "Need to Improve" versus "Competency" ratings in an Audit Process Knowledge landscape.

"CONTINUOUS MONITORING TOOLS, ONCE DEVELOPED AND TESTED, SHOULD FORM AN INTEGRAL PART OF THE GOVERNANCE PROCESSES MANAGED BY THE USER."

Chief audit executive, government agency

Consistent with findings from the past several years of the *Internal Audit Capabilities and Needs Survey*, continuous auditing and CAATs rank as top priorities for CAEs and internal audit professionals, together with continuous monitoring (a new category to the survey). In fact, continuous auditing and CAATs consistently have been among the top areas identified as in need of improvement since 2008. This is a strong indicator of the rapid evolution and rising prevalence of technology in business today. In addition, many organizations still have not fully embraced the use of technology tools as part of their audit processes (see special section on pages 7-8), which suggests there may be a lack of training in these areas for their internal auditors.

Furthermore, the use of these and other technologies is enabling organizations to perform millions of transactions and capture vast amounts of data on a daily basis. Organizations are looking to their internal audit functions to devise efficient and cost-effective ways to monitor these activities and review and analyze this data on a continuous, ongoing basis. Fortunately, there are a variety of auditing technologies available to accomplish this. The key is to enable internal audit team members, through education and training, to use them effectively and efficiently.

The bottom line is that there is an ongoing movement in the internal audit profession from manual, time-intensive and, in many ways, inefficient auditing (relative to today's demands) to technology-enabled auditing practices that facilitate reviews of virtually every transaction and piece of data on a continuing basis, if warranted. More and more internal audit functions are moving in this direction, yet with new technologies and innovations continuing to be introduced at a rapid rate, CAATs and continuous auditing, as well as continuous monitoring, very likely will continue to rank as top priorities for internal audit functions in future Capabilities and Needs surveys.
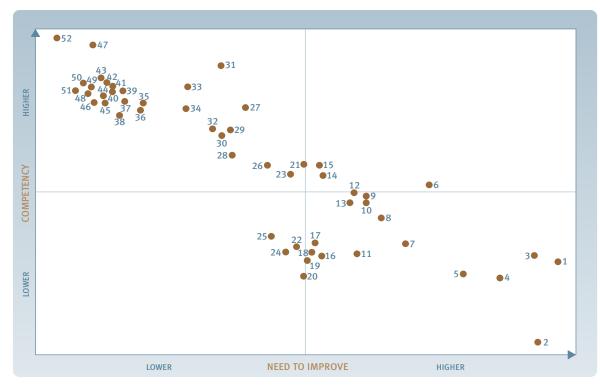
Figure 3: Audit Process Knowledge – Perceptual Map

Number	Audit Process Knowledge	Number	Audit Process Knowledge
1	Continuous auditing	17	Quality Assurance and Improvement Program (IIA Standard 1300) – Ongoing Reviews (IIA Standard 1311)
2	Computer-assisted audit tools (CAATs)	18	Auditing IT – computer operations
3	Continuous monitoring	19	Auditing IT – continuity
4	Data analysis tools – data manipulation	20	Auditing IT – program development
5	Data analysis tools – statistical analysis	21	Enterprisewide risk management
6	Marketing internal audit internally	22	Quality Assurance and Improvement Program (IIA Standard 1300) – External Assessment (Standard 1312)
7	Data analysis tools – sampling	23	Quality Assurance and Improvement Program (IIA Standard 1300) – Periodic Reviews (IIA Standard 1311)
8	Fraud – monitoring	24	Use of self-assessment techniques
9	Fraud – fraud detection/investigation	25	Auditing IT – change control
10	Fraud – fraud risk assessment	26	Operational auditing – effectiveness, efficiency and economy of operations approach
11	Fraud – management/prevention	27	Interviewing
12	Operational auditing – cost-effectiveness/cost reduction	28	Top-down, risk-based approach to assessing internal control over financial reporting
13	Statistically based sampling	29	Presenting to the audit committee
14	Fraud – auditing	30	Report writing
15	Auditing IT – security	31	Resource management (hiring, training, managing)
16	Fraud – fraud risk	32	Operational auditing – risk-based approach

Number	Audit Process Knowledge	Number	Audit Process Knowledge
33	Planning audit strategy	43	Assessing controls design (process level) – compliance controls
34	Presenting to senior management	44	Assessing controls design (process level) – operational controls
35	Assessing risk – entity level	45	Assessing controls operating effectiveness (entity level) – company-level controls
36	Assessing controls design (entity level) – tone at the top/soft controls	46	Assessing controls operating effectiveness (entity level) – monitoring controls
37	Assessing controls operating effectiveness (entity level) – tone at the top/soft controls	47	Assessing controls operating effectiveness (process level) – financial controls
38	Assessing controls design (entity level) – company-level controls	48	Audit planning – entity level
39	Assessing controls design (entity level) – monitoring controls	49	Developing recommendations
40	Assessing controls design (process level) – financial controls	50	Assessing controls operating effectiveness (process level) – compliance controls
41	Assessing risk – process, location, transaction level	51	Assessing controls operating effectiveness (process level) – operational controls
42	Audit planning – process, location, transaction level	52	Conducting opening/closing meetings

Key Questions to Consider:

- Does your organization recognize the value that continuous auditing and continuous monitoring bring to the internal control environment?
- What CAATs are currently being employed by your internal audit function?
- Are management and business process owners involved in continuous auditing and continuous monitoring efforts within your organization?
- Does the organization leverage data analysis and technology-enabled audits to prevent, detect, monitor and investigate fraud, as well as to ensure compliance with applicable laws and regulations?

Three-Year Trends

Table 9: Overall Results, Audit Process Knowledge – Three-Year Comparison

Rank	2012	2011	2010
1	Continuous auditing	Continuous auditing	CAATs
2	CAATs	CAATs	Data analysis tools – statistical analysis
			Data analysis tools – data manipulation
3	Continuous monitoring	Data analysis tools – statistical analysis	Continuous auditing
4	Data analysis tools – data manipulation	Data analysis tools – data manipulation	Auditing IT – program development
5	Data analysis tools – statistical analysis	Auditing IT – program development	Quality Assurance and Improvement Program (IIA Standard 1300) – External Assessment (Standard 1312)

FOCUS ON RESULTS BY COMPANY SIZE

These results show a prioritization within large companies on fraud-related auditing activities (monitoring, detection/investigation, management/prevention, etc.). These organizations likely see the benefits of leveraging technology in their fraud management efforts. Also of note, large companies do not view the use of data analysis tools to be the same level of priority that small and midsize companies do, suggesting that larger organizations are successfully employing and using these tools.

Operational auditing showed up this year as a priority for large companies. This may be due to a continued and strong focus on improving the bottom line. Many large organizations have struggled with the financial and economic recession over the last few years and, in order to satisfy investors and stakeholders, are looking to streamline operations wherever possible and build greater efficiencies.

Table 10: Company Size Results, Audit Process Knowledge

Rank	Small < $1B	Midsize $1B-9B*	Large ≥ $10B
1	Continuous auditing	Computer-assisted audit tools (CAATs)	Continuous auditing
			Operational auditing – cost-effectiveness/cost reduction
2	Continuous monitoring	Continuous auditing	Continuous monitoring
			Use of self-assessment techniques
3	Computer-assisted audit tools (CAATs)	Continuous monitoring	Fraud – monitoring
			Report writing
4	Data analysis tools – data manipulation	Data analysis tools – data manipulation	Resource management (hiring, training, managing)
	Data analysis tools – statistical analysis		Statistically based sampling
5	Marketing internal audit internally	Data analysis tools – statistical analysis	Computer-assisted audit tools (CAATs)
			Data analysis tools – data manipulation
			Fraud – fraud detection/investigation
			Fraud – management/prevention
			Interviewing
			Marketing internal audit internally
			Operational auditing – effectiveness, efficiency and economy of operations approach

* Upon request, Protiviti can provide additional reporting in this broad category.

FOCUS ON CHIEF AUDIT EXECUTIVES

Table 11: CAE Results, Audit Process Knowledge

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1	Computer-assisted audit tools (CAATs)	3.2
2	Continuous auditing	3.5
3	Data analysis tools – data manipulation	3.3
4	Continuous monitoring	3.5
5	Data analysis tools – statistical analysis	3.3

Key Questions for CAEs:

- Do you have adequate visibility into the IT audit function and recognize your responsibility for understanding the organization's IT risks?

- Does your company leverage qualified resources from other departments to audit critical IT-related areas?

- Are you and your auditors familiar with the various auditing tools and technologies in the market-place?

- Can your internal audit function benefit from further training or guidance in data analytics in order to audit the enterprise and business unit data in the most effective manner?

- Can you take advantage of technology-enabled auditing in identifying key cost-reduction opportunities in operational audits you perform?

Table 12: CAE Results, Audit Process Knowledge – Three-Year Comparison

Rank	2012	2011	2010
1	CAATs	Continuous auditing	CAATs
2	Continuous auditing	Data analysis tools – statistical analysis Data analysis tools – data manipulation CAATs	Continuous auditing
3	Data analysis tools – data manipulation	Data analysis tools – sampling	Data analysis tools – statistical analysis
4	Continuous monitoring	Auditing IT – computer operations	Data analysis tools – data manipulation
5	Data analysis tools – statistical analysis	Fraud – monitoring	Quality Assurance and Improvement Program (IIA Standard 1300) – External Assessment (Standard 1312)

Personal Skills and Capabilities

Key Findings – 2012

- Networking effectively and developing outside contacts are top priorities for CAEs and internal audit professionals seeking to stay apprised of leading tools and best practices.

- Other highly sought-after skills include negotiation, persuasion and dealing with confrontation.

Table 13: Overall Results, Personal Skills and Capabilities

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1	Developing outside contacts/ networking	3.5
2 (tie)	Negotiation	3.6
	Persuasion	3.7
3	Dealing with confrontation	3.6
4	Presenting (public speaking)	3.7
5	High-pressure meetings	3.7

Respondents were asked to assess, on a scale of one to five, their competency in 24 areas of personal skills and capabilities, with one being the lowest level of competency and five being the highest. For each area, they were then asked to indicate whether they believe their level of knowledge is adequate or requires improvement, taking into account the circumstances of their organization and industry. (For the areas of knowledge under consideration, see page 23.) Figure 4 depicts a comparison of "Need to Improve" versus "Competency" ratings in a Personal Skills and Capabilities landscape.

This year's results are consistent with those from the 2011 survey. Of note, developing outside contacts and networking rose to the top of the list in the latest results. As organizations and the business climate continue to evolve at a fast pace due to factors including, but not limited to, the development of new internal auditing technologies (continuous auditing, continuous monitoring, CAATs, etc.), and the ongoing introduction of new technologies and innovations in businesses (cloud computing, social media), internal auditing professionals need to keep pace with current best practices, processes and methodologies. Networking with peers and participating in professional organizations such as The IIA are effective ways to accomplish this. In addition, these activities enable internal auditing professionals to build their own credentials as leaders in their field.
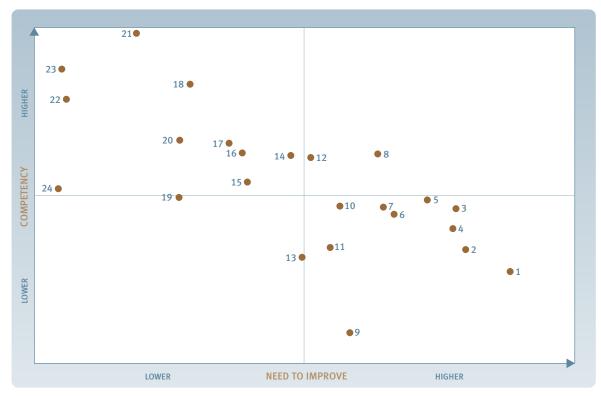
Figure 4: Personal Skills and Capabilities – Perceptual Map

Number	Personal Skills and Capabilities	Number	Personal Skills and Capabilities
1	Developing outside contacts/networking	13	Developing audit committee relationships
2	Negotiation	14	Developing rapport with senior executives
3	Persuasion	15	Creating a learning internal audit function
4	Dealing with confrontation	16	Leveraging others' expertise
5	Presenting (public speaking)	17	Coaching/mentoring
6	High-pressure meetings	18	Presenting (small groups)
7	Leadership (within your organization)	19	Change management
8	Strategic thinking	20	Personnel performance evaluation
9	Developing other board committee relationships	21	Written communication
10	Using/mastering new technology and applications	22	Working effectively with outside parties
11	Leadership (within the internal audit profession)	23	Working effectively with external auditors
12	Time management	24	Working effectively with regulators

Key Questions to Consider:

- Does your organization offer adequate training for staff in "soft" skills so they can work more effectively with various departments? Are you taking advantage of these training opportunities?

- Have you observed interactions between the company's audit professionals and management that may have been handled more effectively from a communications standpoint?

- Is leadership training offered to audit personnel?

- Are you involved with any professional organizations related to internal auditing or your industry? Are you interacting regularly with peers from other organizations?

Three-Year Trends

Table 14: Overall Results, Personal Skills and Capabilities – Three-Year Comparison

Rank	2012	2011	2010
1	Developing outside contacts/ networking	Dealing with confrontation	Presenting (public speaking)
2	Negotiation	Presenting (public speaking)	Dealing with confrontation
2	Persuasion	Presenting (public speaking)	Dealing with confrontation
3	Dealing with confrontation	Negotiation	Developing outside contacts/ networking
4	Presenting (public speaking)	Leadership (within the IA profession)	Persuasion
5	High-pressure meetings	Developing outside contacts/ networking	Strategic thinking

FOCUS ON RESULTS BY COMPANY SIZE

The survey results are largely consistent across company size. Respondents from midsize organizations noted that using and mastering new technology and applications ranks as a higher priority than that of their peers from small and large organizations. For this same group, high-pressure meetings appear to be less of a concern.

Of note, internal auditors in smaller companies tend to be less recognized than their counterparts in larger organizations and, lacking a strong voice or clout, have a more difficult time pushing through their recommendations. Thus the ranking of negotiation as the top area in need of improvement is not a surprise.

Table 15: Company Size Results, Personal Skills and Capabilities

Rank	Small < $1B	Midsize $1B-9B*	Large ≥ $10B
1	Negotiation	Developing outside contacts/ networking	Developing outside contacts/ networking
2	Dealing with confrontation	Persuasion	Dealing with confrontation
2	Presenting (public speaking)	Persuasion	Dealing with confrontation
3	Developing outside contacts/ networking	Negotiation	Negotiation
3	Persuasion	Strategic thinking	Persuasion
3	Persuasion	Using/mastering new technology and applications	Persuasion
4	High-pressure meetings	Dealing with confrontation	High-pressure meetings
4	High-pressure meetings	Presenting (public speaking)	High-pressure meetings
5	Leadership (within your organization)	Developing other board committee relationships	Leadership (within your organization)
5	Leadership (within your organization)	Leadership (within your organization)	Presenting (public speaking)

* Upon request, Protiviti can provide additional reporting in this broad category.

FOCUS ON CHIEF AUDIT EXECUTIVES

Consistent with the results from previous years, a key difference between the responses from CAEs and those of the overall group is the ranking of developing other board committee relationships as a top priority. Also of note, using and mastering new technology and applications ranks as a high priority for CAEs, whereas this ranks lower in the overall response group.

The rising level of compliance and oversight driven by regulators, shareholders and other constituencies further substantiates the need for strong working rapport with board members and senior management. Such rapport improves relationships and, in turn, helps avoid surprises on both sides of the table.

Table 16: CAE Results, Personal Skills and Capabilities

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1	Presenting (public speaking)	3.8
2 (tie)	Developing other board committee relationships	3.8
2 (tie)	Developing outside contacts/ networking	3.8
3 (tie)	Persuasion	3.9
3 (tie)	Using/mastering new technology and applications	3.6
4 (tie)	Negotiation	3.8
4 (tie)	Dealing with confrontation	3.8
5	Time management	3.9

Key Questions for CAEs:

- Does your organization offer adequate training for internal auditors so that they can work more effectively and be knowledgeable about the latest technology developments and risks?
- Is your audit team acquiring, developing and maturing the skills they need to be effective?
- Do you feel your audit department has a strong network of outside experts and contacts that they can reach out to regularly for counsel, guidance and resources?
- Are your auditors keeping apprised of current and relevant regulations and standards?
- What can you do to develop your relationships with other board committees and assist them in acting on and discharging their chartered responsibilities?

Table 17: CAE Results, Personal Skills and Capabilities – Three-Year Comparison

Rank	2012	2011	2010
1	Presenting (public speaking)	Developing other board committee relationships	Developing other board committee relationships
2	Developing other board committee relationships	Developing outside contacts/ networking	Presenting (public speaking)
2	Developing outside contacts/ networking	Time management	Presenting (public speaking)
3	Persuasion	Leadership (within the IA profession)	Developing outside contacts/ networking
3	Using/mastering new technology and applications	Leadership (within the IA profession)	Developing outside contacts/ networking
4	Negotiation	Presenting (public speaking)	Time management
4	Dealing with confrontation	Presenting (public speaking)	Time management
5	Time management	Strategic thinking	Dealing with confrontation

Survey Methodology

More than 800 respondents submitted completed surveys for Protiviti's *Internal Audit Capabilities and Needs Survey*, which was conducted from September through October 2011. The survey consisted of a series of questions grouped into four divisions: Use of Technology in Auditing Business Process Controls, General Technical Knowledge, Audit Process Knowledge, and Personal Skills and Capabilities. Participants were asked to assess their skills and competency by responding to questions concerning 199 topic areas. Respondents from the U.S. financial services, U.S. healthcare, and manufacturing industries were also asked to assess industry-specific skills (these findings are available upon request). The purpose of this survey was to elicit responses that would illuminate the current perceived levels of competency in the many skills necessary to today's internal auditors, and to determine which knowledge areas require the most improvement.

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. These details were used to help determine whether there were distinct capabilities and needs among different sizes and sectors of business or among individuals with different levels of seniority within the internal audit profession. All demographic information was provided voluntarily by respondents.

Position

Chief Audit Executive	24%
Corporate Management	4%
IT Audit Director	1%
Director of Auditing	15%
Audit Manager	21%
IT Audit Manager	4%
Audit Staff	17%
IT Audit Staff	4%
Other	10%

Industry

Financial Services	17%
Healthcare Provider (U.S.)	13%
Manufacturing	12%
Government/Education/Not-for-profit	9%
Insurance	8%
Energy	6%
Technology	4%
Retail	4%
Hospitality	3%
Healthcare Payer (U.S.)	3%
Utilities	3%
Services	2%

Industry *(continued)*

Distribution	2%
Real Estate	2%
Telecommunications	2%
Other	10%

Certification

Certified Public Accountant (CPA)/Chartered Accountant (CA)	44%
Certified Internal Auditor (CIA)	37%
Certified Information Systems Auditor (CISA)	20%
Certified Fraud Examiner (CFE)	12%
Certified Financial Services Auditor (CFSA)	4%
Certified Government Auditing Professional (CGAP)	1%
Other	38%

Size of Organization (by Gross Annual Revenue)

$20 billion or greater	12%
$10 billion - $19.99 billion	8%
$5 billion - $9.99 billion	11%
$1 billion - $4.99 billion	32%
$500 million - $999.99 million	16%
$100 million - $499.99 million	14%
Less than $100 million	7%

Type of Organization

Public	50%
Private	23%
Not-for-profit	16%
Government	8%
Other	3%

Country of Respondents

United States	83%
United Kingdom	5%
Australia	4%
Canada	1%
Switzerland	1%
Other	6%

Education Level

Professional degree	15%
Master's degree	30%
Undergraduate degree	53%
Other	2%

Years in Current Position

Less than 1 year	8%
1-4 years	44%
5-10 years	33%
Greater than 10 years	15%

Existence of Internal Audit Department

Greater than 10 years ago	49%
5-10 years ago	30%
1-4 years ago	18%
Less than 1 year ago	3%

Internal Audit Department Full-Time (or equivalent) Personnel

1-10	64%
11-20	16%
21-50	15%
Greater than 50	5%

Using Resources Through Co-Sourcing Arrangement

Yes	54%
No	46%

Percentage of Annual Audit Hours Co-Sourced to Third-Party Providers

0%	37%
1-10%	25%
11-20%	16%
21-30%	10%
31-40%	5%
41-50%	2%
51-60%	1%
61-70%	1%

Percentage of Annual Audit Hours Co-Sourced to Third-Party Providers *(continued)*

71-80%	1%
81-90%	1%
91-100%	1%

Co-Sourced Firms Used for Completing Annual Work

None	38%
Use 1 firm exclusively	31%
Use 2 to 3 firms	27%
Use more than 3 firms	4%

External Quality Assessment (Standard 1312) Conducted in Last Five Years

Yes	43%
No	45%
No, but one is scheduled	12%

Utilizing Software Application to Administrate Audit Process

Yes	65%
No	35%

If YES: Automated Internal Audit Work Paper Application Utilized

Microsoft Office Tools (Word, Excel)	37%
CCH TeamMate	32%
Internally developed software	12%
Thomson Reuters Auto Audit	12%
Protiviti Governance Portal	7%
Galileo Audit Management System	2%
IBM OpenPages Audit	1%
MetricStream	1%
Mkinsight	1%
Pentana Audit Work System	1%
Other	31%

If NO: Plans to Implement an Automated Internal Audit Work Paper Application in the Next Year

Yes	24%
No	76%

Appendix – Relevant Standards and Laws

Law/Standard	Description	Website
AU Section 322 – The Auditor's Consideration of the Internal Audit Function in an Audit of Financial Statements	Provides the external auditor with guidance on considering the work of internal auditors and on using internal auditors to provide direct assistance to the auditor in an audit performed in accordance with generally accepted auditing standards.	www.aicpa.org
Board Risk Oversight (SEC Item 407(h) of Regulation S-K)	Requires disclosure about the board leadership structure and extent of the board's role in the risk oversight of the company.	www.sec.gov
COBIT	Provides good practices across a domain and process framework and presents activities in a manageable and logical structure. COBIT's good practices represent the consensus of experts.	www.isaca.org
COSO Enterprise Risk Management Framework	Offers organizations a commonly accepted model for evaluating risk management efforts; the framework expands on internal control concepts by providing a more robust focus based on the broader subject of enterprise risk management (ERM).	www.coso.org
COSO Internal Control Framework	Developed by the Committee of Sponsoring Organizations of the Treadway Commission and sponsored by the AICPA, FEI, IIA and others. This is the most dominant control model in the United States.	www.coso.org
Extensible Business Reporting Language (XBRL)	A royalty-free, international information format designed specifically for business information, also referred to as "interactive data" by the SEC.	www.xbrl.org
Evaluating Executive Compensation Risk of Regulation S-K	Requires a company to consider how, if at all, its overall compensation for employees creates incentives that may impact its risk and management of risk.	www.sec.gov
Fair Value Accounting	Also called "mark-to-market," fair value accounting is a way to measure assets and liabilities that appear on a company's balance sheet and income statement. Measuring companies' assets and liabilities at fair value may affect their income statement. SFAS 157 defines in one place the meaning of "fair value."	www.fasb.org
FASB Accounting Standards Codification™	A major restructuring of accounting and reporting standards designed to simplify user access to all authoritative U.S. generally accepted accounting principles (GAAP) by providing the authoritative literature in a topically organized structure.	www.fasb.org
Foreign Corrupt Practices Act (FCPA)	Prohibits U.S. businesses from bribing foreign officials and requires public companies to, among other things, maintain accurate books and records.	www.justice.gov

Law/Standard	Description	Website
Global Technology Audit Guides (GTAG®)	Prepared by The Institute of Internal Auditors (The IIA), each Global Technology Audit Guide (GTAG) is written in straightforward business language to address a timely issue related to information technology management, control, and security. The GTAG series serves as a ready resource for chief audit executives on different technology-associated risks and recommended practices.	www.theiia.org
GTAG 1 – Understanding IT Controls	Explains IT controls and audit practice in a format that allows CAEs to understand and communicate the need for strong IT controls.	www.theiia.org
GTAG 2 – Change and Patch Management Controls	Helps internal auditors ask the right questions of the IT organization to assess its change management capability.	www.theiia.org
GTAG 3 – Continuous Auditing	Helps identify what must be done to make effective use of technology in support of continuous auditing, and highlights areas that require further attention.	www.theiia.org
GTAG 4 – Management of IT Auditing	Helps CAEs sort through the strategic issues regarding planning, performing, and reporting on IT audits.	www.theiia.org
GTAG 5 – Managing and Auditing Privacy Risks	Provides insight into privacy risks that the organization should address when it collects, uses, retains, or discloses personal information.	www.theiia.org
GTAG 6 – Managing and Auditing IT Vulnerabilities	Recommends specific management practices to help achieve and sustain higher levels of effectiveness and efficiency and illustrates the differences between high- and low-performing vulnerability management efforts.	www.theiia.org
GTAG 7 – IT Outsourcing	Provides information on the types of IT outsourcing activities, the IT outsourcing lifecycle, and how outsourcing activities should be managed by implementing well-defined plans that are supported by a companywide risk, control, compliance, and governance framework.	www.theiia.org
GTAG 8 – Auditing Application Controls	Provides information on the role of internal auditors regarding application controls, and how to perform a risk assessment. This guide also includes a list of common application controls, a sample audit plan, and application control review tools.	www.theiia.org
GTAG 9 – Identity and Access Management	Provides insight into what identity and access management means to an organization and recommends internal audit areas for investigation.	www.theiia.org

Law/Standard	Description	Website
GTAG 10 – Business Continuity Management	Provides insight into what BCM means to an organization and how to build a business case, and identifies common risks and requirements.	www.theiia.org
GTAG 11 – Developing the IT Audit Plan	Helps auditors understand the organization's IT environment; the applications and computer operations that are part of the IT infrastructure; how IT applications and operations are managed; and how IT applications and operations link back to the organization.	www.theiia.org
GTAG 12 – Auditing IT Projects	Provides an overview of techniques for effectively engaging with project teams and management to assess IT project risks.	www.theiia.org
GTAG 13 – Fraud Prevention and Detection in an Automated World	Focuses on IT-related fraud risks and risk assessments and how the use of technology can help internal auditors and other key stakeholders within the organization address fraud and fraud risks.	www.theiia.org
GTAG 14 – Auditing User-Developed Applications	Focuses on user-developed application (UDA) risks and building an audit of UDAs into the annual internal audit plan as appropriate.	www.theiia.org
GTAG 15 – Information Security Governance	Provides a thought process to incorporate an audit of information security governance (ISG) into the audit plan, focusing on whether the organization's ISG activity delivers the correct behaviors, practices, and execution of information security.	www.theiia.org
GTAG 16 – Data Analysis Technologies	Helps CAEs understand how to move beyond the tried and true methods of manual auditing toward improved data analysis using technology.	www.theiia.org
The Guide to the Assessment of IT Risk (GAIT)	Describes the relationships among business risk, key controls within business processes, automated controls and other critical IT functionality, and key controls within IT general controls.	www.theiia.org
IIA Practice Advisory 1312-3 – Independence of the External Assessment Team in the Private Sector	All members of the assessment team who perform the external assessment are to be independent of that organization and its internal auditing activity personnel.	www.theiia.org
IIA Practice Advisory 1312-4 – Independence of the External Assessment Team in the Public Sector	In the public sector, internal audit activities at the different tiers of government may be independent for the purpose of external assessments.	www.theiia.org

Law/Standard	Description	Website
IIA Practice Advisory 2050-3 – Relying on the Work of Other Assurance Providers	The internal auditor may rely on or use the work of other internal or external assurance providers in providing governance, risk management, and control assurance to the board.	www.theiia.org
IIA Practice Guide – Assessing the Adequacy of Risk Management	Details three approaches to assurance of the risk management process: a Process Elements approach; an approach based on Principles of Risk Management; and a Maturity Model approach.	www.theiia.org
IIA Practice Guide – Assisting Small Internal Audit Activities in Implementing the *International Standards for the Professional Practice of Internal Auditing*	Provides a working definition of the term "small internal audit activity."	www.theiia.org
IIA Practice Guide – Auditing the Control Environment	Provides guidance on the significance of the control environment; how to determine which elements of the control environment should be addressed by engagements in the periodic audit plan; how to scope, staff, and plan such engagements; and which items to consider in performing related audit work, including evaluating and reporting deficiencies.	www.theiia.org
IIA Practice Guide – Measuring Internal Audit Effectiveness and Efficiency	Helps internal auditors measure their effectiveness and efficiency by providing guidance on establishing a performance measurement process, identifying key performance measures, and monitoring and reporting on the level of customer service provided to internal audit stakeholders.	www.theiia.org
IIA Standard 1110 – Functional Reporting Interpretation	Establishes organizational independence, requiring that "the chief audit executive must report to a level within the organization that allows the internal audit activity to fulfill its responsibilities."	www.theiia.org
IIA Standards 2010.A2 and 2410.A1 – Audit Opinions and Conclusions	Describe the process of formulating and communicating audit opinions and conclusions to stakeholders.	www.theiia.org
IIA Standard 2110.A1 – Ethics Programs	The internal audit activity must evaluate the design, implementation and effectiveness of the organization's ethics-related objectives, programs and activities.	www.theiia.org
IIA Standard 2120.A2 – Fraud Risk Management	The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.	www.theiia.org

Law/Standard	Description	Website
IIA Standard 2450 – Overall Opinions	Establishes the importance of considering stakeholder expectations when issuing audit opinions and supporting these opinions with reliable evidence.	www.theiia.org
International Financial Reporting Standards (IFRS)	Developed by the International Accounting Standards Board (IASB) and intended to be applied by profit-oriented entities to their financial statements in order to provide information on financial position, operating performance and cash flow that is useful to decision-makers such as shareholders, creditors, employees and the general public.	www.iasb.org
ISO 9000 (quality management and quality assurance)	Represents an international consensus on good quality management practices consisting of standards and guidelines relating to quality management systems and related supporting standards.	www.iso.org
ISO 14000 (environmental management)	Addresses various aspects of environmental management.	www.iso.org
ISO 27000 (information security)	Provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system.	www.iso.org
ISO 31000 (risk management)	Seeks to provide a universally recognized paradigm for practitioners and companies employing risk management processes to replace the myriad of existing standards, methodologies and paradigms that differ between industries, subject matters and regions.	www.iso.org
Reporting on Controls at a Service Organization – SSAE 16/AU 324 (replaces SAS 70)	For service organizations that use subservice organizations and if the inclusive method is used, the audit report must include a written assertion by the subservice organization.	www.aicpa.org
Revenue Arrangements with Multiple Deliverables (EITF 08-1 (ASU 2009-13))	Provides criteria required to separate arrangements with multiple deliverables into individual units of accounting, as well as the amount to allocate to each unit of accounting.	www.fasb.org
Sarbanes-Oxley Section 301 (Complaints regarding accounting, internal controls or auditing matters)	Directs the national securities exchanges and national securities associations to prohibit the listing of any security of an issuer that is not in compliance with the audit committee requirements mandated by the Sarbanes-Oxley Act of 2002.	www.sec.gov

Law/Standard	Description	Website
Sarbanes-Oxley Section 302 (Disclosure controls and procedures)	Addresses all financial information disclosed to investors, including MD&A in Forms 10Q and 10K.	www.sec.gov
Sarbanes-Oxley Section 404 (Internal control over financial reporting)	Requires issuers to publish information in their annual reports concerning the scope, adequacy and effectiveness of the internal control structure and procedures for financial reporting.	www.sec.gov
Six Sigma	A disciplined, data-driven approach and methodology for eliminating defects (driving towards six standard deviations between the mean and the nearest specification limit) in any process, from manufacturing to transactional and from product to service.	www.isixsigma.com
Standards for the Professional Practice of Internal Auditing (IIA Standards)	Principles-focused; provides a framework for performing and promoting internal auditing.	www.theiia.org
Stock-Based Compensation (FAS 123R Share-Based Payment)	Requires all entities (with limited exceptions) to recognize the fair value of share-based payment awards. Thus entities must address challenging issues in accounting for options and other share-based payment awards.	www.fasb.org
UK Bribery Act	Guidance to help commercial organizations understand the sorts of procedures they can put in place to prevent bribery.	www.justice.gov.uk
U.S. GAAP	Comprised of many standards, interpretations, opinions and more that are developed by the Financial Accounting Standards Board (FASB), the American Institute of Certified Public Accountants (AICPA) and the Securities and Exchange Commission (SEC).	www.fasb.org

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 Global 500 companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is proud to be a Principal Partner of The IIA. More than 700 Protiviti professionals are members of The IIA and are actively involved with local, national and international IIA leaders to provide thought leadership, speakers, best practices, training and other resources that develop and promote the internal audit profession.

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

Internal Audit and Financial Controls

We work with audit executives, management and audit committees at companies of virtually any size, public or private, to assist them with their internal audit activities. This can include starting and running the activity for them on a fully outsourced basis or working with an existing internal audit function to supplement their team when they lack adequate staff or skills. Protiviti professionals have assisted hundreds of companies in establishing first-year Sarbanes-Oxley compliance programs as well as ongoing compliance. We help organizations transition to a process-based approach for financial control compliance, identifying effective ways to appropriately reduce effort through better risk assessment, scoping and use of technology, thus reducing the cost of compliance. Reporting directly to the board, audit committee or management, as desired, we have completed hundreds of discrete, focused financial and internal control reviews and control investigations, either as part of a formal internal audit activity or apart from it.

One of the key features about Protiviti is that we are not an audit/accounting firm, thus there is never an independence issue in the work we do for clients. Protiviti is able to use all of our consultants to work on internal audit projects – this allows us at any time to bring in our best experts in various functional and process areas. In addition, Protiviti can conduct an independent review of a company's internal audit function – such a review is called for every five years under standards from The Institute of Internal Auditors.

Among the services we provide are:

- Internal Audit Outsourcing and Co-Sourcing
- Financial Control and Sarbanes-Oxley Compliance
- Internal Audit Quality Assurance Reviews and Transformation
- Audit Committee Advisory

For more information about Protiviti's Internal Audit and Financial Controls solutions, please contact:

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

Other Thought Leadership from Protiviti

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

- **2011 Sarbanes-Oxley Compliance Survey – Where U.S.-Listed Companies Stand: Reviewing Cost, Time, Effort and Processes**

- **2011 IT Audit Benchmarking Survey**

- **Board Risk Oversight – A Progress Report (from COSO and Protiviti): Where Boards of Directors Currently Stand in Executing Their Risk Oversight Responsibilities**

- **Changes to The IIA Standards: What Board Members and Executive Management Need to Know**

- **Cloud Computing: Internal Audit's Role in Identifying Risks, Defining Strategy, Evaluating the Implementation Process and Monitoring Vendor Relationships**

- **FS Insights** – "Setting the 2012 Audit Committee Agenda for Financial Institutions"

- **Guide to Internal Audit: Frequently Asked Questions About Developing and Maintaining an Effective Internal Audit Function** (Second Edition)

- **Guide to International Financial Reporting Standards: Frequently Asked Questions** (Second Edition)

- **Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements** (Fourth Edition)

- **Internal Audit Capabilities and Needs Survey** (2006-2011)

- **Internal Auditing Around the World** (Volumes 1-7)

- **Powerful Insights (Protiviti's podcast series)**
  - Enterprise Risk Management and Board Risk Oversight – A Tale of Two Surveys from COSO
  - Fraud Risk Assessment – Identifying Vulnerabilities to Fraud and Misconduct
  - Fraud Risk Management: Safeguarding Your Reputation and Well-Being in Today's Economic Climate
  - Internal Audit Quality Assessment Reviews – Required as well as Beneficial
  - Sarbanes-Oxley Compliance: Where U.S.-listed Companies Stand Today
  - Technology-Enabled Audits – Increasing Productivity and Delivering More Timely and Reliable Results
  - The Benefits of Outsourcing the Internal Audit Function
  - COSO Issues Exposure Draft for Updated Internal Control – Integrated Framework
  - Top Business Challenges in 2012
  - Social Media Use in Companies – Managing the Risks Effectively

- **Social Media and Internet Policy and Procedure Failure – What's Next?**

- **Spreadsheet Risk Management: Frequently Asked Questions**

- **Testing the Reporting Process – Validating Critical Information**

- **The Bulletin** – "Setting the 2012 Audit Committee Agenda for Non-Financial Services Companies"

- **Using High Value IT Audits to Add Value and Evaluate Key Risks and Controls**

KnowledgeLeader^{SM} provided by protiviti®

KnowledgeLeader^{SM} 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 800 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 Model^{SM}, 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 KLplus^{SM}. 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

AUSTRALIA
Garran Duncan
+61.3.9948.1205
garran.duncan@protiviti.com.au

BELGIUM
Jaap Gerkes
+31.6.1131.0156
jaap.gerkes@protiviti.nl

BRAZIL
Ricardo Lemos
+55.11.5503.2020
ricardo.lemos@protivitiglobal.com.br

CANADA
Carmen Rossiter
+1.647.288.4917
carmen.rossiter@protiviti.com

CHINA (Hong Kong and Mainland China)
Albert Lee
+852.2238.0499
albert.lee@protiviti.com

FRANCE
Francis Miard
+33.1.42.96.22.77
f.miard@protiviti.fr

GERMANY
Michael Klinger
+49.69.963.768.155
michael.klinger@protiviti.de

INDIA
Adithya Bhat
+91.22.6626.3310
adithya.bhat@protiviti.co.in

ITALY
Alberto Carnevale
+39.02.6550.6301
alberto.carnevale@protiviti.it

JAPAN
Yasumi Taniguchi
+81.3.5219.6600
yasumi.taniguchi@protiviti.jp

MEXICO
Roberto Abad
+52.55.5342.9100
roberto.abad@protiviti.com.mx

MIDDLE EAST
Manoj Kabra
+965.2295.7700
manoj.kabra@protivitiglobal.com.kw

THE NETHERLANDS
Jaap Gerkes
+31.6.1131.0156
jaap.gerkes@protiviti.nl

SINGAPORE
Matthew Field
+65.6220.6066
matthew.field@protiviti.com

SOUTH KOREA
Jeong Suk Oh
+82.2.3483.8200
jeongsuk.oh@protiviti.co.kr

SPAIN
Andrew Clinton
+44.20.7024.7570
andrew.clinton@protiviti.co.uk

UNITED KINGDOM
Andrew Clinton
+44.20.7024.7570
andrew.clinton@protiviti.co.uk

UNITED STATES
Brian Christensen
+1.602.273.8020
brian.christensen@protiviti.com

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	Woodbridge
Denver	Portland	
Fort Lauderdale	Richmond	
Houston	Sacramento	

ARGENTINA
Buenos Aires*

BRAZIL
Rio de Janeiro*
São Paulo*

CANADA
Kitchener-Waterloo
Toronto

MEXICO
Mexico City*

PERU
Lima*

VENEZUELA
Caracas*

ASIA-PACIFIC

AUSTRALIA
Brisbane
Canberra
Melbourne
Perth
Sydney

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

INDIA
Bangalore
Mumbai
New Delhi

INDONESIA
Jakarta**

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

SOUTH KOREA
Seoul

EUROPE

FRANCE
Paris

GERMANY
Frankfurt
Munich

ITALY
Milan
Rome
Turin

SPAIN
Madrid

THE NETHERLANDS
Amsterdam

UNITED KINGDOM
London

MIDDLE EAST

BAHRAIN
Manama*

KUWAIT
Kuwait City*

OMAN
Muscat*

UNITED ARAB EMIRATES
Abu Dhabi*
Dubai*

 * Protiviti Member Firm
** Protiviti Alliance Member

protiviti®
Risk & Business Consulting.
Internal Audit.