Assessing the Top Priorities for Internal Audit Functions

2014 Internal Audit Capabilities and Needs Survey

protiviti®
Risk & Business Consulting.
Internal Audit.

Powerful Insights. Proven Delivery.®

Introduction

In organizational psychology, “proactivity” refers to behavior that is *anticipatory*, *change-oriented* and *highly adaptive*. Why is this noteworthy? Because such behaviors, and professionals who practice them, are in great demand throughout internal audit functions, according to the results of our 2014 Internal Audit Capabilities and Needs Survey.

Internal audit functions must anticipate and respond to a constant stream of new challenges – many of which deliver uncertain and still unfolding risk implications, from emerging technologies and new auditing requirements and standards to rapidly evolving business conditions.

For example, in nearly every company over the past 12 months, the use of mobile and social media applications has presented new challenges, many of which are still emerging. Organizations’ growing reliance on cloud computing and data, in general, poses similarly complex challenges.

Yet, these issues represent only a portion of those crowding internal audit’s 2014 priority list. Our findings show that:

- **Social media, mobile applications, cloud computing and security (specifically with regard to the NIST Cybersecurity Framework) are critical areas of concern** – Social media applications and related risks are top priorities for internal auditors to address, as are risks surrounding mobile applications, cloud computing and security.
- **CAATs and data analysis remain on center stage** – As indicated in past years of our study, internal auditors plan to strengthen their knowledge of computer-assisted auditing tools, and continuous auditing and monitoring techniques. Additionally, internal audit functions intend to leverage more advanced forms of data analysis to support risk management and overall business objectives.
- **Fraud management efforts focus more on technology as well as prevention** – Auditors are concentrating more time and attention on fraud prevention and detection in increasingly automated business environments and workplaces.
- **“We have to keep pace with a raft of regulatory, rules-making and standards changes”** – The updated COSO Internal Control – Integrated Framework represents a major change for internal audit, with significant implications for many financial, risk management and compliance activities. However, strengthening knowledge of the new COSO framework ranks as a lower priority compared to other critical rules-making changes internal auditors are digesting, including new Standards from The Institute of Internal Auditors (IIA) and new cybersecurity guidelines from the U.S. government.
- **Internal auditors want to take their collaboration with business partners to a new level** – Internal audit’s longstanding desire to improve collaboration with the rest of the business has intensified, as is evident in the priority that CAEs and respondents place on communicating, and even marketing, the expertise and value that internal audit provides to the rest of the enterprise.

We are pleased that more than 600 CAEs and internal audit executives and professionals participated in our study this year. They represent a broad range of industries and organizations (see the Methodology and Demographics section for details). We greatly appreciate the time they invested in our study.

In closing, we once again acknowledge the tremendous global leadership provided by The IIA for our profession in advancing the role of internal audit functions in business today.

Protiviti
March 2014

Social Media Risk and the Audit Process

Key Findings

- More organizations are formalizing processes for managing social media risk – this is evident in the increasing adoption of social media policies and growing inclusion of social media considerations in audit plans and risk assessment efforts.
- Executive management is becoming more interested and involved in the management of social media risk.
- Financial loss is viewed to pose the highest level of social media risk; monitoring reputation risk stands out as the greatest benefit to addressing social media risk.
- Significant improvements remain necessary, particularly related to the inclusion of social media evaluations in audit plans as well as the integration of social media into incident response activities.

For the second consecutive year in our survey, we examine social media risk and how it is being integrated into audit and risk management processes within organizations. In this part of our study, we:

- Generate a snapshot of social media usage and management in organizations.
- Identify how internal audit is addressing social media risk.
- Flesh out obstacles that inhibit internal audit's understanding, assessment and monitoring of social media risk.

Social media risk management remains a crucial capability within internal audit functions. Our results indicate several signs of progress in developing and applying this capability. Executive management teams also appear more aware of social media's importance as an audit and risk management issue, and more willing to participate in shaping and managing their organization's social media risk management capabilities.

That said, the results suggest more progress is needed.

Social Media Use: External Communications and Policies on the Rise

For internal auditors, the evolving use of social media within the enterprise presents significant challenges from a risk management standpoint. This should come as no surprise: Social media is a top-of-mind issue throughout most organizations today. Of note, it also was ranked among the top technology challenges in Protiviti's 3rd Annual IT Audit Benchmarking Survey.[1]

Two crucial steps to address social media risks include establishing a social media strategy and developing a related social media policy.

[1] www.protiviti.com/ITAuditSurvey.

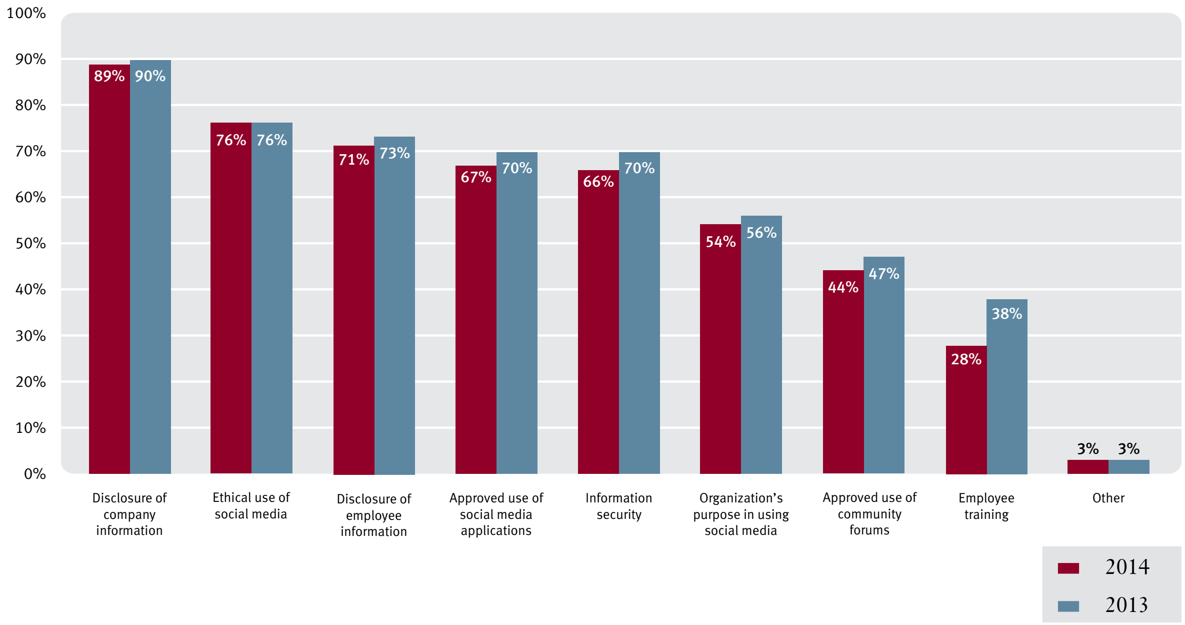
Does your organization have the following in place?

	Yes		No	
	2014	2013	2014	2013
Social media strategy	55%	53%	45%	47%
Social media policy	63%	57%	37%	43%

Interestingly, while there is little year-over-year change in the results for social media strategy, there is a significant increase in the number of organizations with a social media policy.

As noted in the accompanying chart, most policies address areas such as disclosure of company and employee information, ethical use of social media, and approved applications. Of note, fewer companies appear to be leveraging social media for employee training (as indicated in our year-over-year results).

If your organization has a social media policy, which of the following areas does it address?



Additionally, it appears that while fewer organizations are leveraging social media technologies for purposes of internal communications, more are doing so as part of their external communication efforts.

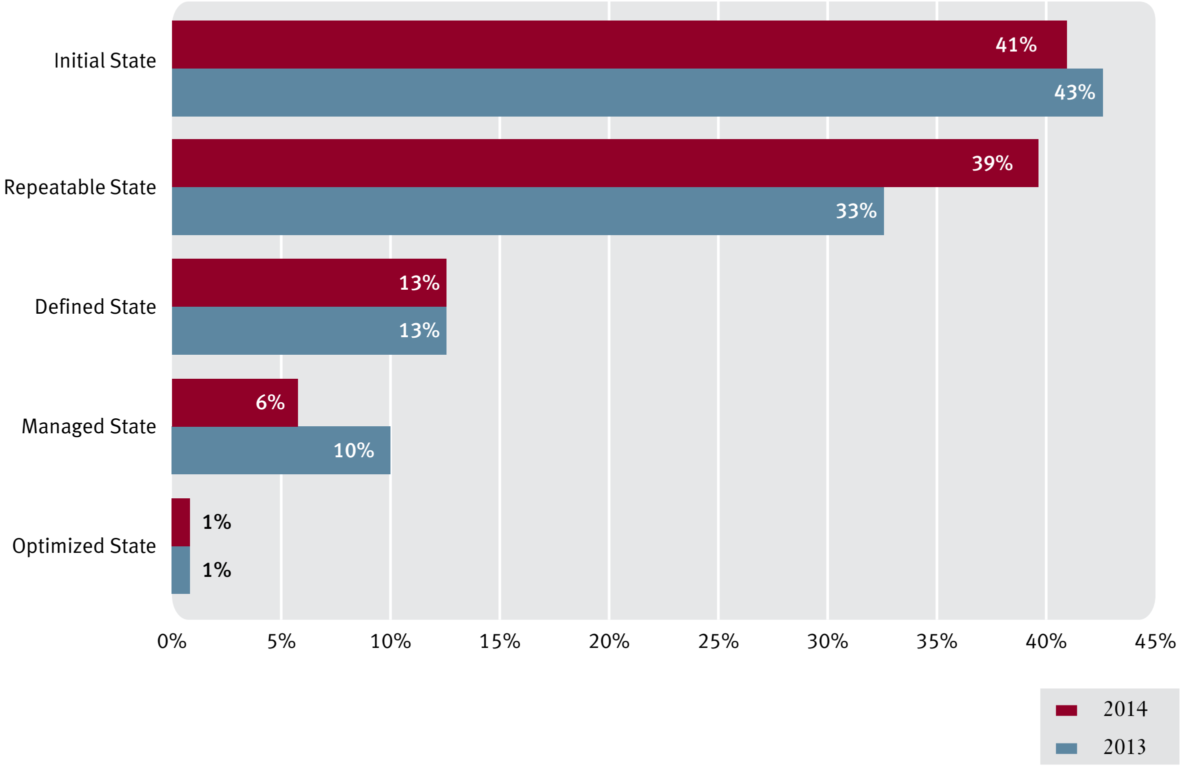
Most organizations implementing social media in a significant way are doing so because of the value they expect to receive from it. In most cases, that value is increased revenue. The role social media plays in increasing sales is through attracting new customers, creating market excitement around products and using current customers as sales liaisons, among other activities. All of this revolves around communicating externally, which is why more organizations are emphasizing social media campaigns.

How does your organization currently leverage social media technology for the following?

Activity	Yes		No	
	2014	2013	2014	2013
External communication	74%	64%	26%	36%
Internal communication	39%	44%	61%	56%

These results also explain, in part, why marketing and PR/communications staff appear to be more heavily involved in assessing the organization's social media risk exposure (see page 7).

Using the following Capability Maturity Model (adapted from the Carnegie Mellon Institute), how would you rate the current state of your organization's social media process?

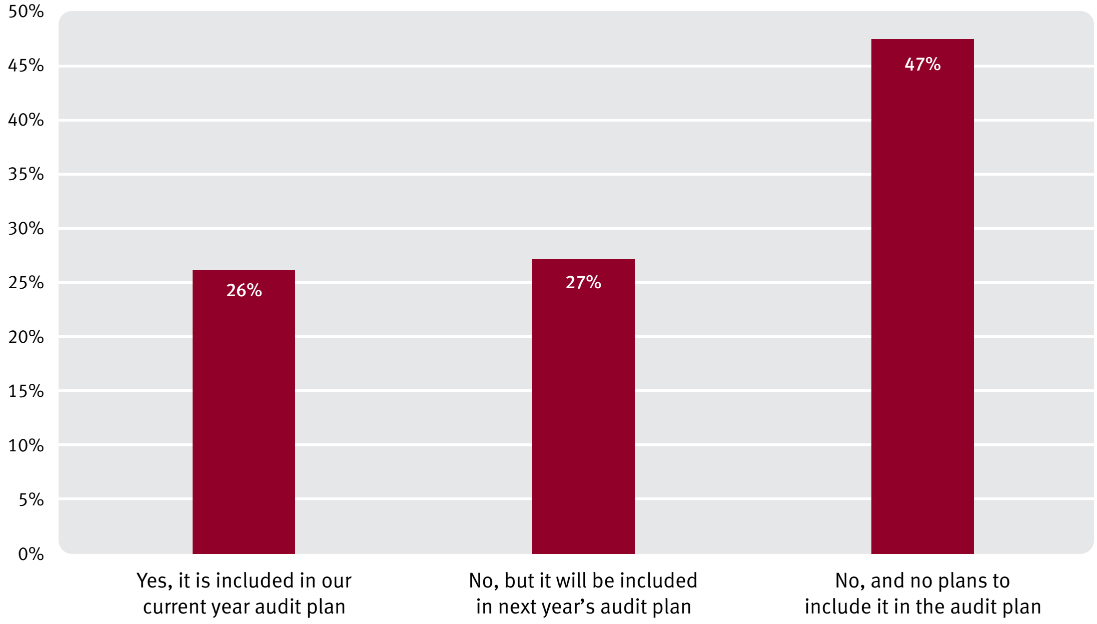


Social media processes continue to rate at the lower end of the maturity scale for most organizations, illustrating that, in many respects, companies are just getting started in establishing their social media risk management capabilities.

It is encouraging that 53 percent of organizations are addressing cybersecurity risks related to social media in their audit plans, or will do so next year (see next page). However, much more progress is needed, particularly given recent national attention on cyber attacks as well as federal regulations released in 2014.[2]

[2] *Protiviti Flash Report*, "Cybersecurity Framework: Where Do We Go From Here?", February 25, 2014, www.protiviti.com/en-US/Documents/Regulatory-Reports/Information-Technology/IT-FlashReport-NIST-Cybersecurity-Framework-Where-Do-We-Go-From-Here-022514-Protiviti.pdf.

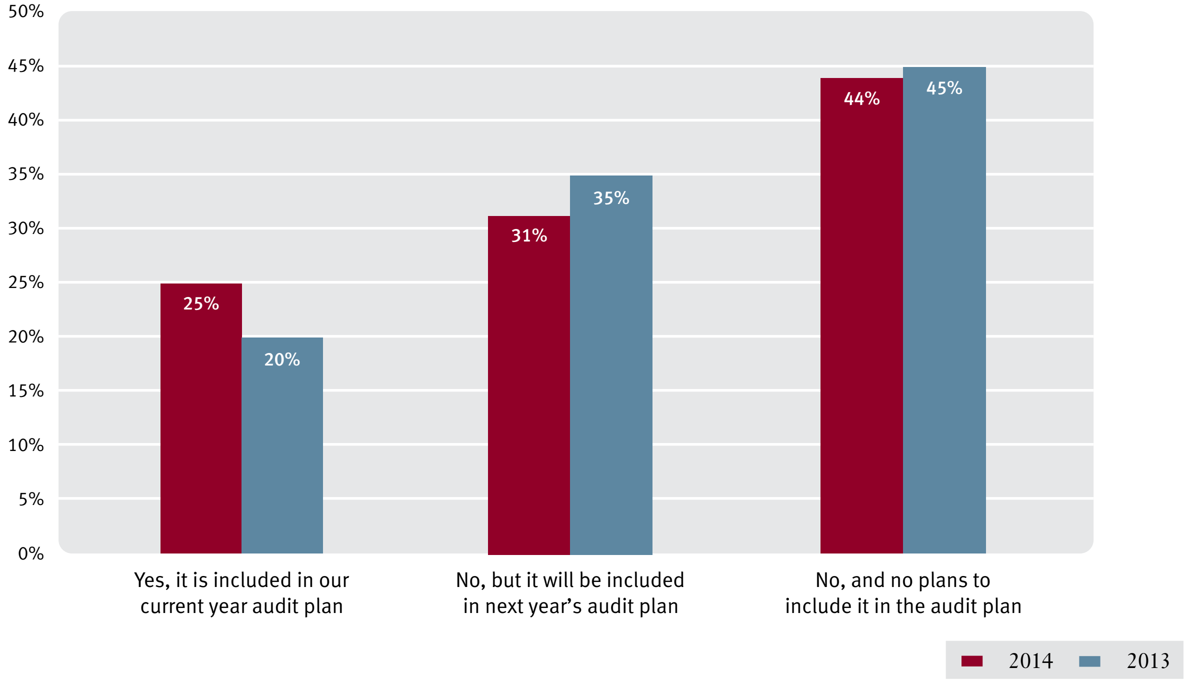
Does your audit plan specifically address cybersecurity risk related to the use of social media?



Addressing Social Media in the Audit Process

Consistent with last year's findings, a majority of organizations either have included social media risk in their audit plans or plan to do so next year, but many still do not and have no plans to do so.

Is evaluating and auditing social media risk part of your audit plan?



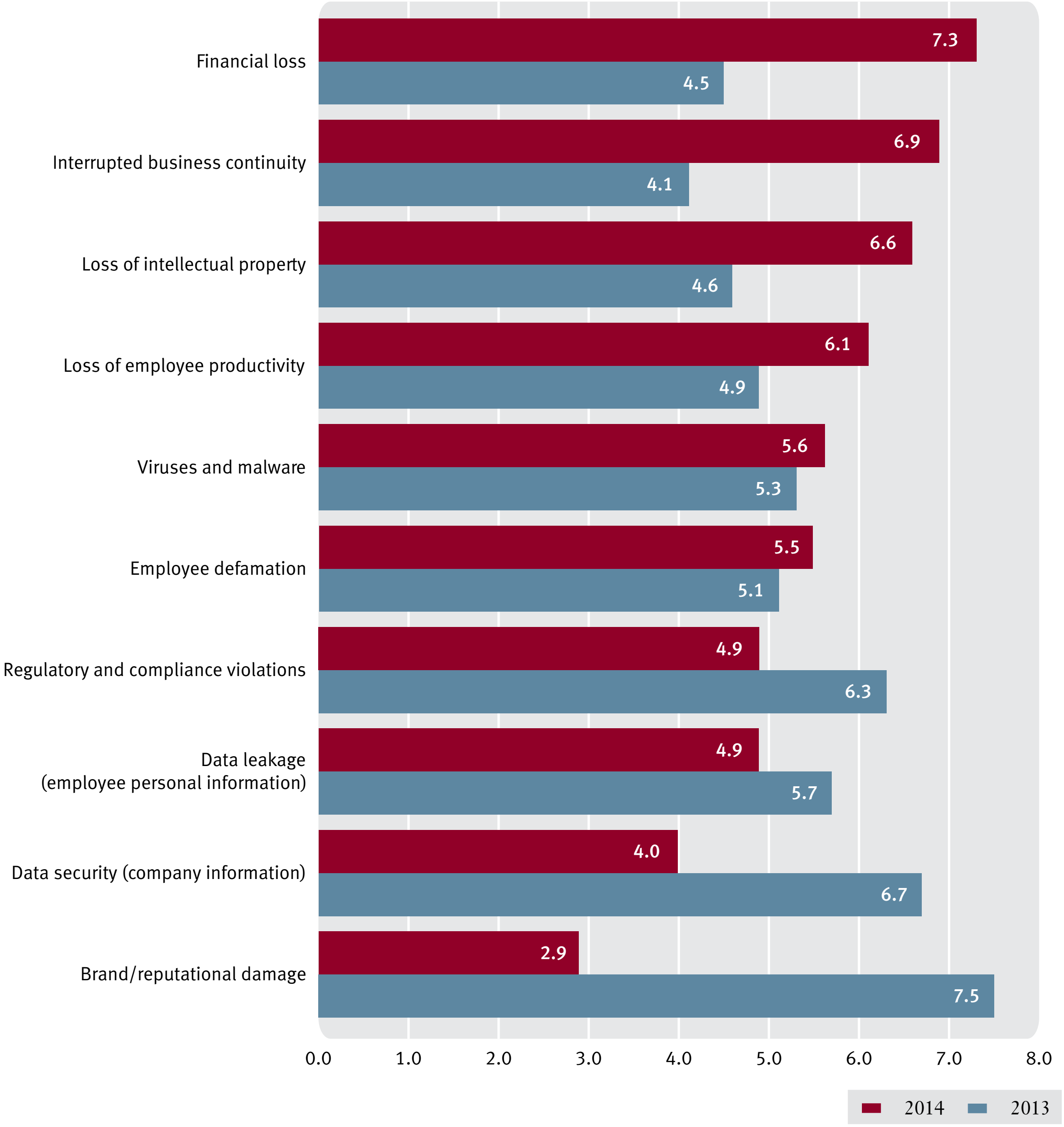
Given the minimal year-over-year change in the results, it is possible that internal audit professionals are underestimating the obstacles preventing, or delaying, the inclusion of social media risk in the audit plan; otherwise, we would expect to see a significantly higher percentage of organizations evaluating and auditing these areas.

Our respondents also rated issues deemed to pose the highest level of social media risk. They include:

- Financial loss
- Interrupted business continuity
- Loss of intellectual property
- Loss of employee productivity
- Viruses and malware

These motivations are compelling; direct hits to the bottom line represent the most frequently cited social media risk. These reasons should persuade the board, executive management and chief audit executives to take a more active and vigilant approach to managing social media risks.

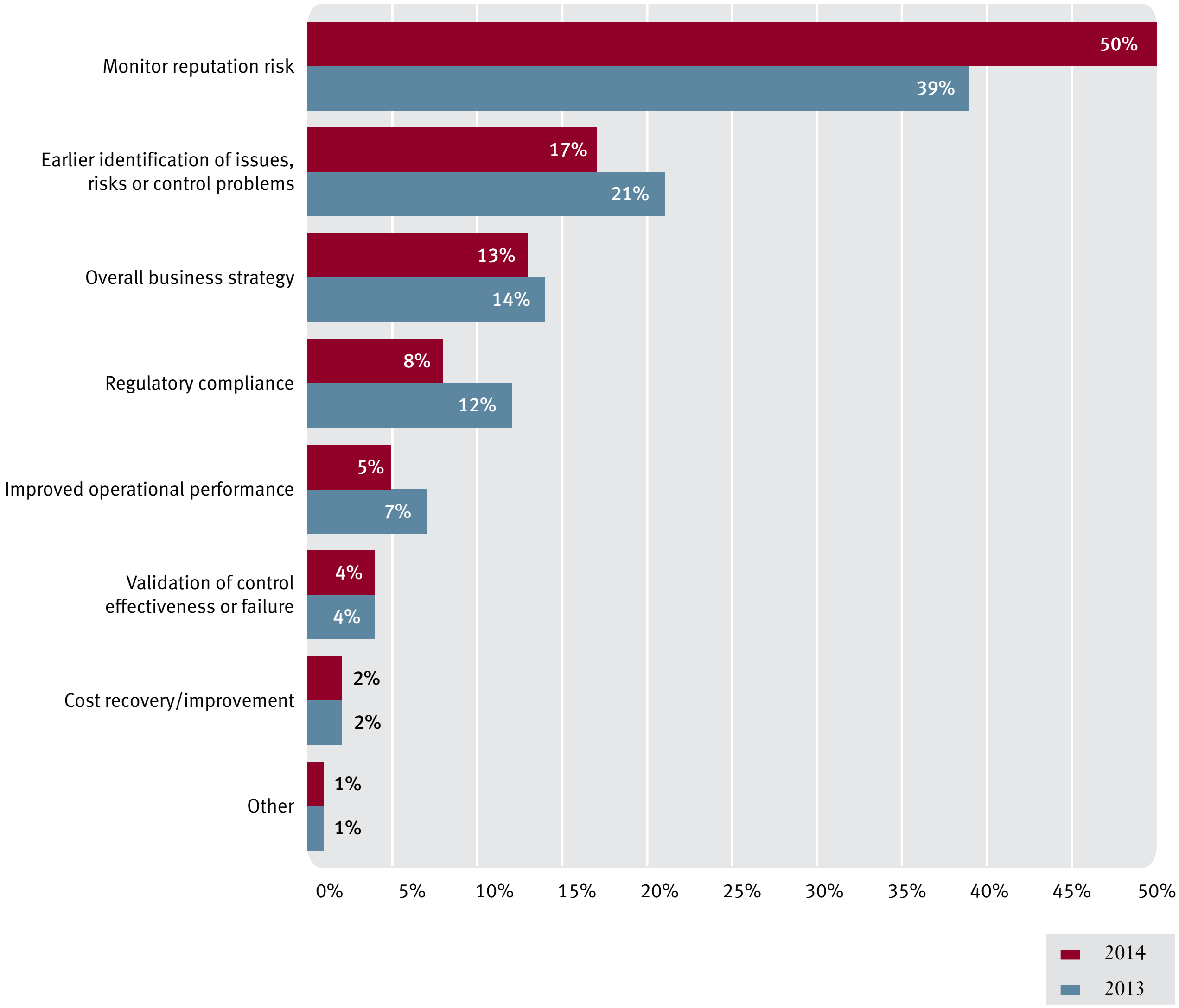
On a scale of 1 to 10, with 10 representing the highest risk level and 1 indicating the lowest risk level, please rate the level of social media risk that each of the following areas poses to your organization.



There are some interesting year-over-year trends in these findings:

- Financial loss rose to the top of the list this year.
- Business continuity rose nearly three points, ranking as the second-highest social media risk.
- Data leakage and security dropped to the lower end of the spectrum with regard to social media risk, suggesting that while these represent critical risks for organizations to manage, they may be viewed as less severe specifically with regard to social media usage.

Where do you currently perceive the greatest value for addressing social media risk to your organization?

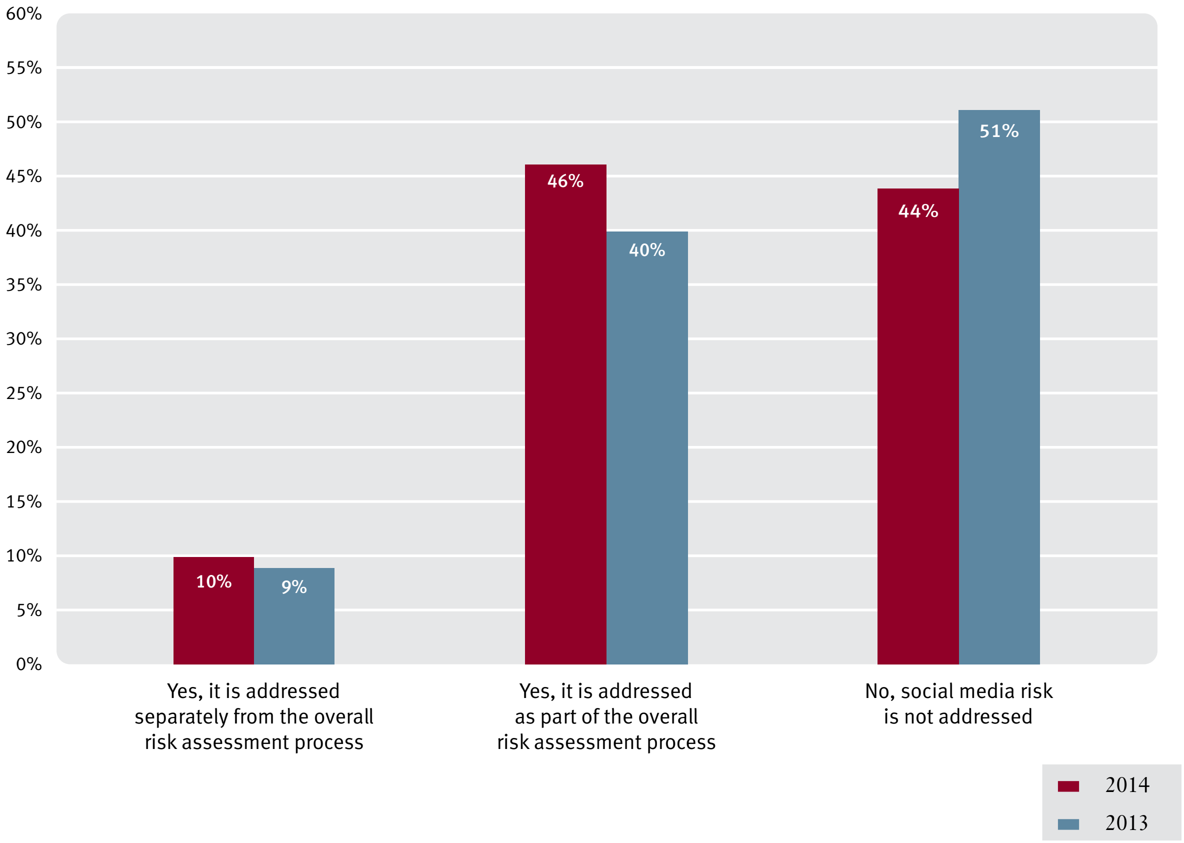


As noted in the results above, monitoring reputation risk stands out as the area in which organizations see the greatest value in addressing social media risk – in fact, this increased significantly compared to last year's results. Other notable benefits:

- Earlier identification of issues, risks or control problems
- Overall business strategy
- Regulatory compliance

Although just one in four organizations are evaluating social media risk as part of their current audit plans, 56 percent address social media in their risk assessment processes – a 7-point increase from last year's results.

Does your organization address social media in its risk assessment?



This assessment work, our respondents indicated, requires a high degree of collaboration across numerous functions and business units. According to our results, those functions that play the most significant role in the assessment of social media risks include:

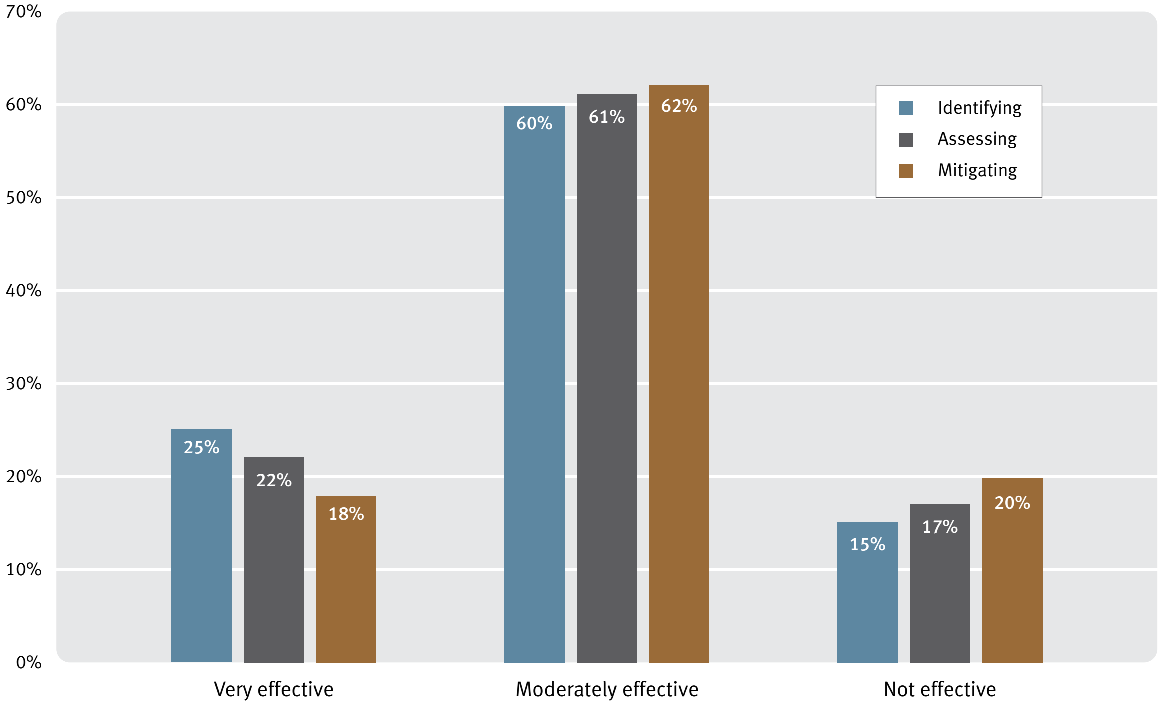
- Marketing/PR/Corporate communications
- Information technology
- Internal audit/IT audit
- Legal
- Executive management

The marketing/PR/corporate communications function showed a significant year-over-year increase in its level of involvement in assessing the organization's social media risk exposure. This is not surprising when considering the growing and widespread use of social media activities in an organization's external marketing and communications activities (as noted earlier).[3]

[3] See related findings on page 1 regarding external communications.

Social Media and Risk Management Obstacles

How effective is your organization at identifying/assessing/mitigating social media risk to an acceptable level?*

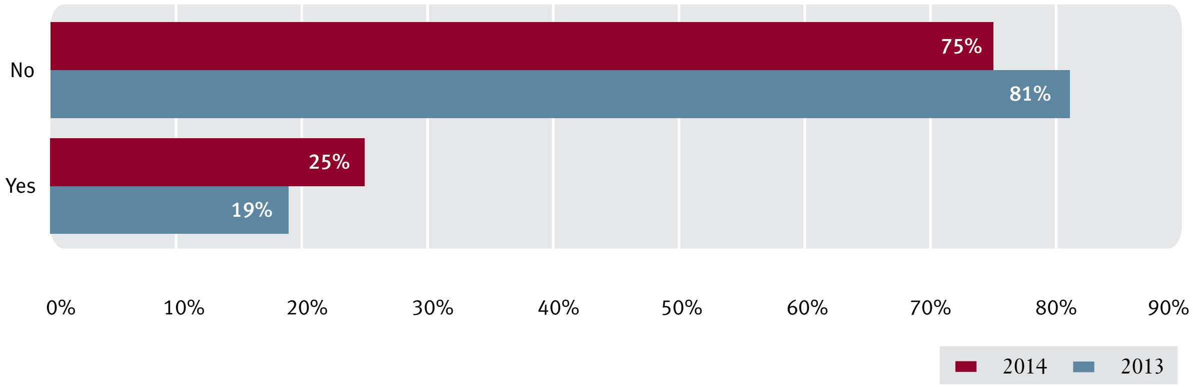


* Note: These results closely mirror the response in our 2013 study.

What is most interesting here is the relatively high percentage of organizations rating their ability to identify, assess and mitigate social media risk as moderately effective or better when, as reported earlier, 44 percent do not evaluate or audit social media risk as part of their audit plan. Similarly, 44 percent have no plans to include social media risk as part of their risk assessment processes.

Clearly, there is progress to be made, but improving social media risk management capabilities is impeded by several obstacles, the most prevalent of which may be staffing. One in four of our respondents indicated that a lack of skills and resources prevents them from addressing social media risk sufficiently in their audit plans – a 6-point increase compared to our 2013 results.

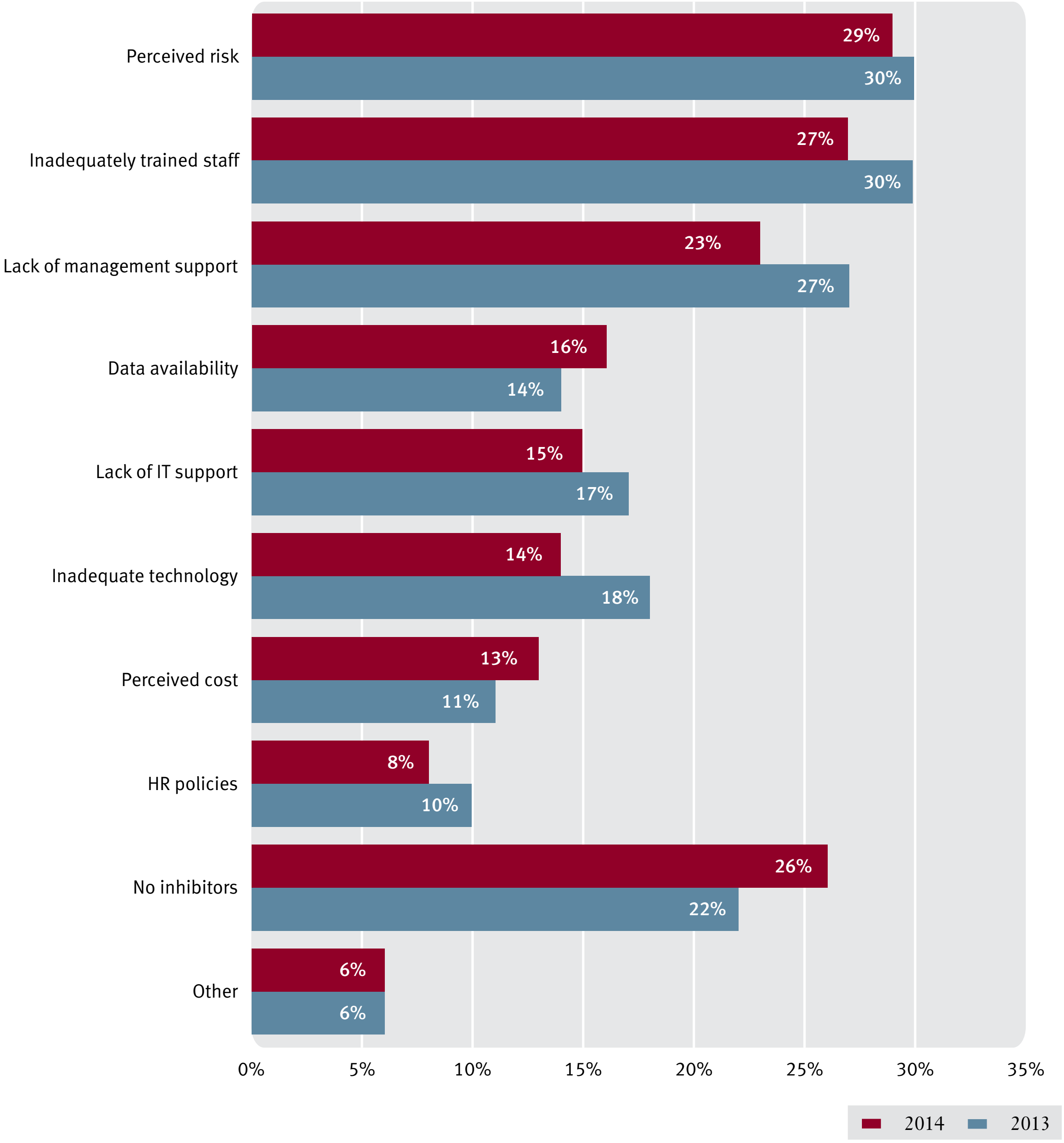
Are there specific areas of social media risk that you are not able to address sufficiently in your audit plan due to lack of resources/skills?



Furthermore, it is clear that inadequately trained staff continues to pose a formidable roadblock (though there was a slight decrease in the year-over-year results). Internal audit functions may possess enough people to address social media risk, but not the right skills. This issue can be addressed by raising awareness, providing training, and expanding collaborations with IT, marketing and communications, executive management, legal, and business process owners within the organization, as well as with external experts.

Armed with this understanding, internal audit can more effectively address other inhibitors, including confusing perceptions of social media risk throughout the organization, lack of management support, data availability problems and insufficient IT support.[4]

What inhibits internal audit's involvement in assessing social media risk?



[4] For additional information on managing social media risk, read Issue 43 of Protiviti's *Board Perspectives: Risk Oversight* newsletter, "Social Business: What it Means to Your Risk Profile," available at www.protiviti.com.

General Technical Knowledge

Key Findings

- Mobile applications, cloud computing and social media applications are top priorities for internal auditors to address in the coming year.
- Enhancing big-data-related knowledge and data analysis capabilities – via guidance provided in The IIA's GTAG 16 (Data Analysis Technologies), for example – represents a key focal point for internal audit functions.
- New guidance and standards are drawing significant attention – not only the new COSO framework, but also myriad standards from The IIA, ISO and NIST (cybersecurity).

Overall Results, General Technical Knowledge

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1	Mobile applications	2.6
2	NIST Cybersecurity Framework	2.4
3	Social media applications	2.8
4	Cloud computing	2.8
5	GTAG 16 – Data Analysis Technologies	2.9

Commentary – Overall Findings

Respondents were asked to assess, on a scale of one to five, their competency in 49 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 12-13.) Figure 1 depicts a comparison of "Need to Improve" versus "Competency" ratings in a General Technical Knowledge landscape.

Judging from this year's results, an internal auditor's skills-development and knowledge-acquisition workload appears to have no boundaries. These workloads are challenging on two fronts.

First, there is the sheer number of changes in guidance and standards. COSO's new framework was finalized and published last year.[5] This significant overhaul – the first to the framework since it was initially introduced more than two decades ago – governs much of internal audit's work as well as the organization's financial reporting and related risk management and compliance activities.

However, the new COSO framework represents just one of dozens of knowledge areas respondents are scrambling to learn. In addition to grasping the 17 internal control principles at the heart of the new COSO framework, internal auditors want to enhance their understanding of recently enacted guidance from The IIA that addresses, among other areas, data analysis technologies, IT security, and fraud prevention and detection in an automated world. Additionally, survey respondents expressed a need to improve their knowledge of IIA Standards 1110, 2010.A2, and 2410.A1.

Internal Audit Action Items

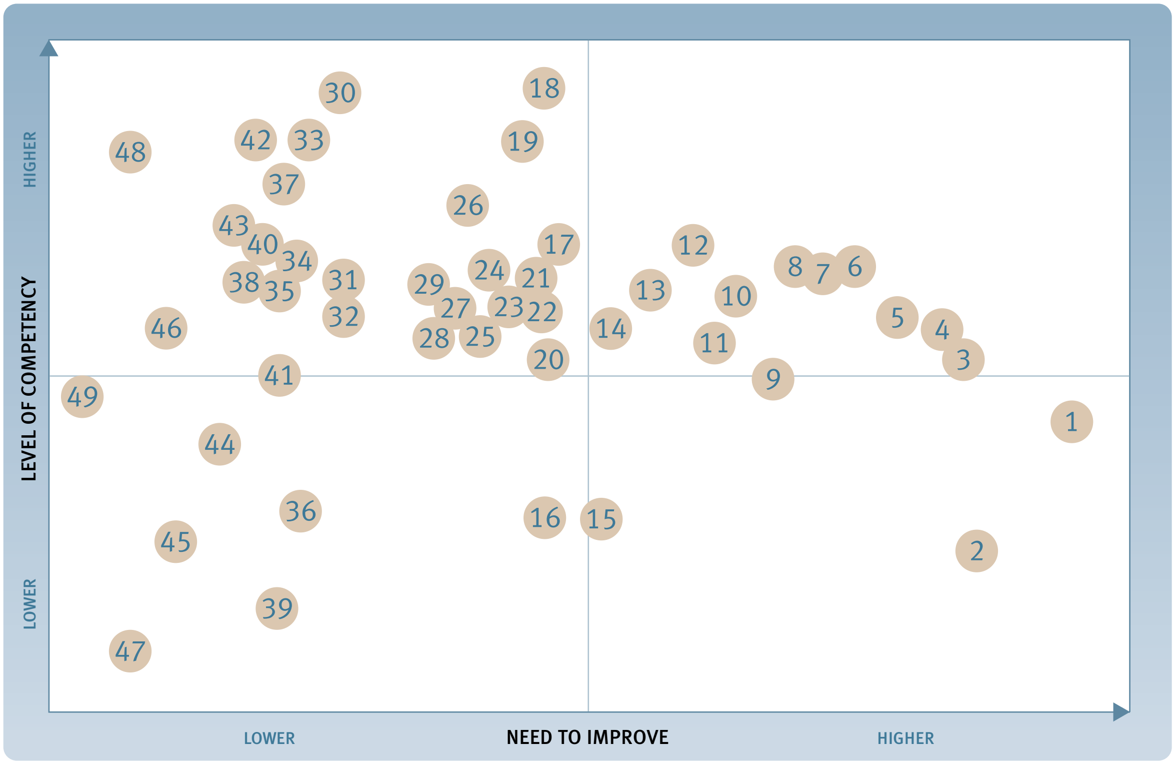
- Collaborate with functional and operational colleagues to produce and maintain current, practical and risk-savvy policies for social media and mobile device/application usage.
- Evaluate the degree to which fraud detection and fraud prevention activities are sufficiently proactive, as well as effective in the face of new social, mobile and cloud-computing tools.
- Ensure sufficient attention is devoted throughout the organization to modifying, as needed, a wide range of business processes and practices to align with guidance in the updated COSO Internal Control Framework.

Second, there is new and emerging technology, along with the risk implications that remain unknown as they unfold in real time. CAEs and internal audit professionals want to understand more clearly the risk and control environment related to mobile applications, cloud computing and social media applications as use of these tools in their organizations increases. This rapidly increasing adoption – and its attendant risks – helps explain why the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) Cybersecurity Framework also ranks as a top priority. Of note, the competency score for the NIST framework is relatively low, reflecting this as a new area for internal auditors and one with significant room for improvement.

The highly dynamic and flexible nature of social media and mobile applications as well as cloud computing offer valuable opportunities to increase organizational agility and responsiveness. These technologies pose new security, privacy, legal and reputation risks for internal audit to recognize, understand and monitor – at a time when IT security lapses are occurring more and more frequently. Applying a rigorous and regimented process for identifying and monitoring social media – and mobile-related risks, in particular – represents a major challenge for the internal audit function. Addressing this challenge effectively requires collaboration with functional and business partners throughout the organization to ensure that appropriate usage policies are developed, constantly updated, understood and adhered to, and monitored vigilantly.

[5] *The Bulletin*, "The Updated COSO Internal Control Framework: Frequently Asked Questions," Volume 5, Issue 3, Protiviti, 2013: www.protiviti.com/en-US/Pages/The-Bulletin.aspx.

Figure 1: General Technical Knowledge – Perceptual Map



Number	General Technical Knowledge	Number	General Technical Knowledge
1	Mobile applications	15	ISO 31000 (risk management)
2	NIST Cybersecurity Framework	16	ISO 27000 (information security)
3	Social media applications	17	IT governance
4	Cloud computing	18	Fraud risk management
5	GTAG 16 – Data Analysis Technologies	19	2013 COSO Internal Control Framework
6	Recently enacted IIA Standards – Audit Opinions and Conclusions (Standards 2010.A2 and 2410.A1)	20	GTAG 14 – Auditing User-developed Applications
7	Recently enacted IIA Standard – Overall Opinions (Standard 2450)	21	GTAG 3 – Continuous Auditing
8	Recently enacted IIA Standard – Functional Reporting Interpretation (Standard 1110)	22	GTAG 5 – Managing and Auditing Privacy Risks
9	The Guide to the Assessment of IT Risk (GAIT)	23	COBIT
10	GTAG 13 – Fraud Prevention and Detection in an Automated World	24	GTAG 8 – Auditing Application Controls
11	GTAG 6 – Managing and Auditing IT Vulnerabilities	25	GTAG 17 – Auditing IT Governance
12	Practice Advisory 2120-3 – Internal Audit Coverage of Risks to Achieving Strategic Objectives	26	Practice Guide – Assessing the Adequacy of Risk Management
13	Practice Advisory 2320-4 – Continuous Assurance	27	GTAG 12 – Auditing IT Projects
14	GTAG 15 – Information Security Governance	28	GTAG 7 – IT Outsourcing

Number	General Technical Knowledge	Number	General Technical Knowledge
29	GTAG 4 – Management of IT Auditing	40	Practice Guide – Assisting Small Internal Audit Activities in Implementing the International Standards for the Professional Practice of Internal Auditing
30	COSO Enterprise Risk Management Framework	41	GTAG 2 – Change and Patch Management Controls
31	GTAG 10 – Business Continuity Management	42	Practice Guide – Auditing the Control Environment
32	GTAG 11 – Developing the IT Audit Plan	43	Reporting on Controls at a Service Organization – SSAE 16/AU 324 (replaces SAS 70)
33	Practice Guide – Measuring Internal Audit Effectiveness and Efficiency	44	International Financial Reporting Standards (IFRS)
34	GTAG 9 – Identity and Access Management	45	ISO 9000 (quality management and quality assurance)
35	Practice Advisory 2050-3 – Relying on the Work of Other Assurance Providers	46	Country-specific enterprise risk management framework
36	Six Sigma	47	ISO 14000 (environmental management)
37	GTAG 1 – Understanding IT Controls	48	Corporate social responsibility
38	Practice Advisory 2320-3 – Audit Sampling	49	Fair value accounting
39	Extensible Business Reporting Language (XBRL)		

Key Questions for Internal Audit to Consider

- Do you conduct ongoing assessments of potential risks related to the use of new and existing mobile and social media applications? Does your organization have practical, effective and current social media and mobile-device/applications policies in place?
- Have you and your staff reviewed the NIST Cybersecurity Framework?
- Do you play a central role in monitoring and evaluating compliance with these policies?
- As data becomes an increasingly valuable, voluminous and dispersed corporate asset, what steps are you taking to work with management to strengthen the internal controls and risk management processes surrounding critical information?
- Do you, and the company as a whole, understand the implications of the new COSO Internal Control Framework, and what steps are you taking to strengthen this understanding?
- Are your organization's efforts to adapt current internal audit, risk management, compliance and financial reporting practices to the principles within the new COSO framework sufficient?
- Are your organization's fraud prevention and detection capabilities keeping pace with the increasingly automated and data-driven nature of your business operations?
- Are risk management processes pertaining to your organization's data both effective and efficient – even as the volume of this data continues to increase exponentially?
- How can updated and/or new data analysis and continuous monitoring tools be used to fortify your fraud prevention and detection capabilities?

Overall Results, General Technical Knowledge – Three-Year Comparison

2014	2013	2012
Mobile applications	Social media applications	Social media applications
NIST Cybersecurity Framework	Recently enacted IIA Standard – Functional Reporting Interpretation (Standard 1110)	Cloud computing
	Recently enacted IIA Standards – Audit Opinions and Conclusions (Standards 2010.A2 and 2410.A1)	
Social media applications	GTAG 16 – Data Analysis Technologies	GTAG 13 – Fraud Prevention and Detection in an Automated World
	Recently enacted IIA Standard – Overall Opinions (Standard 2450)	
	Cloud computing	
Cloud computing	The Guide to the Assessment of IT Risk (GAIT)	Fraud risk management
	GTAG 13 – Fraud Prevention and Detection in an Automated World	
	ISO 27000 (information security)	
	COSO Internal Control Framework (DRAFT 2012 version)	
GTAG 16 – Data Analysis Technologies	Practice Guide – Assessing the Adequacy of Risk Management	GTAG 16 – Data Analysis Technologies
	GTAG 6 – Managing and Auditing IT Vulnerabilities	
	Fraud risk management	

Focus on Results by Company Size

Company Size Results, General Technical Knowledge		
Small ‹ US$1B	Medium US$1B-$9B	Large › US$10B
Mobile applications	Mobile applications	Cloud computing
NIST Cybersecurity Framework	NIST Cybersecurity Framework	Fraud risk management
		ISO 31000 (risk management)
		Social media applications
The Guide to the Assessment of IT Risk (GAIT)	Recently enacted IIA Standards – Audit Opinions and Conclusions (Standards 2010.A2 and 2410.A1)	Six Sigma
Social media applications	GTAG 16 – Data Analysis Technologies	Mobile applications
	Recently enacted IIA Standard – Overall Opinions (Standard 2450)	
Cloud computing	GTAG 13 – Fraud Prevention and Detection in an Automated World	2013 COSO Internal Control Framework
		Country-specific enterprise risk management framework
		Extensible Business Reporting Language (XBRL)
GTAG 6 – Managing and Auditing IT Vulnerabilities		
		Recently enacted IIA Standards – Audit Opinions and Conclusions (Standards 2010.A2 and 2410.A1)
	Social media applications	
		GTAG 16 – Data Analysis Technologies
GTAG 16 – Data Analysis Technologies		
		Practice Advisory 2120-3 – Internal Audit Coverage of Risks to Achieving Strategic Objectives
		Practice Advisory 2320-4 – Continuous Assurance

Focus on Chief Audit Executives

The responses from CAEs are consistent with the overall results: mobile applications, cloud computing and social media applications rank among their top priorities. In addition, similar to the overall response, CAE competency levels for the NIST Cybersecurity Framework are relatively low, highlighting this as an area with significant room for improvement.

CAE Results, General Technical Knowledge

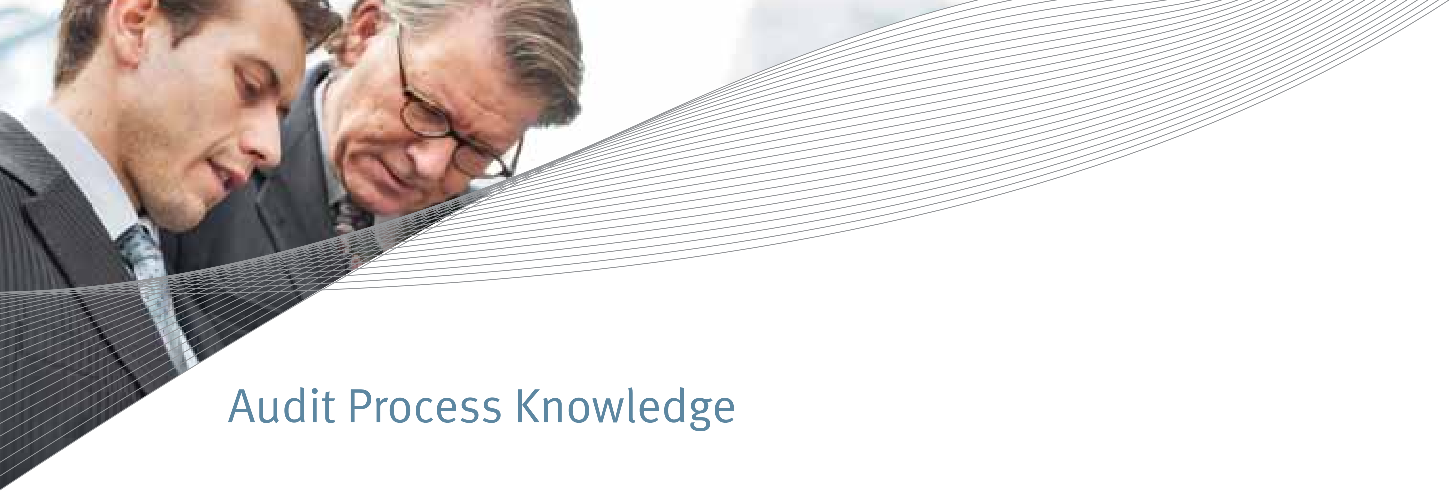
"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1	Mobile applications	2.7
2 (tie)	Cloud computing	2.8
	NIST Cybersecurity Framework	2.3
3	GTAG 16 – Data Analysis Technologies	3.0
4	Social media applications	2.8
5	GTAG 6 – Managing and Auditing IT Vulnerabilities	2.9

Key Questions for CAEs

- Are the CAE, CIO, and other C-suite and business-unit executives actively discussing their expectations for how current and emerging technology-related risks are managed and monitored?
- Are there similar discussions taking place regarding the nature of data risks and how those risks should be managed?
- Do C-level executives and board members maintain a clear understanding of the technology-related risks the organization confronts?
- Does the internal audit function conduct a specific IT audit risk assessment when formulating the overall audit plan?
- Are evaluations of social media and mobile application risk included in the audit plan?
- Does the internal audit function possess the expertise and staffing necessary to monitor and manage new and emerging technology risks effectively?
- Is the internal audit function keeping pace with new guidance and requirements from external standard-setters including The IIA, COSO and other organizations?

CAE Results, General Technical Knowledge – Three-Year Comparison

2014	2013	2012
Mobile applications	Social media applications	Social media applications
Cloud computing	Recently enacted IIA Standard – Functional Reporting Interpretation (Standard 1110)	Cloud computing
NIST Cybersecurity Framework	COSO Internal Control Framework (DRAFT 2012 version)	GTAG 13 – Fraud Prevention and Detection in an Automated World
GTAG 16 – Data Analysis Technologies		
Social media applications	Recently enacted IIA Standards – Audit Opinions and Conclusions (Standards 2010.A2 and 2410.A1)	GTAG 16 – Data Analysis Technologies
GTAG 6 – Managing and Auditing IT Vulnerabilities	Cloud computing	International Financial Reporting Standards (IFRS)
	ISO 27000 (information security)	



Audit Process Knowledge

Key Findings

- Internal auditors are intent on improving the way they leverage technology (e.g., continuous monitoring and auditing as well as advanced data analysis techniques) and the way they address technology-related risks proactively (e.g., auditing IT security and fraud monitoring).
- Leveraging computer-assisted auditing tools (CAATs) remains a top priority.
- There is a notable emphasis by CAEs on marketing internal audit internally.

Overall Results, Audit Process Knowledge

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1	Computer-assisted audit tools (CAATs)	3.0
2	Data analysis tools – data manipulation	3.1
3	Data analysis tools – statistical analysis	3.1
4	Auditing IT – new technologies	3.0
5	Data analysis tools – sampling	3.2

Commentary – Overall Findings

Respondents were asked to assess, on a scale of one to five, their competency in 35 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 20-21.) Figure 2 depicts a comparison of "Need to Improve" versus "Competency" ratings in an Audit Process Knowledge landscape.

Technology and technology-analyst firms delight in publishing research showing how quickly the amount of data in the world doubles (every 18 months, according to a recent count).[6] Given the double-edged nature of data, internal auditors can be forgiven for feeling as if the data in their organizations' enterprise systems doubles every 18 days. Data fuels CAATs, sampling and statistical

[6] Press, Gil. "A Very Short History of Big Data," Forbes.com, May 9, 2013: www.forbes.com/sites/gilpress/2013/05/09/a-very-short-history-of-big-data/2/.

analyses, as well as continuous auditing and monitoring capabilities – all of which are top priorities for internal auditors, and all of which represent ways of harnessing technology to expand internal audit's effectiveness and efficiency.

Data, of course, also represents an increasing source of fraud. As organizational dependence on data increases, fraudulent activity necessarily grows more technologically sophisticated and information-based. As our results suggest, internal auditors want to apply more sophisticated techniques and tools to both prevent and detect this type of fraud.

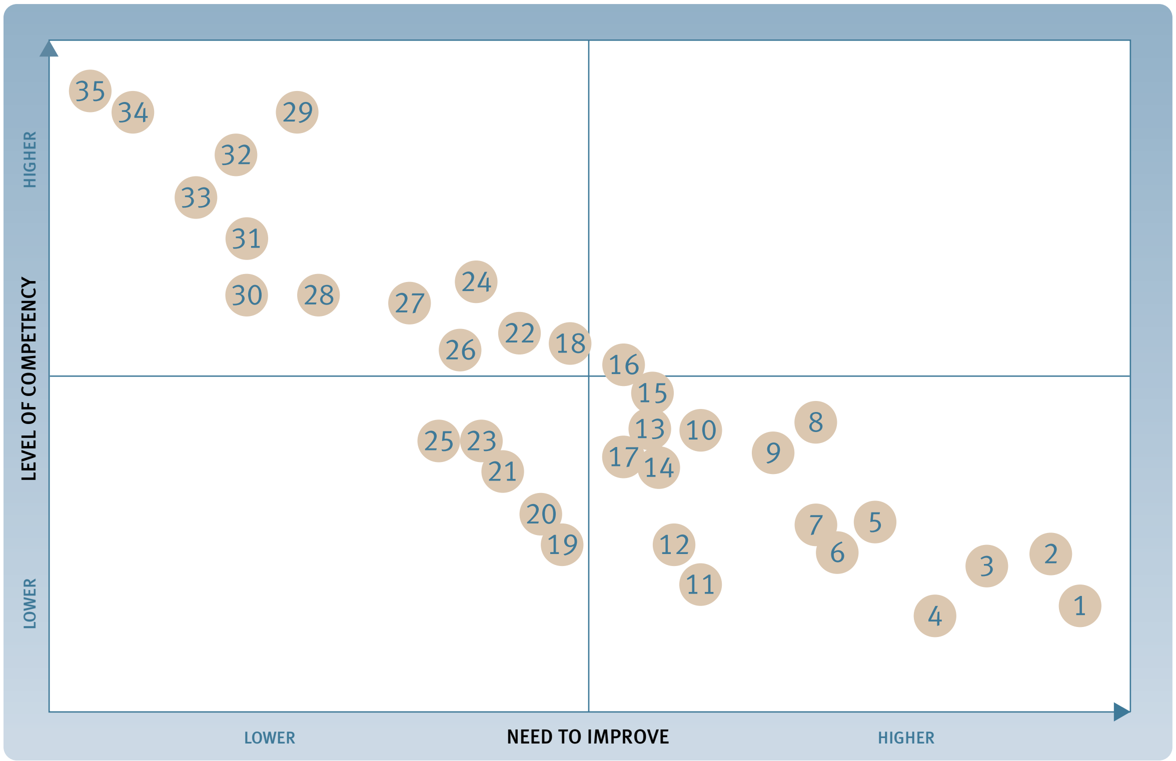
Internal Audit Action Items

- In straightforward, business-case terms, ensure the CEO, CFO and audit committee members are aware of the value CAATs deliver and the potential for additional investments in these tools and related technologies that support continuous monitoring and auditing as well as advanced data analysis techniques.
- Create and/or update a formal internal communications plan that conveys clearly the ways in which the internal audit function adds value to the organization and the specific services, expertise and types of collaboration it uses to deliver this value.
- Regularly assess the degree to which current staffing and talent levels enable the internal audit function to address new and emerging risks and opportunities related to new IT systems, applications and tools; data analysis approaches; and technology-and data-related fraud.

This simultaneous interaction of harnessing data's benefits while mitigating its weaknesses suggests that internal auditors are taking a more proactive approach to managing data-related risks. This is apparent in the growing demand for data governance, classification and retention expertise.

These priorities are also evident in another interesting survey finding: marketing internal audit internally. Our respondents, including CAEs, place a substantially higher emphasis on marketing internal audit internally compared to previous years of our study (it ranks overall as a top 10 priority this year and in the top five for CAEs). This suggests that internal audit wants to get the word out: *As the organization becomes more data-driven, we can help.*

Figure 2: Audit Process Knowledge – Perceptual Map



Number	Audit Process Knowledge	Number	Audit Process Knowledge
1	Computer-assisted audit tools (CAATs)	15	Fraud – fraud risk
2	Data analysis tools – data manipulation	16	Fraud – fraud risk assessment
3	Data analysis tools – statistical analysis	17	Fraud – management/prevention
4	Auditing IT – new technologies	18	Operational auditing – cost effectiveness/ cost reduction
5	Data analysis tools – sampling	19	Auditing IT – computer operations
6	Continuous auditing	20	Auditing IT – continuity
7	Continuous monitoring	21	Auditing IT – change control
8	Marketing internal audit internally	22	Assessing risk – emerging issues
9	Fraud – monitoring	23	Quality Assurance and Improvement Program (IIA Standard 1300) – Periodic Reviews (IIA Standard 1311)
10	Statistically based sampling	24	Self-assessment techniques
11	Auditing IT – program development	25	Quality Assurance and Improvement Program (IIA Standard 1300) – External Assessment (IIA Standard 1312)
12	Auditing IT – security	26	Operational auditing – effectiveness, efficiency and economy of operations approach
13	Fraud – auditing	27	Enterprisewide risk management
14	Fraud – fraud detection/investigation	28	Assessing risk – entity level

Number	Audit Process Knowledge	Number	Audit Process Knowledge
29	Report writing	33	Assessing risk – process, location, transaction level
30	Top-down, risk-based approach to assessing internal control over financial reporting	34	Audit planning – entity level
31	Operational auditing – risk-based approach	35	Audit planning – process, location, transaction level
32	Presenting to senior management		

Key Questions for Internal Audit to Consider

- To what degree do you understand the value that continuous auditing, continuous monitoring, and other data analytics tools and capabilities bring to the internal control environment (and to internal audit's advisory capabilities)? How can you further this understanding?
- What CAATs and data analytics tools do you currently use and what sorts of changes (removing outdated tools, upgrading effective applications, making new investments) would help today and in the years ahead?
- How can you collaborate more effectively with management and business process owners in continuous auditing and continuous monitoring efforts?
- How can your existing fraud prevention, detection, monitoring and investigation activities be improved or upgraded to better address data- and information-related fraud risks?

Overall Results, Audit Process Knowledge – Three-Year Comparison		
2014	2013	2012
CAATs	Data analysis tools – data manipulation	Continuous auditing
	Fraud – monitoring	
Data analysis tools – data manipulation	Auditing IT – new technologies	CAATs
	Fraud – fraud risk assessment	
Data analysis tools – statistical analysis	Data analysis tools – statistical analysis	Continuous monitoring
	Fraud – fraud detection/ investigation	
Auditing IT – new technologies	Fraud – management/prevention	Data analysis tools – data manipulation
	CAATs	
Data analysis tools – sampling	Data analysis tools – sampling	Data analysis tools – statistical analysis

Focus on Results by Company Size

Company Size Results, Audit Process Knowledge		
Small ‹ US$1B	Medium US$1B-9B	Large › US$10B
Data analysis tools – data manipulation	CAATs	Data analysis tools – data manipulation
		Fraud – fraud risk
CAATs	Auditing IT – new technologies	Assessing risk – entity level
		Assessing risk – process, location, transaction level
		Enterprisewide risk management
		CAATs
		Continuous auditing
		Data analysis tools – sampling
		Fraud – auditing
		Fraud – fraud detection/investigation
		Fraud – fraud risk assessment
		Fraud – management/prevention
Data analysis tools – statistical analysis	Data analysis tools – statistical analysis	Continuous monitoring
		Data analysis tools – statistical analysis
		Statistically based sampling
		Fraud – monitoring
Auditing IT – new technologies	Data analysis tools – data manipulation	Auditing IT – security
		Operational auditing – effectiveness, efficiency and economy of operations approach
		Operational auditing – risk-based approach
		Presenting to senior management
		Self-assessment techniques
		Top-down, risk-based approach to assessing internal control over financial reporting
Data analysis tools – sampling	Continuous monitoring	Auditing IT – program development
		Marketing internal audit internally
		Operational auditing – cost effectiveness/cost reduction
		Report writing

Focus on Chief Audit Executives

Feedback from CAEs in the survey mirrors the overall response. Clearly, data analysis tools, continuous auditing and monitoring, and fraud prevention are top priorities for internal audit functions. It is also noteworthy that our CAE respondents are placing greater value on marketing internal audit internally.

CAE Results, Audit Process Knowledge

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1	Auditing IT – new technologies	3.1
2	Computer-assisted audit tools (CAATs)	3.2
3	Data analysis tools – data manipulation	3.3
4	Marketing internal audit internally	3.5
5	Data analysis tools – statistical analysis	3.2

Key Questions for CAEs

- Is your staff communicating a consistent message to the business regarding the internal audit function's role, value and expertise?
- Are you monitoring the degree to which the internal audit function's fraud risk management capability is current, robust and proactive ("on its toes" as opposed to "on its heels") given the new technology that regularly enters the organization?
- Is your vision for the introduction or addition of CAATs and related continuous monitoring and auditing capabilities documented in a formal strategy and business case?
- Do you ensure that executive management, the board and leaders throughout the business understand the value of CAATs and data analysis tools that the internal audit function uses (or wants to use) to strengthen its contributions to the business?
- How do you ensure that the level of training your internal auditors receive is sufficient in the face of a constantly changing enterprise technology environment?
- Do you maintain access to qualified resources from other departments (and, in some cases, external service providers) to assist with internal audit's work on complex and dynamic technology-related areas?
- What are you doing to communicate – and market – internal audit's value, expertise and specific offerings to the rest of the organization? And are there opportunities to make this message clearer, more accurate and/or more effective?

CAE Results, Audit Process Knowledge – Three-Year Comparison

2014	2013	2012
Auditing IT – new technologies	Data analysis tools – data manipulation	CAATs
CAATs	Auditing IT – new technologies	Continuous auditing
Data analysis tools – data manipulation	Data analysis tools – sampling	Data analysis tools – data manipulation
Marketing internal audit internally	CAATs	Continuous monitoring
Data analysis tools – statistical analysis	Data analysis tools – statistical analysis	Data analysis tools – statistical analysis
	Fraud – fraud risk assessment	

Personal Skills and Capabilities

Key Findings

- Presenting (public speaking), negotiation, persuasion, and using/mastering new technology and applications are among the top areas and "soft skills" in need of improvement.
- These priorities point to the rising importance that collaboration – inside the function, throughout the enterprise and even beyond the organization – plays in determining internal audit's ultimate success.

Overall Results, Personal Skills and Capabilities

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1	Presenting (public speaking)	3.4
2	Negotiation	3.4
3 (tie)	Persuasion	3.5
	Using/mastering new technology and applications	3.5
4 (tie)	Dealing with confrontation	3.5
	Time management	3.6
5 (tie)	Developing other board committee relationships	3.4
	Developing outside contacts/networking	3.6

Commentary – Overall Findings

Respondents were asked to assess, on a scale of one to five, their competency in 19 areas of personal skills and capabilities, with one being the lowest level of competency and five being the highest. For each area, respondents 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 27.) Figure 3 depicts a comparison of "Need to Improve" versus "Competency" ratings in a Personal Skills and Capabilities landscape.

As a top internal audit executive asserted in a 2013 report from The IIA and Robert Half on key internal auditor attributes, "Soft skills are the new hard skills."[7] This observation serves as the de facto theme of that report, and it sheds light on the growing value of the personal skills that our respondents report they are deploying to take the internal audit function's collaborative efforts to new heights.

Internal Audit Action Items

- Define at what point internal audit expertise and insights are sought by business colleagues as they make important decisions, and identify ways to help ensure this expertise can be provided as early as possible in the decision-making process.
- Consider the need for a functional branding/communications effort designed to ensure that all areas of the business understand internal audit's role and expertise and the value of collaborating with internal audit on an ongoing basis.
- Develop formal rotational programs designed to expose internal auditors to as many different parts of the business as possible.
- Take an expansive view of potential training opportunities that help groom internal auditors for leadership roles while simultaneously strengthening internal audit's collaboration with other departments.

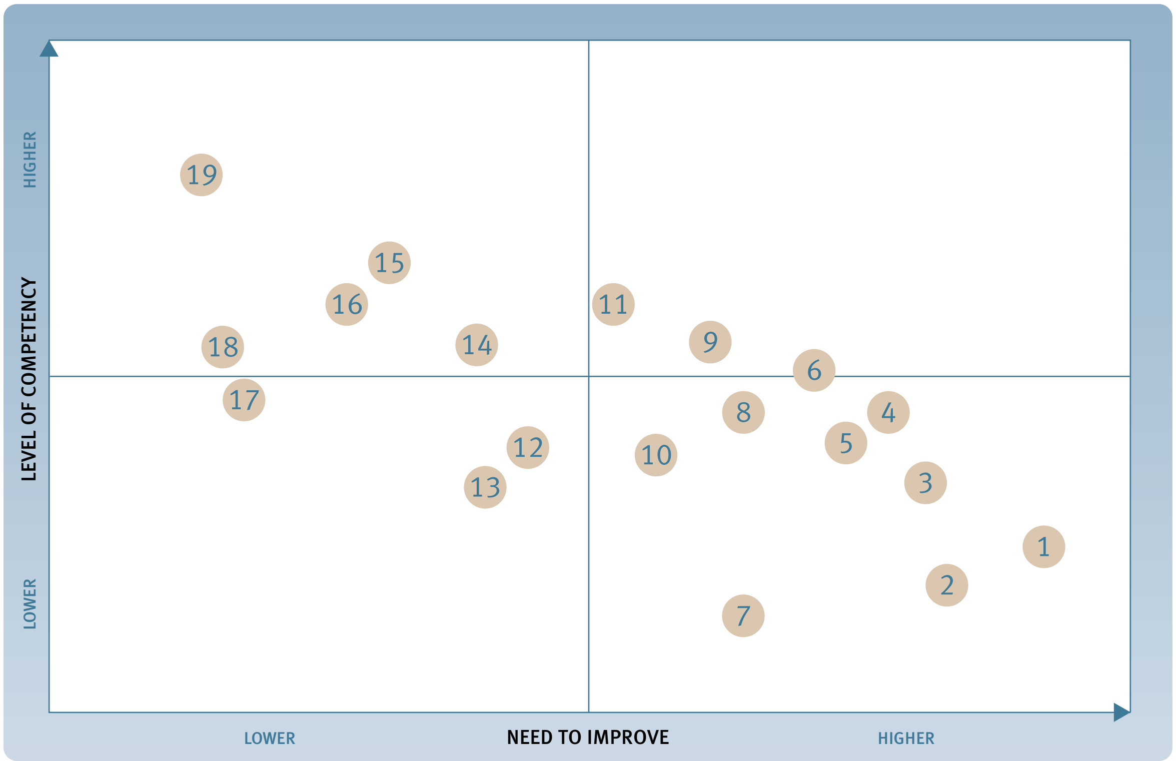
Our findings indicate that internal auditors are strengthening interpersonal skills, such as public speaking, dealing with confrontation, persuasion and negotiation, in tandem with technical skills such as mastering new technology, to help strengthen relationships inside and outside their functions and their organizations.

For many years in our survey, internal auditors have expressed a goal to sharpen personal skills. While this goal remains as important as ever, the ways that internal auditors treat and cultivate their collaborative capabilities have reached a new, more strategic level.

This final point is noteworthy. Deeper, more meaningful collaboration can help internal auditors address nearly every item on their lengthy priority lists. By developing and sustaining deep and constructive partnerships throughout the business, internal auditors can ensure that their expertise is applied in advance of strategic decisions – that is to say, with sufficient proactivity.

[7] Chambers, Richard F., McDonald, Paul, "Succeeding as a 21st Century Internal Auditor: 7 Attributes of Highly Effective Internal Auditors," http://rhmr.mediaroom.com/sevenattributes. (Note: Protiviti is a subsidiary of Robert Half.)

Figure 3: Personal Skills and Capabilities – Perceptual Map



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

Key Questions for Internal Audit to Consider

- When is our expertise sought by business colleagues – prior to an important business decision being made, or after the fact?
- To what degree do we recognize the role that technology (e.g., social media applications, mobile devices and collaborative software) can play in cultivating more collaboration between our internal auditors and the rest of the organization, including the board?
- To what degree do our internal audit leaders and executives express a desire to strengthen our function's collaborative capability and support this objective with training, exercises and related practices?
- Have opportunities for rotational work, stretch assignments, training classes and leadership development been formalized into personal development plans?
- To what degree are leading collaboration practices being identified and shared within the internal audit function?

Overall Results, Personal Skills and Capabilities – Three-Year Comparison		
2014	2013	2012
Presenting (public speaking)	Dealing with confrontation	Developing outside contacts/ networking
Negotiation	Negotiation	Negotiation
	Persuasion	Persuasion
Persuasion	High-pressure meetings	Dealing with confrontation
Using/mastering new technology and applications	Presenting (public speaking)	
Dealing with confrontation	Strategic thinking	Presenting (public speaking)
Time management		
Developing other board committee relationships	Developing other board committee relationships	High-pressure meetings
	Using/mastering new technology and applications	
Developing outside contacts/ networking		
	Leadership (within the IA profession)	
	Time management	

Focus on Results by Company Size

<table>
<tr><th colspan="3">Company Size Results, Personal Skills and Capabilities</th></tr>
<tr><th>Small ‹ US$1B</th><th>Medium US$1B-9B</th><th>Large › US$10B</th></tr>
<tr><td>Presenting (public speaking)</td><td>Using/mastering new technology and applications</td><td>Time management</td></tr>
<tr><td rowspan="4">Persuasion</td><td rowspan="2">Dealing with confrontation</td><td>Negotiation</td></tr>
<tr><td rowspan="2">Presenting (public speaking)</td></tr>
<tr><td rowspan="2">Presenting (public speaking)</td></tr>
<tr><td>Strategic thinking</td></tr>
<tr><td>Developing outside contacts/ networking</td><td rowspan="3">Negotiation</td><td rowspan="3">Persuasion</td></tr>
<tr><td>Developing other board committee relationships</td></tr>
<tr><td>Negotiation</td></tr>
<tr><td>Dealing with confrontation</td><td rowspan="2">Developing other board committee relationships</td><td>Coaching/mentoring</td></tr>
<tr><td>Leadership (within your organization)</td><td>Using/mastering new technology and applications</td></tr>
<tr><td>High-pressure meetings</td><td rowspan="3">High-pressure meetings</td><td rowspan="2">Developing outside contacts/ networking</td></tr>
<tr><td rowspan="4">Time management</td></tr>
<tr><td rowspan="2">Presenting (small groups)</td></tr>
<tr><td rowspan="3">Persuasion</td></tr>
<tr><td rowspan="2">Leadership (within the internal audit profession)</td></tr>
<tr><td>Using/mastering new technology and applications</td></tr>
</table>

Focus on Chief Audit Executives

The findings from CAEs are very similar to the overall response. It is noteworthy that using/mastering new technology and applications figures as a top priority for CAEs as well as all respondents. All internal audit professionals, regardless of their title or years of experience, see value in strengthening their use of technology to enhance their collaborations with business colleagues.

CAE Results, Personal Skills and Capabilities

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1	Presenting (public speaking)	3.6
2	Developing other board committee relationships	3.7
3	Using/mastering new technology and applications	3.7
4 (tie)	Dealing with confrontation	3.8
	Persuasion	3.7
5 (tie)	Developing outside contacts/networking	3.8
	Negotiation	3.7

Key Questions for CAEs

- Do our internal auditors possess the interpersonal skills necessary to foster deep; ongoing; at times, difficult; and ultimately, valuable working relationships throughout the entire organization?
- In terms of personal skills development, do you lead by example?
- How innovative are the approaches you use to develop the personal skills of your staff? Are there opportunities to introduce new, potentially more effective practices?
- What opportunities exist to expose your staff to external expertise that ultimately will strengthen their performance and relationships inside the organization?

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

2014	2013	2012
Presenting (public speaking)	Dealing with confrontation	Presenting (public speaking)
Developing other board committee relationships	Developing other board committee relationships	Developing other board committee relationships
Using/mastering new technology and applications		Developing outside contacts/ networking
Dealing with confrontation	Developing outside contacts/ networking	Persuasion
Persuasion	Negotiation	Using/mastering new technology and applications
Developing outside contacts/ networking	Using/mastering new technology and applications	
Negotiation	Time management	Negotiation
		Dealing with confrontation
	Persuasion	Time management
	Strategic thinking	

Methodology and Demographics

More than 600 respondents submitted completed surveys for Protiviti's Internal Audit Capabilities and Needs Survey, which was conducted from September through November 2013.

The survey consisted of a series of questions grouped into four divisions: Social Media Risk and the Audit Process, 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 nearly 200 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	20%
Director of Auditing	11%
IT Audit Director	1%
Audit Manager	26%
IT Audit Manager	4%
Audit Staff	22%
IT Audit Staff	6%
Corporate Management	2%
Other	8%

Industry

Financial Services (U.S.)	14%
Healthcare (U.S.) – Provider	14%
Government/Education/Not-for-profit	11%
Manufacturing	11%
Insurance (excluding healthcare payer)	5%
Retail	5%
CPA/Public Accounting/Consulting Firm	4%
Energy	4%
Financial Services (Non-U.S.)	4%
Technology	3%
Healthcare (U.S.) – Payer	2%
Hospitality	2%
Services	2%

Industry *(continued)*

Telecommunications	2%
Utilities	2%
Distribution	1%
Healthcare (Non-U.S.)	1%
Life Sciences/Bio-tech	1%
Real Estate	1%
Other	11%

Certification

Certified Public Accountant (CPA)/Chartered Accountant (CA)	43%
Certified Internal Auditor (CIA)	39%
Certified Information Systems Auditor (CISA)	20%
Certified Fraud Examiner (CFE)	11%
Certified Information Technology Professional (CITP)	6%
Certified Financial Services Auditor (CFSA)	3%
Certified Government Auditing Professional (CGAP)	1%

Size of Organization (by Gross Annual Revenue)

$20 billion or greater	10%
$10 billion - $19.99 billion	9%
$5 billion - $9.99 billion	12%
$1 billion - $4.99 billion	25%
$500 million - $999.99 million	14%
$100 million - $499.99 million	16%
Less than $100 million	14%

Type of Organization

Public	40%
Private	32%
Not-for-profit	17%
Government	10%
Other	1%

Organization Headquarters

North America	79%
Asia Pacific	7%
Europe	5%
Middle East	3%
Africa	2%
India	2%
Latin America	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, and has served more than 35 percent of FORTUNE 1000® and FORTUNE Global 500® companies. Protiviti and its independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. The firm also works 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 (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Internal Audit and Financial Advisory

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 Advisory solutions, please contact:

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

Protiviti Internal Audit and Financial Advisory 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

Raul Silva
+55.11.2198.4200
raul.silva@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@protivitiglobal.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

Sidney Lim
+65.6220.6066
sidney.lim@protiviti.com

SOUTH KOREA

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

UNITED KINGDOM

Lindsay Dart
+44.207.389.0448
lindsay.dart@protiviti.co.uk

UNITED STATES

Brian Christensen
+1.602.273.8020
brian.christensen@protiviti.com

THE AMERICAS

UNITED STATES

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

ARGENTINA*

Buenos Aires

BRAZIL*

Rio de Janeiro
São Paulo

CANADA

Kitchener-Waterloo
Toronto

CHILE*

Santiago

MEXICO*

Mexico City
Monterrey

PERU*

Lima

VENEZUELA*

Caracas

EUROPE/MIDDLE EAST/AFRICA

FRANCE

Paris

GERMANY

Frankfurt
Munich

ITALY

Milan
Rome
Turin

THE NETHERLANDS

Amsterdam

UNITED KINGDOM

London

BAHRAIN*

Manama

KUWAIT*

Kuwait City

OMAN*

Muscat

QATAR*

Doha

UNITED ARAB EMIRATES*

Abu Dhabi
Dubai

SOUTH AFRICA*

Johannesburg

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

* Protiviti Member Firm
** Protiviti Alliance Member

protiviti®
Risk & Business Consulting.
Internal Audit.

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.