Navigating Technology's Top 10 Risks

TECHNOLOGY

Core Report

Internal Audit's Role

Philip E. Flora
CIA, CISA, CFE, CCSA

Sajay Rai
CPA, CISSP, CISM

The IIA Research Foundation

CBOK
The Global Internal Audit
Common Body of Knowledge

About CBOK

SURVEY FACTS

Respondents	14,518*
Countries	166
Languages	23

EMPLOYEE LEVELS

Chief audit executive (CAE)	26%
Director	13%
Manager	17%
Staff	44%

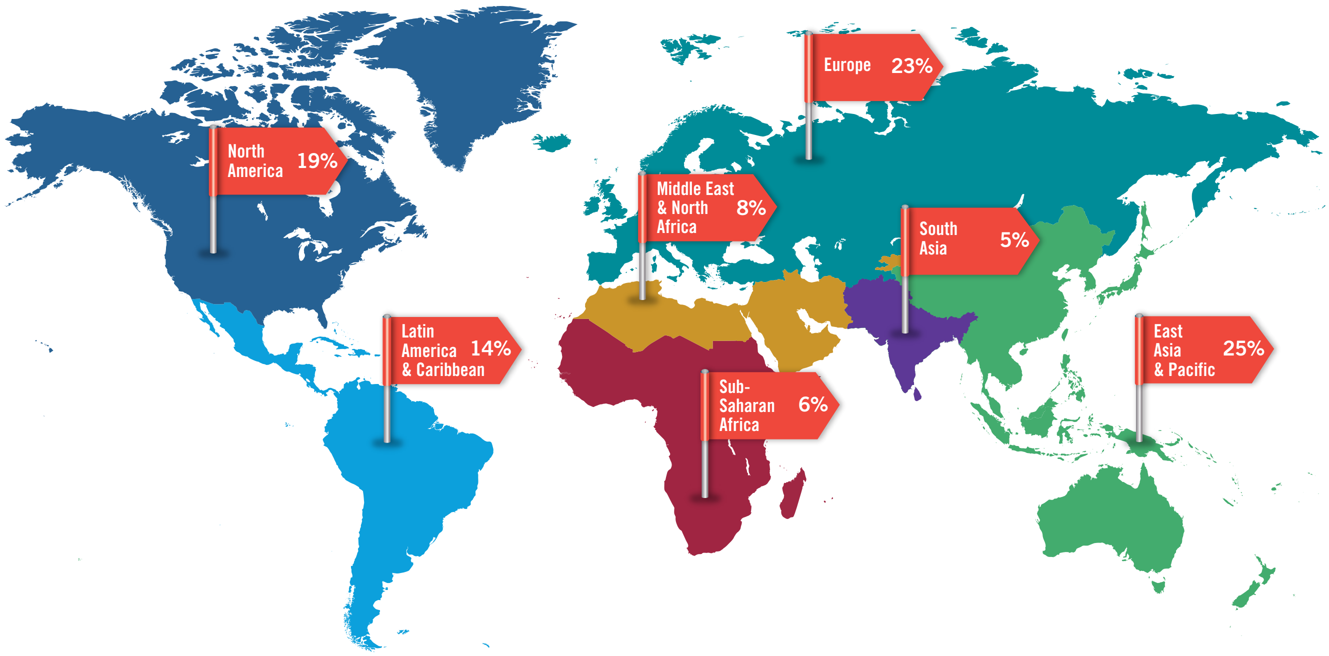
*Response rates vary per question.

The Global Internal Audit Common Body of Knowledge (CBOK) is the world's largest ongoing study of the internal audit profession, including studies of internal audit practitioners and their stakeholders. One of the key components of CBOK 2015 is the global practitioner survey, which provides a comprehensive look at the activities and characteristics of internal auditors worldwide. This project builds on two previous global surveys of internal audit practitioners conducted by The IIA Research Foundation in 2006 (9,366 responses) and 2010 (13,582 responses).

Reports will be released on a monthly basis through July 2016 and can be downloaded free of charge thanks to the generous contributions and support from individuals, professional organizations, IIA chapters, and IIA institutes. More than 25 reports are planned in three formats: 1) core reports, which discuss broad topics, 2) closer looks, which dive deeper into key issues, and 3) fast facts, which focus on a specific region or idea. These reports will explore different aspects of eight knowledge tracks, including technology, risk, talent, and others.

Visit the CBOK Resource Exchange at www.theiia.org/goto/CBOK to download the latest reports as they become available.

CBOK 2015 Practitioner Survey: Participation from Global Regions



Note: Global regions are based on World Bank categories. For Europe, fewer than 1% of respondents were from Central Asia. Survey responses were collected from February 2, 2015, to April 1, 2015. The online survey link was distributed via institute email lists, IIA websites, newsletters, and social media. Partially completed surveys were included in analysis as long as the demographic questions were fully completed. In CBOK 2015 reports, specific questions are referenced as Q1, Q2, and so on. A complete list of survey questions can be downloaded from the CBOK Resource Exchange.

CBOK Knowledge Tracks

Future

Global Perspective

Governance

Management

Risk

Standards & Certifications

Talent

Technology

Contents

Executive Summary 4

1 Cybersecurity 5

2 Information Security 7

3 IT Systems Development Projects 9

4 IT Governance 12

5 Outsourced IT Services 15

6 Social Media Use 17

7 Mobile Computing 19

8 IT Skills Among Internal Auditors 21

9 Emerging Technologies 23

10 Board and Audit Committee Technology Awareness 25

Conclusion 26

Executive Summary

Are the primary and emerging technology risks in your organization being identified and managed appropriately? This is one of the key questions that audit committees and boards of organizations everywhere are asking. This report provides internal auditors, board members, and audit committees with key information to help navigate the most important technology risks today.

You will learn:

- The top 10 technology risks
- Key questions for internal auditors to ask about these risks
- Key activities for addressing technology risks

The top 10 risks were identified using interviews with chief audit executives (CAEs) and information technology (IT) specialists from Africa, Latin America, the Middle East, Europe, Canada, and the United States. In addition, perspectives about technology risks are reported from the CBOK 2015 Global Internal Audit Practitioner Survey, the largest survey of internal auditors in the world. The order of the risks may differ in priority depending on the market in which you operate.

This report not only guides readers through the maze of complex current and emerging technology issues, it also addresses the organizational side of risks caused by low levels of IT skills within the internal audit department and the lack of awareness among the board of directors.

1 Cybersecurity

> *"Regarding cybersecurity, most leaders don't understand how much risk they are assuming."*
>
> —Scott Klososky, Partner in Future Point of View, LLC, USA

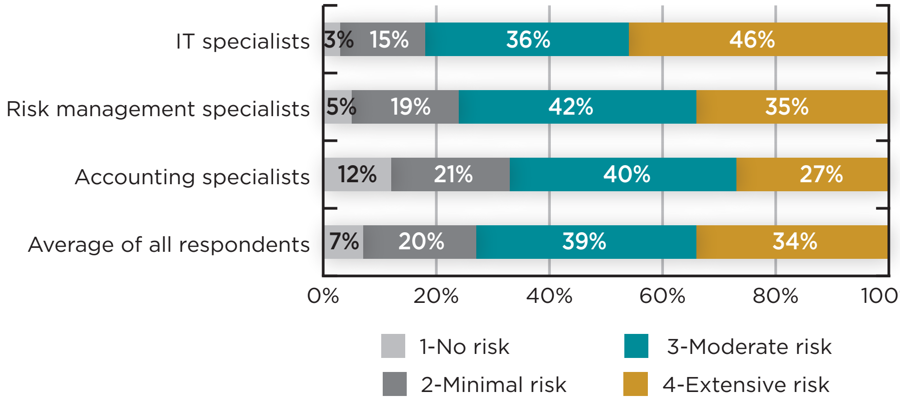
Cybersecurity is probably the most discussed IT topic among executives, internal auditors, audit committees, and the board of directors. Therefore, it is #1 on our list of technology's top 10 risks.

One of the biggest cybersecurity risks facing organizations is the possibility of external perpetrators stealing sensitive or confidential data. Most organizations recognize the damage such data breaches can cause to their brands and reputations. **Exhibit 1** confirms these sentiments, as more than 70% of survey respondents consider the risk of a data breach as extensive or moderate. It is also worth noting that the IT specialists consider this risk to be even higher (82%). This may be explained by the fact that IT specialists understand the technology better and know the gaps that can be exploited.

Internal Audit's Role

Internal auditors can play an integral role in the organization to ensure that cybersecurity risks are addressed appropriately. Depending on the size of the organization, the role they play may vary in terms of the activities they perform and the questions they may ask. Within small organizations (with fewer than 1,500 employees), 5 out of 10 internal audit departments perform minimal or no cybersecurity-related audit activity; whereas the internal audit department performs extensive audit activity related to cybersecurity within 4 out 10 of large organizations. (Q92, *n* = 9,929)

Exhibit 1 **Risk Levels for Data Breaches That Can Damage the Brand**



Note: Q93: In your opinion, what is the level of inherent risk at your organization for the following emerging information technology (IT) areas? Those who answered "not applicable/ I don't know" were excluded from the calculations. Due to rounding, some totals may not equal 100%. *n* = 1,038 for IT; *n* = 1,139 for risk management; *n* = 1,678 for accounting; *n* = 9,426 for all respondents.

> *Auditors should ensure that their company has a process for learning from their own experiences and those of other organizations. Collaboration is occurring, for example through the Financial Services—Information Sharing and Analysis Center, a global organization used extensively in the financial institution industry for sharing ideas to combat cybersecurity and related threats.*
>
> —James Alexander,
> CIA, CFE, CISA,
> Chief Risk Officer,
> Unitus Community
> Credit Union,
> Portland, Oregon

KEY QUESTIONS FOR INTERNAL AUDIT TO ASK

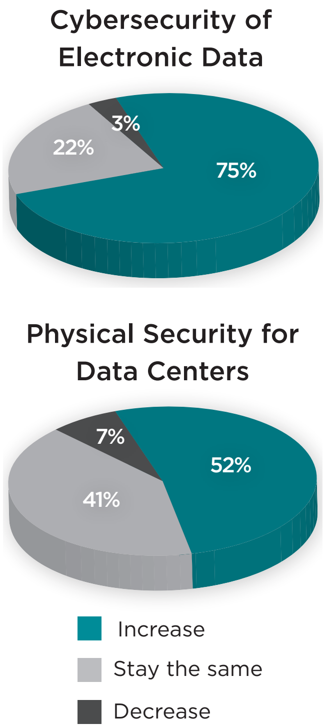
1. Is the organization able to monitor suspicious network intrusion?
2. Is the organization able to identify whether an attack is occurring?
3. Can the organization isolate the attack and restrict potential damage?
4. Is the organization able to know whether confidential data is leaving the organization?
5. If an incident does occur, is a written crisis management plan in place that has been tested and is in line with organizational risk?
6. If an incident does occur, does the organization have access to forensic skills to assist with the incident?
7. Is the incident team in place and do they know their roles and responsibilities?

KEY ACTIVITIES FOR INTERNAL AUDIT TO PERFORM

1. Conduct an annual independent vulnerability scan and a penetration test of the external facing network.
2. Verify that simulation exercises are performed in relation to the organization's crisis management plan to prepare the incident team in case of an actual incident.
3. Conduct an audit of network architecture to determine compliance with network policy and procedures.
4. Conduct an audit of a recent incident and determine whether the policies, procedures, and tools were applied as planned and whether the forensic experts were deployed during the incident.

2 Information Security

Exhibit 2 Audit Coverage



Cybersecurity of Electronic Data

Physical Security for Data Centers

Note: Q94: In the next two to three years, do you think the internal audit activity related to these technology areas will increase, decrease, or stay the same? *n* = 11,163.

Although cybersecurity receives a lot of media attention, information security is just as critical and comes in at #2 on our list of technology's top 10 risks. Information security refers to protecting the confidentiality, integrity, and availability of information that is critical to the organization.

In the past, most organizations focused on protecting the network perimeter and spent a considerable portion of their security budget on perimeter defense, investing in network perimeter appliances such as firewalls, intrusion detection, intrusion prevention, content filtering, and network monitoring. However, with all the current news about large-scale data breaches, it is obvious that focusing only on the network perimeter is not the right strategy. It is a foregone conclusion that if external perpetrators want to penetrate an organization's network, they will find a way to do so. The focus now is on a layered defense of critical information, rather than a single layer of protection against the network perimeter.

A good information security program in an organization usually has an executive or high-level manager, such as a chief information security officer (CISO), who is responsible for the program. At a minimum, an information security program encompasses:

- Robust risk assessment process
- Effective governance and compliance procedures
- Documented and communicated information security policies and standards
- Effective security awareness training program
- Efficient access control procedures
- Tested disaster recovery, business continuity, and incident response programs
- Operational asset management, network management, patch management, and change management processes
- Tight physical security

Internal Audit's Role

Internal audit has a major role to play in ensuring that an organization's information security program is effective and efficient. Internal audit plans should continue to include both physical security and cybersecurity activities, although cybersecurity activities will probably increase more rapidly. As shown in **exhibit 2**, more than 75% of respondents plan to increase cybersecurity activity, compared to 52% for physical security.

> *“Organizational information security and risk management can’t enable containment of key risks without employees being informed about managing the risks and being empowered to take action.”*
>
> —Grace Lwanga, Technical Director, IT Audit, World Vision International

KEY QUESTIONS FOR INTERNAL AUDIT TO ASK

1. When was the last time the information security policy was reviewed and updated?
2. What is the success rate of the information security awareness training program? Is the training mandatory? What are the repercussions for those who have not yet completed the training?
3. When was the last time a risk assessment was performed? Is risk assessment performed for all new third-party vendors?
4. Does the organization simulate incidents to determine their readiness?
5. When was the last disaster recovery test performed? Was it successful? What issues were encountered?
6. What compliance requirements does the organization have? Health Insurance Portability and Accountability Act of 1996 (HIPAA)? Sarbanes-Oxley Act of 2002 (SOX)? PCI Security Standards Council?
7. Can an external perpetrator penetrate the physical parameter using social engineering? (An example of this kind of breach would be a perpetrator starting a casual conversation with an employee outside the building and following the employee into the building when he or she scans the badge to enter.)
8. Does the organization log and monitor the activities of privileged users (those who have administrative authority to manage the IT environment)?

KEY ACTIVITIES FOR INTERNAL AUDIT TO PERFORM

1. Perform a vulnerability scan for the internal network.
2. Review the access control review process. Are the owners actually reviewing the access list or is the review a compliance exercise, where the owners just say “approved” without actually looking at the list?
3. Use third parties to conduct a simulated attack and audit the results. For example, conduct a phishing email exercise to determine the effectiveness of the awareness training program (medium and large organizations).
4. Audit the backup of critical information and verify that the backups are performed routinely.
5. Audit the activity of privileged users and verify that only authorized users have the privileged capabilities. Also, verify that privileged users are logged and monitored.
6. Perform an audit of those third parties who have access to the organization’s critical assets, or review the third parties’ Statement on Standards for Attestation Engagements (SSAE) No. 16 reports (large organizations).

3 IT Systems Development Projects

> “Organizations need to learn quickly from any systems development mistakes so they can become more successful at developing and implementing core applications for the enterprise.”
>
> —Edward Carr,
> IT Audit Chief,
> Office of Internal Audit,
> State of Ohio

A large portion of IT’s budget is spent on system development projects and, therefore, the topic comes in at #3 on our list of top 10 technology risks. To remain viable, almost every organization will need to develop or update their technology systems. Unfortunately, the chances of success are low. According to the CHAOS Report published by The Standish Group, IT systems development projects performed as follows over an extended time:

- Overall success rate: 16.2%
- Challenged projects: 52.7%
- Impaired (canceled): 31.1%

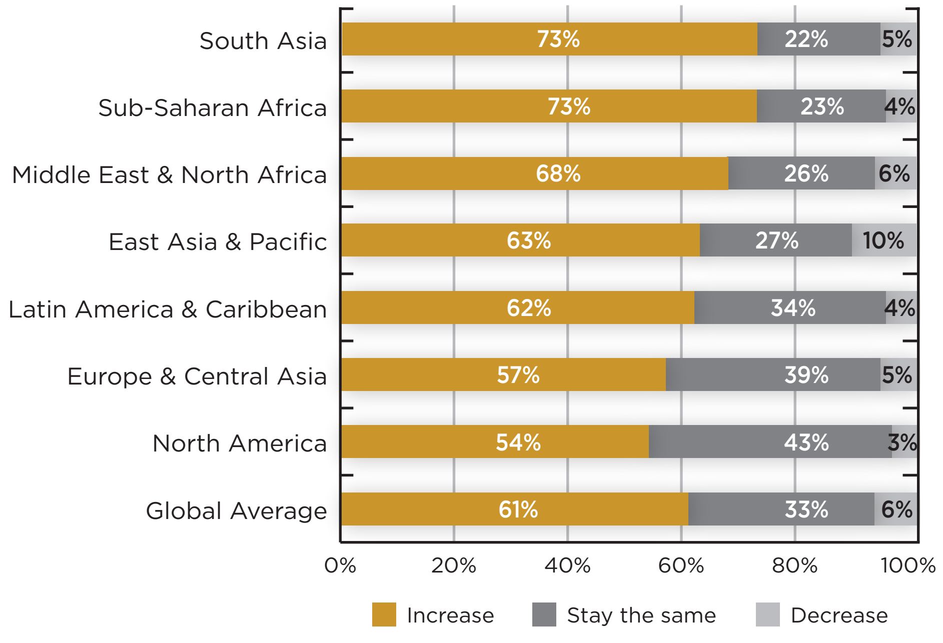
One study estimated that software failure costs companies $50 to $80 billion annually.*

The majority of survey respondents recognize the importance of continuing or increasing audits and assurance of major technology projects (see **exhibit 3**). About 6 out of 10 of all respondents expect to increase these audits.

Objectives for core system projects must be monitored throughout development and after implementation.

* *CIO Journal*, January 2014, as quoted in *The Wall Street Journal*.

Exhibit 3 Assurance for Major IT Projects in the Future



Note: Q94: In the next two to three years, do you think the internal audit activity related to these technology areas will increase, decrease, or stay the same? Topic: Audits/project management assurance of major projects. *n* = 11,019.

EXPECTATIONS GAPS

Here are some common reasons why IT systems development projects fail to meet management expectations:

- Forced implementation dates (the date of project completion is set before the project team performs appropriate planning and/or project estimation techniques)
- Unrealistic expectations
- Expectations and resources do not match
- Consequences for weak project performance are not applied consistently
- Infrequent/ inaccurate status reporting (earned value not used)

Examples of project objectives not achieved in many organizations are missed deadlines, cost overruns, efficiencies not delivered as expected, flawed software that was not tested before implementation, reduced integration from the initial plan, and less functionality than was identified in the business case when the project was approved.

Finally, another important issue is weak leadership, which can undermine a project at many levels. Common areas of weak leadership include:

- The project champion at the executive level offers limited support or is unengaged.
- Business analysts are weak or not appropriately trained.
- Risk management is weak or poor.
- Project manager or management is weak or inexperienced.
- Project steering committees are ineffective.

Internal Audit's Role

Internal audit should consider performing audits for each aspect of the systems development life cycle (SDLC). Typical elements of the SDLC include a feasibility study, requirements study, requirements definition, detailed design, programming, testing, installation, and post-implementation review.*

* See ISACA Glossary of Terms available at www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf.

KEY QUESTIONS FOR INTERNAL AUDIT TO ASK

1. How are the projects approved within the organization?
2. How are the projects kicked off or initiated within the organization?
3. How are the projects managed within the organization?
4. Do major projects have an executive management champion?
5. Is there a project steering committee in place, and are meetings held periodically?
6. If vendors are involved in the project development, what is the contract administrative process?
7. Are monthly status reports provided?
8. What process does the organization follow if the project is running over budget or taking more time to complete?
9. Does the organization have a process in place to cancel projects if objectives are not being met?
10. Does the IT organization conduct studies of user satisfaction with the outcome and cost of IT projects?

KEY ACTIVITIES FOR INTERNAL AUDIT TO PERFORM

1. Conduct audits throughout the lifecycle of key IT systems development projects. The lifecycle includes contract compliance, project management, costs (such as vendor staffing/billings), project progress, change orders, incentive/bonus programs, and so on.
2. Participate in project audits with the vendor's audit/quality teams to limit the number of audits and/or gain additional knowledge. This will also minimize disruption to the project.
3. Conduct an audit of the organization's project management methodology.
4. Review the portfolio of projects and audit whether the methodology is being followed, especially for projects that are not within budget or on time.
5. Verify that the users are involved in changes to the project scope and deliverables.
6. After the project is completed, review the results of the user satisfaction study conducted by the IT organization, or conduct your own user satisfaction study to verify the results provided by the IT organization.
7. Determine whether a project post mortem/lessons learned activity occurs and is used for future project process improvement.

For more information, see The IIA's *GTAG 12: Auditing IT Projects*, 2009, available at www.theiia.org under Standards & Guidance.

4 IT Governance

DEFINITION OF IT GOVERNANCE

IT governance consists of the leadership, organizational structures, and processes that ensure that the enterprise's information technology supports the organization's strategies and objectives.

—From International Professional Practices Framework (Altamonte Springs, FL: The Institute of Internal Auditors, 2013), 43.

COMPONENTS OF EFFECTIVE IT GOVERNANCE

- Organization and governance structures
- Executive leadership and support
- Strategic and operational planning
- Service delivery and measurement
- IT organization and risk management

—From *GTAG 17: Auditing IT Governance* (Altamonte Springs, FL: The Institute of Internal Auditors, July 2012).

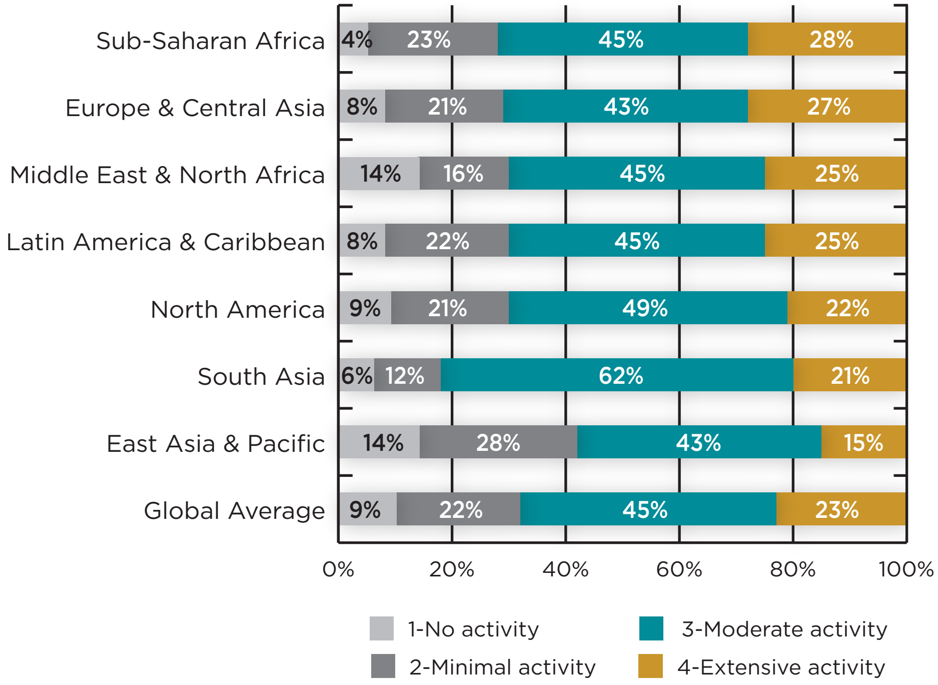
In the wake of recent corporate scandals, significant blame is being placed not only on corporate governance but also on IT governance. Therefore, this topic is #4 on our list of top 10 technology risks.

In many organizations, management is questioning the amount of money spent on IT, and there is increased emphasis to monitor IT costs. This increased emphasis is also due to the widening gap of what IT thinks the business needs and what the business thinks IT can deliver. At a minimum, a good IT governance program must have the following three elements:

- Clear alignment to business
- Measurable value delivery to business
- Accountable controls of resources, risk, performance, and cost

About 3 out of 10 respondents say internal audit activity for IT governance at their organization is none or minimal, which is an area of concern (see **exhibit 4**). Considering the amount

Exhibit 4 **IT Governance Activity**



Note: Q72: What is the extent of activity for your internal audit department related to governance reviews? Topic: Reviews of governance policies and procedures related to the organization's use of information technology (IT) in particular. CAEs only. Those who answered "not applicable/I don't know" were excluded from the calculations. *n* = 2,545.

HOW TO PLAN AN IT GOVERNANCE AUDIT

In scoping and executing an IT governance audit, the internal audit engagement team should:

- Determine whether the IT function aligns with and understands the organization's objectives and strategies.
- Determine the effectiveness of IT resource and performance management.
- Assess risks that may adversely affect the IT environment.

—From *GTAG 17: Auditing IT Governance* (Altamonte Springs, FL: The Institute of Internal Auditors, 2012), 15.

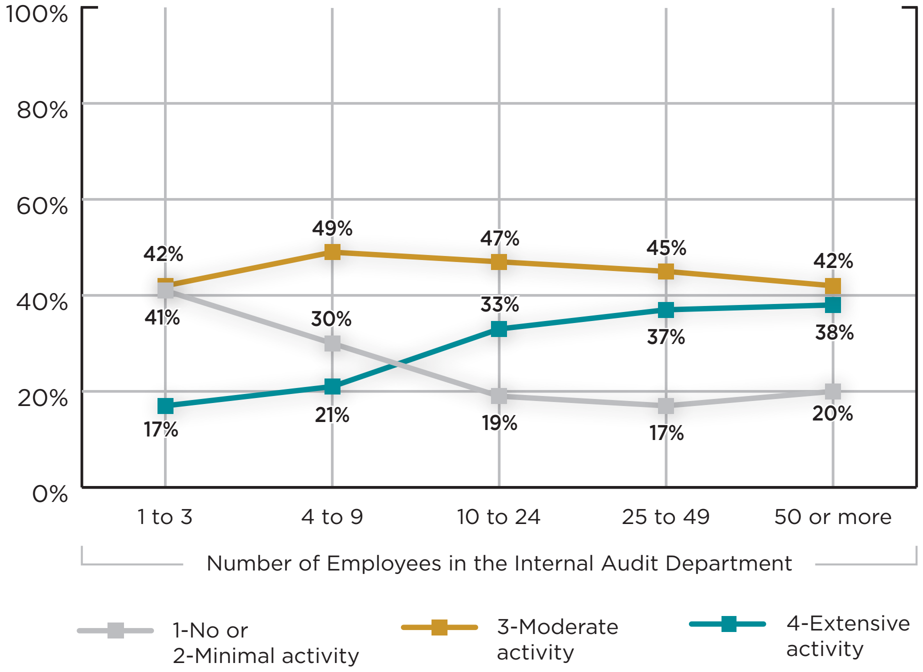
of money spent on technology and its impact on customers and operations, nearly all internal audit departments should have at least moderate activity for IT governance. Among survey respondents, the broadest level of activity for IT governance is in South Asia, with 8 out of 10 respondents reporting moderate or extensive activity.

Internal Audit's Role

Internal audit can help the organization by providing assurance where IT is performing well and has appropriate controls in place to mitigate risk based on the organization's risk tolerance. Another equally important business objective is for the IT infrastructure to be in place to take advantage of opportunities to move the business forward.

Small internal audit departments appear to have difficulty allocating time to review IT governance. In audit departments with three employees or fewer, 4 out of 10 say they have no or minimal activity for IT governance (see **exhibit 5**).

Exhibit 5 **IT Governance Activity Compared to Internal Audit Department Size**



Note: Q72: What is the extent of activity for your internal audit department related to governance reviews? Topic: Reviews of governance policies and procedures related to the organization's use of information technology (IT) in particular. CAEs only. Those who answered "not applicable/I don't know" were excluded from the calculations. *n* = 2,497.

KEY QUESTIONS FOR INTERNAL AUDIT TO ASK

1. What activities is IT performing to align with business? How often does IT meet with business to understand their needs?
2. What is the business perception of IT capabilities and performance?
3. How does IT determine the value it provides to the business?
4. How do IT executives determine the appropriate number of resources to be employed within IT?
5. Does IT perform an IT risk assessment periodically?
6. Does IT have key performance metrics defined to measure its performance?
7. How does IT manage its cost?

KEY ACTIVITIES FOR INTERNAL AUDIT TO PERFORM

1. Assess the "tone at the top" of the IT organization in relation to corporate culture, defined performance measures/expectations, service-level agreements (SLAs), customer service, and so on.
2. Periodically, perform an audit to determine whether the IT function aligns with and understands the organization's strategic priorities.
3. Review the effectiveness of IT resource and performance management.
4. Assess risks that may adversely affect the IT environment.
5. Audit the cost measures in place within the IT environment.
6. Survey the business to determine the business leaders' perception of IT capabilities and performance.
7. Compare the compliance program within the organization to established frameworks such as Control Objectives for Information and Related Technology (COBIT), Committee of Sponsoring Organizations of the Treadway Commission (COSO), National Institute of Standards and Technology (NIST), and International Organization for Standardization (ISO) 27001 and ISO 27002, as appropriate (large organizations).

5 Outsourced IT Services

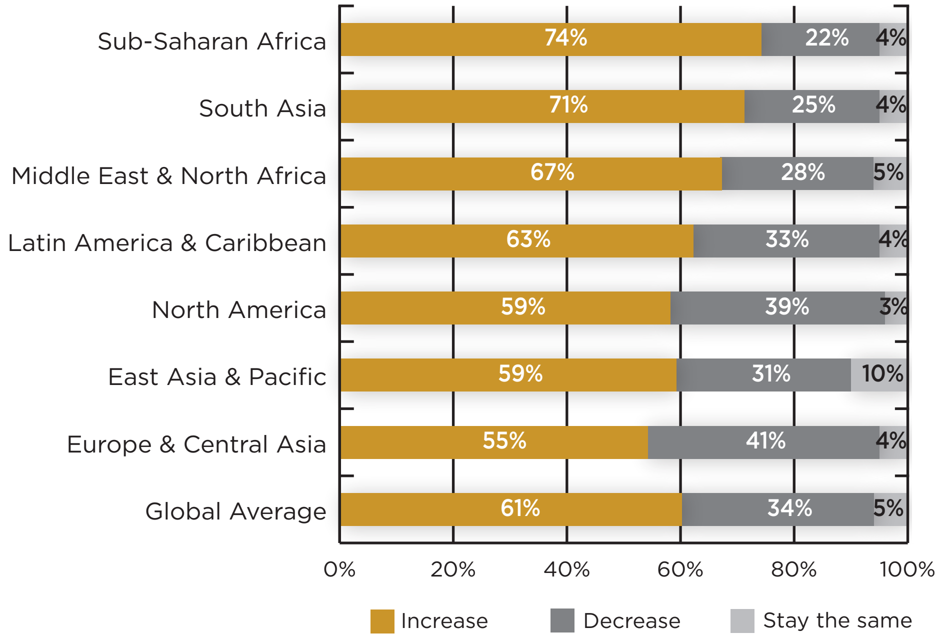
> “Outsourcing IT services equates to providing someone the keys to your kingdom and expecting/trusting them to manage the information as you would.”
>
> —Drew Perry,
> CISSP, CISA ,
> IT Compliance Manager,
> Ashland, Inc.

As mentioned in the previous section, an increased focus on IT costs has resulted in the outsourcing of some key IT services. This has resulted in even more focus on IT governance and elevated outsourced IT services to #5 on our list of the top 10 technology risks. Outsourced IT services can expose an organization to risk that may remain undiscovered until a failure occurs. In some cases, outsourcing places essential technology processes outside the direct control of management. On average, 6 out of 10 internal auditors surveyed say they expect an increase in audits of outsourced IT services over the next year (see **exhibit 6**). The largest increase is expected in Sub-Saharan Africa and the smallest in Europe.

Internal Audit’s Role

Internal auditors can prevent some outsourcing problems from occurring by getting involved earlier in the outsourcing cycle. For example, internal audit should ensure that the initial contract addresses oversight, monitoring, auditing, physical and logical security, appropriate staffing, a contact person, access to information, business continuity plans/disaster recovery, SLAs, and reporting.

Exhibit 6 Future Audits of Outsourced IT



Note: Q94: In the next two to three years, do you think the internal audit activity related to these technology areas will increase, decrease, or stay the same? Topic: Audits of IT procurement, including third parties or outsourced services. *n* = 11,020.

KEY QUESTIONS FOR INTERNAL AUDIT TO ASK

1. Are the outsourced services significant to the organization?
2. Does the organization have a well-defined outsourcing strategy?
3. What is the governance structure relating to outsourced operations? Are roles and responsibilities clearly defined?
4. Was a detailed risk analysis performed at the time of outsourcing, and is regular risk analysis being done?
5. Do formal contracts or SLAs exist for the outsourced activities?
6. Does the SLA clearly define key performance indicators (KPIs) for monitoring vendor performance?
7. How is compliance with the contract or SLA monitored?
8. What is the mechanism used to address noncompliance with the SLA?
9. Are the responsibilities of owning the data system, communication system, operating system, utility software, and application software clearly defined and agreed upon with the service provider?
10. What is the process for gaining assurance on the operating effectiveness of the internal controls on the service provider's end?

KEY ACTIVITIES FOR INTERNAL AUDIT TO PERFORM

1. Get involved early in the outsourcing contract process.
2. Audit a third-party vendor and review their SLAs and KPIs.
3. Review a third-party service where a noncompliance occurred and determine whether the appropriate steps were taken.
4. Ensure that all source code delivered by the outsourcer is scanned for malware.
5. Audit the decision-making process of determining how an organization decides what elements of IT should be outsourced.
6. Select an existing key vendor and review the risk assessment performed before selecting the vendor.

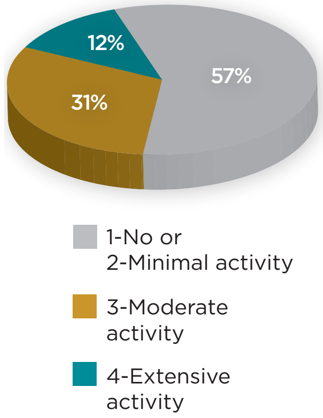
RESOURCES

Auditing Outsourced Functions, 2nd Edition, by Mark Salamasick (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 2012).

GTAG 7: Information Technology Outsourcing, 2nd Edition (Altamonte Springs, FL: The Institute of Internal Auditors, 2012).

6 Social Media Use

Exhibit 7 Assurance for Employee Use of Social Media



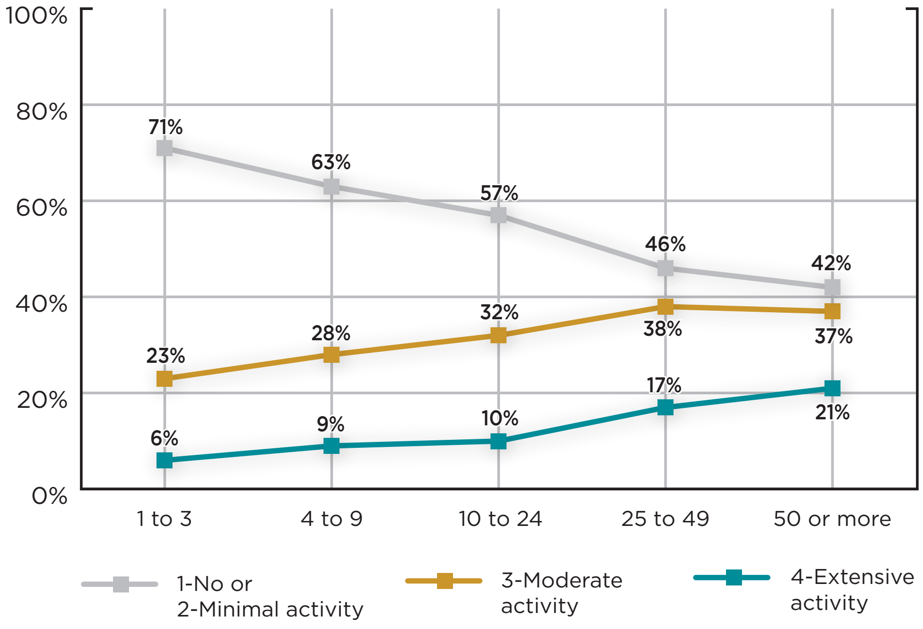
Note: Q92: For information technology (IT) security in particular, what is the extent of the activity for your internal audit department related to the following areas? Those who answered "not applicable/I don't know" were excluded from the calculations. *n* = 9,747.

The speed with which social media spreads messaging has prompted organizations to define social media policies and procedures, which is why it is #6 on our list. These policies have mainly focused on the ways employees can use social media tools and the restrictions imposed on them as to the content that can be shared on social media. If an employee violates the social media policy and posts a harmful message, the potential risks for an organization include:

- Exposure to legal liability, such as defamation, harassment, and privacy violations
- Leakage of proprietary information or trade secrets, which could impact competitiveness
- Damage to the organization's reputation through false, disparaging, or reckless communications

As shown in **exhibit 7**, the current activity of assurance by internal audit for

Exhibit 8 Social Media Assurance Compared to Internal Audit Department Size



Note: Q92: For information technology (IT) security in particular, what is the extent of the activity for your internal audit department related to the following areas? Topic: The organization's procedures for how employees use social media. Those who answered "not applicable/I don't know" were excluded from the calculations. *n* = 8,980.

RESOURCE

Auditing Social Media: A Governance and Risk Guide by Peter Scott and Mike Jacka (John Wiley & Sons with The IIA, 2011).

employee use of social media is very low. Nearly 6 out of 10 respondents report no or minimal activity. Only 1 out of 10 say they have extensive activity. Larger internal audit departments are more likely to be active in social media assurance (see **exhibit 8**). Nevertheless, 4 out of 10 of the largest internal audit departments still indicate no or minimal activity in this area.

To address the social media risks, organizations must incorporate the following steps as part of their social media procedures:

1. Define an appropriate social media business-use policy.
2. Communicate the policy via a security awareness and training program.
3. Implement the policy through deployment of "content filtering" software for technologies, such as Web 2.0.
4. Monitor the results to ensure the policy is being followed.
5. Enforce the policy for those who violate it.

Internal Audit's Role

Internal auditors can play a key role in managing the risks associated with social media. They can play the role of consultants while the organization is implementing the steps outlined above. In addition, internal audit should consider including a social media audit as part of its annual audit plan.

KEY QUESTIONS FOR INTERNAL AUDIT TO ASK

1. How does the organization use social media to reach its clients or customers?
2. What content is allowed to be posted on social media sites?
3. Is there a group or person responsible for monitoring the actual content available on social media sites (performing a scan of social media sites)?
4. What content is monitored by the "content filtering" software? Who monitors the alerts created by the software?
5. What are the consequences for an employee who violates the social media policy?

KEY ACTIVITIES FOR INTERNAL AUDIT TO PERFORM

1. Perform an audit of social media policies and procedures.
2. Review the adequacy of the awareness training to ensure that the social media topic is covered.
3. Understand the use of "content filtering" software and its effectiveness to monitor the content's entry and exit.
4. Perform an independent scan of social media sites to determine the organizational content that is available.

7 Mobile Computing

> *"Information travels with its users, therefore security data must be as robust in mobile devices as it is in the headquarters. Tablets, personal computers, mobile phones, Smartwatches, etc. are small data centers where most of the company´s strategic information is stored (or data enough to attack the central servers). The amount of equipment that is stolen and/or lost aggravates the situation."*
>
> — Alejandro Rembado Mendizábal, CAE, Telefonica de Argentinal

The proliferation of mobile devices as well as improvements in technology, features, and applications have revolutionized the workforce and given new meaning to the term "mobile computing and mobile worker," and is #7 on our list of top 10 technology risks. Yesterday's mobile worker typically worked with a laptop, connecting remotely to the organization's network. Today's mobile worker typically harnesses more computing power by working with mobile devices such as phones or tablets that use specially designed applications to conduct business.

Mobile devices provide organizational users with portable computing power, Internet connectivity wherever there is Wi-Fi or cellular service, and the convenience of having one device for personal and business use. At the same time, mobile devices—whether organization- or employee owned—have introduced a myriad of device and network configuration risks that challenge an IT department's traditional approach to risk management.

Security Risks

Information stored on mobile devices may include personal and organizational data. It may be compromised if the device is physically lost or stolen, the device user leaves the organization without deleting company data from the device, or appropriate security controls are not in place and operating as intended.

Compliance Risks

With the advent of bring your own device (BYOD), organizations largely rely on users to comply with applicable policies and procedures, such as guidelines for updating software or operating systems. Users who consider updates to be overly intrusive or degrading to the performance of the device might choose not to install the updates or to bypass controls.

Privacy Risks

BYODs may raise privacy concerns from the perspectives of the organization and the employee. For example, it may be increasingly difficult for an organization to protect a stakeholder's privacy when personally identifiable information (PII) is accessed or stored on a smart device. Conversely, employees may have privacy concerns that their smart device enables intrusive monitoring by the organization, or that the organization might inadvertently wipe personal information (e.g., pictures and contact information) from their device when organizational data is deleted.

Management Risks

BYODs require the management of expanded IT support services. As the number of device types increases, so does the potential for network vulnerabilities. In addition, when the devices are upgraded, the requirement to properly dispose of the device may increase management risk. If BYODs are provided for outside service providers, the management of organizational data on the service provider's BYOD devices may increase management risks as well.

Legal Risks

An organization needs to understand the legal implications of storing its data on smart devices, such as whether and how litigation holds and e-discovery requirements apply.

Internal Audit's Role

As shown in **exhibit 9**, only 51% of the internal audit departments reported moderate or extensive activity, which means almost half the organizations are doing no or minimal activity in this area.

KEY QUESTIONS FOR INTERNAL AUDIT TO ASK

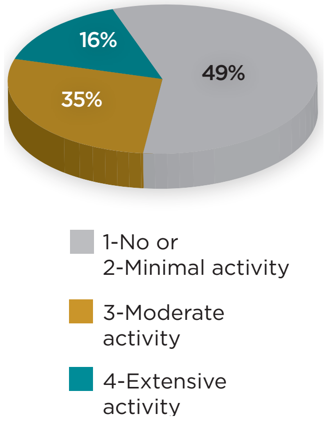
1. Does the organization have a process to inventory all mobile computing devices?
2. How does the organization manage stolen or lost mobile computing devices?
3. How does the organization manage BYODs?
4. How does the organization manage the content on mobile devices when an employee leaves the organization?
5. Are the mobile devices encrypted?

KEY ACTIVITIES FOR INTERNAL AUDIT TO PERFORM

1. Perform an audit of the inventory process of mobile computing devices.
2. Perform an audit of how lost or stolen devices are managed.
3. Understand the way an organization decides on the type of information that can be stored on the mobile devices.
4. Verify that sensitive information is not stored on mobile devices or that sensitive information is encrypted.

> *"Online banking in Africa and parts of the Middle East poses a great risk than in other regions due to the high use of cell phones for online banking."*
>
> —Grace Lwanga, Technical Director, IT Audit, World Vision International

Exhibit 9 Assurance for Use of Mobile Devices



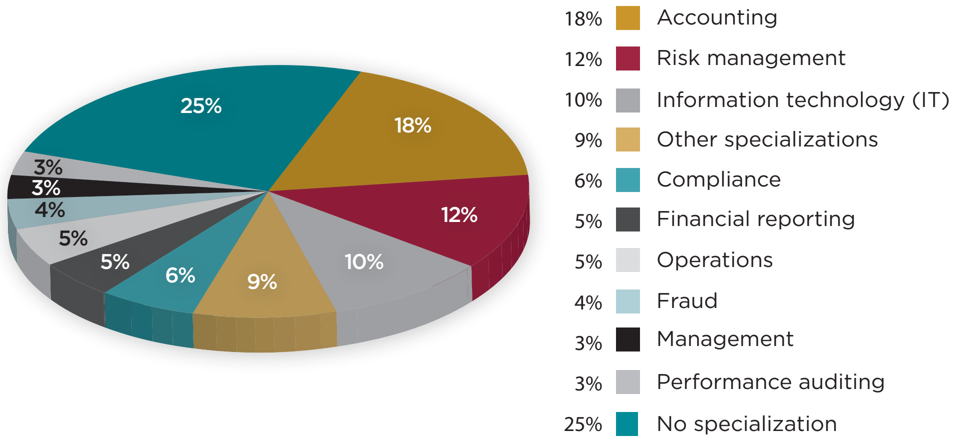
Note: Q92: For information technology (IT) security in particular, what is the extent of the activity for your internal audit department related to the following areas?

8 IT Skills Among Internal Auditors

The number of qualified IT auditors is a continuing problem for internal audit, and the topic is #8 on our list of top 10 technology risks. Among survey respondents, only 10% say they specialize in IT (see **exhibit 10**). This problem is caused by a number of things, the most prevalent being that IT professionals have the opportunity to use new technology and command higher salaries than IT auditors, says Mark Salamasick, executive director of Audit Academic Institutions for the University of Texas System. "Salaries for auditors with a technology background/expertise are generally not in line with salaries of IT positions, resulting in less than optimum IT audit-skilled auditors in many organizations."

One approach to increase the number of auditors with IT skills is to provide IT training to operational/financial auditors with an IT aptitude. However, it can be difficult for these internally trained internal audit staff members to establish their credibility with the IT department and management. Sudarsan Jayaraman, managing director for IT Consulting Services for Protiviti–Middle East, commented, "IT auditors need more specialized skills to be successful in performing many high-risk audit activities/engagements. Unless IT auditors have high-level skills, including experience as IT professionals, management is often not comfortable with their skills and audit results."

Exhibit 10 **Technical Specializations Among Survey Respondents**



Note: Q11: In addition to performing general internal audit activities, do you have an area of technical specialization for which you have had formal training and in which you spend a majority of your time working? *n* = 13,144.

Internal Audit's Role

Internal audit can take several steps to address the shortage of IT skills within their department. The first step is to take an inventory of IT skill shortage within their group by:

1. Understanding the types of technologies used within the organization
2. Mapping the technology skills within the group to the technologies used within the organization
3. Identifying the skill gap for all the technologies that are not covered by the internal audit group

After the gaps are identified, internal audit has several options to address the skill gaps:

Option 1: Develop the skills internally by allocating an appropriate amount of budget and providing training to the team.

Option 2: Implement a process of rotating IT skills by working with the chief information officer (CIO).

Option 3: Work with a third-party service provider to outsource or co-source and address the IT skill gap.

KEY ACTIVITIES FOR INTERNAL AUDIT TO PERFORM

The following six action items are useful for developing relationships between internal audit and the IT department and to increase awareness of IT processes in general:

1. Build relationships with key IT staff and demonstrate how IT audit adds value to the organization.
2. Attend key IT meetings (e.g., IT systems development project steering committees, information security updates, new technologies, etc.) to better understand significant IT challenges and risks.
3. Meet periodically with primary IT staff members, including the chief technology officer (CTO) and the CISO.
4. Hire auditors who have backgrounds in technology to increase IT skills and audit credibility with IT management.
5. Perform IT governance audits.
6. Work with and share information about key organizational risks with other risk management, governance, control, and compliance areas to reduce duplication of effort and minimize disruption to an already overwhelmed IT staff.

Finally, report to the board about progress achieved in these six activities. This will strengthen the technology understanding of the board and audit committee and will hold internal audit accountable for growth in IT auditing effectiveness.

9 Emerging Technologies

The pace with which the technology is changing and evolving is mind-boggling and can rapidly introduce new risks to an organization. Therefore, the topic of emerging technology is #9 on our list of top 10 technology risks. Emerging technology can mean different things to different organizations. To some, the use of smart devices may be an emerging technology; in others, the use may already be established. For the purposes of this discussion, we define emerging technology as that which is not in use within the organization today but may be deployed in the near future. Examples include:

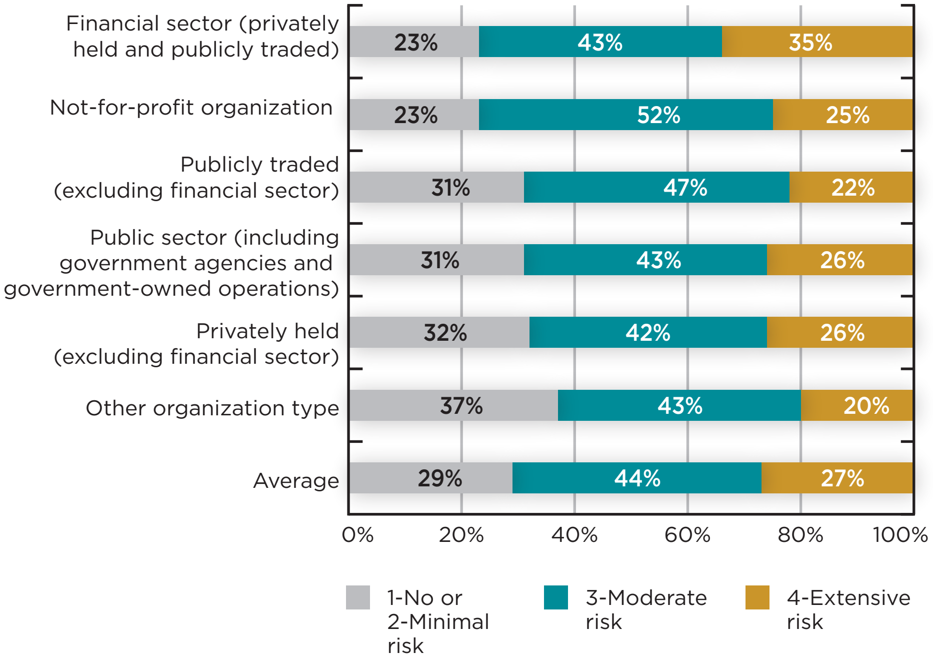
- Predictive data analysis
- Big data
- Fog computing (where cloud computing is extended to the edge of the enterprise's network)
- 3D printing (where printers are programmed to output three-dimensional objects)
- The Internet of things (where everyday objects like refrigerators or microwaves have network connectivity and can send and receive data)
- Robotics

It is also possible that a certain technology may already be deployed within one industry (for example, big data in the financial sector) but not in other industries. These differences would affect the perceived level of risk as well. As **exhibit 11** shows, the finance industry perceives the highest level of risk for big data reliability.

Internal Audit's Role

Internal audit can play a key role in the adoption of emerging technologies within the organization. It can get involved in the early stages of the evaluation process of a new technology and provide guidance in terms of its risk and control requirements. For example, if an organization is considering adopting the cloud computing services for the first time, internal audit can be part of the technology task force to determine the additional risks introduced by such an environment (or, in some cases, the reduction in risks).

Exhibit 11 **Big Data Reliability Risk Compared by Organization Type**



Note: Q93: In your opinion, what is the level of inherent risk at your organization for the following emerging information technology areas? Those who answered “not applicable/ I don’t know” were excluded from the calculations. Due to rounding, some totals may not equal 100%. *n* = 9,373.

KEY QUESTIONS FOR INTERNAL AUDIT TO ASK

1. Does the organization have a team that evaluates emerging IT technologies?
2. Does the organization have a formal process of evaluating emerging technologies?
3. How does the organization identify the risks introduced by emerging technologies?
4. What current projects are underway where new technology will be deployed within the production environment?

KEY ACTIVITIES FOR INTERNAL AUDIT TO PERFORM

1. Obtain an inventory of current technologies in use.
2. Understand the new projects where emerging technology may be deployed.
3. Audit the risk process for emerging technologies (how risk is identified during the evaluation of emerging technology).
4. Discuss with the IT technology team to understand their strategy for adopting emerging technologies.

10 Board and Audit Committee Technology Awareness

"In problem post mortems, a frequent root cause is that people didn't understand their own business—'how it works' and 'what if?' To overcome this problem and give people the opportunity to act before it's too late, it's vital to create an environment where people can deeply understand their situation and options."

—Brian Barnier,
Principal, ValueBridge
Advisors & Fellow, OCEG

A number of organizations have limited IT expertise represented on their board of directors. Therefore, this topic is #10 on our list of top 10 technology risks. An appropriate level of IT knowledge on the board is necessary for the board to hold IT accountable for performance. Gunther Meggeneder, senior vice president, Corporate Internal Audit and Compliance, ista International, observes, "It is important for the Board/Audit Committee over the next few years to have more IT expertise similar to how they have progressed in having strong financial representation."

Because IT enables the business and requires a significant investment, it is risky for a board to lack IT knowledge.

"Within the next four to five years, every Board of Directors should have an IT technologist or at least have someone that sits on their advisory board," says Scott Klososky, partner in Future Point of View, LLC.

Internal Audit's Role

Internal audit plays a key role and is the main conduit of bringing technology awareness to the board and the audit committee. It is responsible for gauging the technology savviness of its audit committee and playing the role of educator and/or consultant to the audit committee.

KEY QUESTIONS FOR INTERNAL AUDIT TO ASK

1. What is the organization's IT strategy if technology changes are planned?
2. Does the audit committee understand the IT risks, and can it relate in context of enterprise risks?
3. Does the audit committee understand its responsibility and role it plays in context of enterprise risk and technology awareness?

KEY ACTIVITIES FOR INTERNAL AUDIT TO PERFORM

1. Ensure that technology awareness is included in meetings with the audit committee.
2. Act as advisors to the organization when it is making decisions on emerging technology (e.g., when the organization is planning to move sensitive information in the cloud or when sensitive information is housed with a third-party service provider).

Conclusion

Internal auditors have worked diligently to think strategically, understand the business, and add value. Now they need to be proactive to identify emerging technologies that could impact their organizations. Experts offer these recommendations:

1. Implement a process for being situationally aware.
2. Watch for warning signals in your industry or environment.
3. Ask "what if?"
4. Maintain a list of emerging technology risks and opportunities that can be reviewed to determine their potential impact.
5. When a risk or opportunity is identified, take action to follow up in response.

Although it is impossible to predict the future, we can be certain that the technology landscape will change. Internal auditors should be prepared to adapt.

About the Project Team

CBOK Development Team

CBOK Co-Chairs:
Dick Anderson (United States)
Jean Coroller (France)
Practitioner Survey Subcommittee Chair:
Michael Parkinson (Australia)
IIARF Vice President: Bonnie Ulmer

Primary Data Analyst: Dr. Po-ju Chen
Content Developer: Deborah Poulalion
Project Managers: Selma Kuurstra and Kayla Manning
Senior Editor: Lee Ann Campbell

Report Review Committee

Ulrich Hahn (Germany)
Steve Hunt (United States)
Richard Martin (United States)

Michael Parkinson (Australia)
Kurt Reding (United States)
Dave Williams (United States)

Sponsorship

This report is sponsored in part by The IIA-Austin Chapter. We thank them for their generous support.

About the Authors

Note: This content of this report is a collaboration between Phil Flora, who developed the list of top 10 risks, conducted interviews with experts around the world, and developed the initial text, and Sajay Rai, who developed final text and provided the key questions and key activities for each chapter.

P**hilip E. Flora**, CIA, CISA, CFE, CCSA, is the principal/managing member for FloBiz & Associates, LLC, member of the YCN Group, and an IIA training consultant. Phil has more than 30 years of auditing experience and was the chief audit executive (CAE) at a not-for-profit public corporation for more than 16 years. He helped create an Internal Audit Leadership Development Program that has helped develop more than 50 future audit leaders. Phil is currently a member of The IIARF's Board of Trustees. He is past chair of The IIA's International Committee and The IIARF's Committee of Research and Education Advisors (CREA), and has served on IIA international committees since 2000. He has been a frequent speaker at various state, regional, national, and international conferences and training events for the past 10 years. Phil received a bachelor's degree in accounting from Virginia Commonwealth University.

S**ajay Rai**, CPA, CISSP, CISM, is co-founder and owner of Securely Yours, LLC. With more than three decades of experience in IT, Sajay Rai brings a wealth of knowledge in information security and risk, IT audit, business continuity, disaster recovery, and privacy. Before starting Securely Yours, Sajay served as a partner at Ernst & Young LLP, responsible for the information advisory practice in the Detroit Metro area, and was also the national leader for Ernst & Young's security and risk practices. Prior to Ernst & Young, he was with IBM, where he led its information security and business continuity practices. He has served on The IIA's Professional Issues Committee (PIC) and as a board member of the IIA–Detroit Chapter. He holds a master's degree in information management from Washington University of St. Louis and a bachelor's degree in computer science from Fontbonne College of St. Louis.

Your Donation Dollars at Work

CBOK reports are available free to the public thanks to generous contributions from individuals, organizations, IIA chapters, and IIA institutes around the world.

Donate to CBOK

www.theiia.org/goto/CBOK

About The IIA Research Foundation

CBOK is administered through The IIA Research Foundation (IIARF), which has provided groundbreaking research for the internal audit profession for the past four decades. Through initiatives that explore current issues, emerging trends, and future needs, The IIARF has been a driving force behind the evolution and advancement of the profession.

Limit of Liability

The IIARF publishes this document for information and educational purposes only. IIARF does not provide legal or accounting advice and makes no warranty as to any legal or accounting results through its publication of this document. When legal or accounting issues arise, professional assistance should be sought and retained.

Contact Us

The Institute of Internal Auditors Global Headquarters
247 Maitland Avenue
Altamonte Springs, Florida 32701-4201, USA