A Global View of Financial Services Auditing

FUTURE

Closer Look

Challenges, Opportunities, and the Future

Jennifer F. Burke
CPA, CRP, CFF, CFS

Steven E. Jameson
CIA, CFSA, CRMA, CPA, CFE

The IIA Research Foundation

CBOK
The Global Internal Audit Common Body of Knowledge

Sponsored by

Crowe Horwath

About CBOK

SURVEY FACTS

Respondents	14,518*
Countries	166
Languages	23

EMPLOYEE LEVELS

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

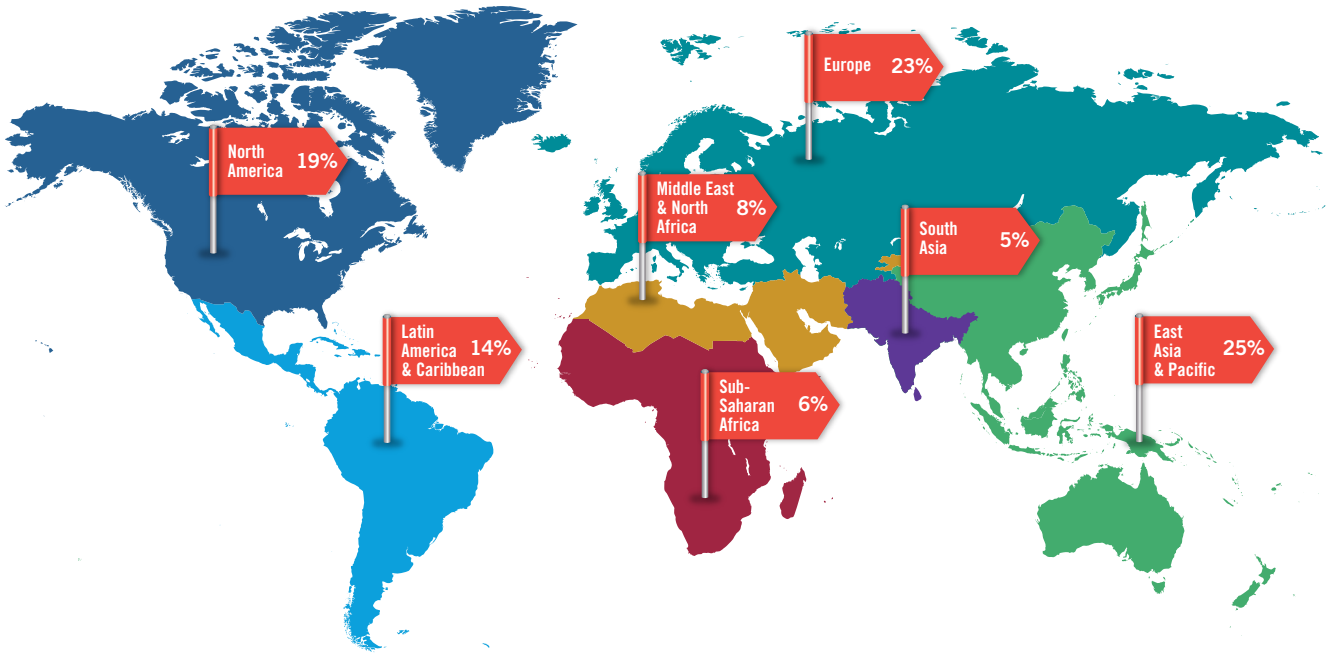
*Response rates vary per question.

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

Many in the financial services industry will agree that times have never been more challenging than they are today. While there are many issues facing internal auditors at financial institutions, this report focuses on the following key challenges:

1. Regulatory requirements, which generally top most financial institutions' risk lists
2. Managing governance committee agendas that are increasingly crowded
3. Heightened expectations for internal auditors
4. Increased technology risks as cyber criminals find new ways to penetrate defenses
5. Coordination among all lines of defense
6. Resource allocation management

Regulatory compliance has continued to move up the list of priorities and often assumes a starring role in discussions from the back office to the boardroom. New and changed regulation has required increased spending for additional staffing, new technologies, revised processes, and even a reduction in fees and revenue for financial institutions. The changes have been so encompassing that even the indirect partners and vendors that serve financial institutions have been impacted in significant ways.

Those charged with governance activities and oversight have found their workloads expanding. Time demands for more and longer meetings to cover expanded agendas have challenged financial institutions to become more efficient in order to devote sufficient time to the ever-increasing number of issues that need to be discussed. The number of attendees at these meetings has also contributed to lengthier meetings.

While internal auditors have long sought to be recognized and invited to be part of strategic discussions at their financial institutions, the heightened expectations from multiple stakeholders that have elevated the internal audit activity have also brought unique challenges. Given the nature of internal audit to focus on problems, weaknesses, and uncontrolled risks, these heightened expectations have put increased pressure on internal auditors to make the right call—and increased the consequences for those who make the wrong call.

Internal auditors have often leveraged technology to provide increased audit coverage over expanded audit universes while effectively using limited resources. Today, technology is expanding so quickly that maintaining effective control is almost impossible. To add to the challenge, criminals now use technology to facilitate continuous global attacks against financial institutions and their customers.

There are some rays of hope for internal auditors in financial institutions as new defense models are created and adopted to tackle the many challenges they face. The Three Lines of Defense is one model that has gained more widespread acceptance and adoption around the globe in recent years. Internal auditors in financial institutions are challenged with finding ways to effectively implement this model in a way that works for their organizations. In smaller institutions, the lines between the second and third lines of defense are often blurry, challenging internal auditors to clarify roles and responsibilities.

Generational differences, expanded skill-set requirements, shrinking resource pools, and rotational chief audit executive (CAE) programs are creating challenges in managing audit resources. Such challenges have always been part of the job for most CAEs. While not necessarily a new challenge in and of itself, the methods that were used in the past to manage resource challenges do not always work today. New methods and approaches for resource acquisition and management must be developed to work in the future.

1 Regulatory Challenges for Financial Services Internal Auditors

> *"Pre-planning is more important now as extra complexities are part of regulatory changes, and organizations must plan for reduced revenue due to some of the changes."*
>
> —James Alexander, Chief Risk Officer, Unitus Community Credit Union, Portland, Oregon

Ask financial services internal auditors what keeps them up at night and most will put regulatory challenges high on their long list of key risks. There was a time when regulatory compliance was primarily left up to the legal and compliance departments, leaving internal auditors to focus on financial and operational issues. Today, regulatory compliance touches every function in a financial institution.

Compliance and regulatory risk topped the list when CAEs worldwide were asked to choose the top five risks on which their internal audit departments were focusing the greatest level of attention in 2015. Compliance and regulatory risk was followed closely by operational risk (see **exhibit 1**). CAEs from the financial sector also indicate that their audit plans focus on these areas, although they plan to devote more of the audit plan to operational issues rather than concentrating on compliance (see **exhibit 2**).

Exhibit 1 Risk Areas CAEs Plan to Focus on in 2015

Risk Area	Percentage Response
Compliance/regulatory	83%
Operational	78%
Risk management assurance/effectiveness	68%
Information technology	67%
Strategic business risks	53%

Note: Q66: Please identify the top five risks on which your internal audit department is focusing the greatest level of attention in 2015. CAEs only. Filtered by financial sector. *n* = 582.

Exhibit 2 Risk Areas Comprising Highest Percentage of 2015 Audit Plan

Risk Area	Percentage of Audit Plan
Operational	25%
Compliance/regulatory	16%
Risk management assurance/effectiveness	14%
Information technology	11%
Strategic business risks	10%

Note: Q49: What percentage of your 2015 audit plan is made up of the following general categories of risk? CAEs only. Filtered by financial sector. *n* = 558.

> *"Wall Street banks and their foreign rivals have paid out $100 billion in U.S. legal settlements since the financial crisis, with more than half of the penalties extracted in the past year."*
>
> —FinancialTimes.Com, March 25, 2014

New Regulatory Agencies and Laws Worldwide

In the past, regulatory changes seemed to be less impactful. They might affect what or how much was disclosed to consumers, disclosure forms might be revised, and so on. Recent changes in the past few years seem to not only impact what and how much is released on disclosure forms, but they also require substantial operational changes to systems and processes. These changes seem to have a pyramiding effect on multiple systems and operational units. Changes today are greater and more intrusive on bank operations.

New regulatory agencies with increased and expanded powers have been created to oversee and monitor financial institutions. The Financial Services Authority of Indonesia, the Financial Conduct Authority and the Prudential Regulation Authority in the United Kingdom, and the Consumer Financial Protection Bureau in the United States are but a few examples of the new governing bodies emerging around the world.

New laws and regulations have been enacted with ever-increasing volume and frequency. Examples of new and revised regulations include Basel III, a comprehensive set of reform measures to strengthen regulation, supervision, and risk management developed by the Basel Committee from the Bank of International Settlements, and the revised directive on Markets in Financial Instruments (MiFID II) and the regulation on Markets in Financial Instruments (MiFIR), both from the European Union.

In the past, the establishment of new or revised laws and regulations included proposals for public comment, consensus gathering, and sufficient implementation periods to ensure those affected were able to effectively implement new and revised regulations. That approach has been brushed aside with a process that emphasizes expediency under the mantra of protecting consumers and investors at all cost. Many describe this new approach as "regulation by enforcement." Record fines and penalties reaching well into the billions of dollars have been levied against financial institutions over the past few years.

Traditionally, internal auditors in the financial services industry have not been heavily involved in auditing for regulatory compliance. Regulatory compliance audits or reviews were usually conducted by a separate compliance group. In recent years, particularly due to the operational impact of regulatory changes and the increased risk of lack of regulatory compliance, internal audit groups have become much more involved in regulatory compliance issues, including auditing compliance or the compliance group, tracking and monitoring compliance with laws and regulations, evaluating operational impact from compliance changes, ensuring systems are in place to monitor consumer complaints, evaluating the adequacy of regulatory training for employees, and serving as liaison between their financial institution and the armies of regulators who visit or are permanently stationed in their financial institutions.

> *Due to scrutiny of banks, regulators are increasing their reliance on internal audit and hence many banks are considering creating specific audit teams to concentrate only on regulator requests. This will alleviate the capacity constraints faced by audit teams.*
>
> —Jenitha John, CAE, FirstRand, South Africa

Regulator expectations for internal auditors have also increased significantly. These expectations can vary based on the size of the institution and the specific regulator that may oversee the operation. In many cases, regulatory expectations go beyond The IIA's *International Standards for the Professional Practice of Internal Auditing* (*Standards*) for financial institutions, particularly in the areas of independence, reporting structure, audit coverage, audit reports, and challenging management. In some countries, the regulators also expect internal audit to review and comment on the risk and control culture within the organization. These expectations have been elevated to the point where some have suggested that maybe internal audit should have a formal, direct reporting relationship to the regulators. Various indirect reporting relationships are already in place in some countries.

In an unprecedented expansion of regulatory authority, even the vendors that serve financial institutions have come under the scrutiny of financial services regulatory agencies. While the regulators are generally not able to directly regulate nonfinancial services organizations, new laws and regulations have been enacted and enforced on financial institutions in such a manner that vendors who serve financial institutions must comply or risk being disqualified as a service provider. Reputation risk can increase regulatory scrutiny on the financial institution even when a vendor has an isolated issue with a non-core service.

Regulatory compliance was once primarily a cost consideration for financial institutions. Today, laws and regulations have been enacted and enforced such that revenue sources are being affected. The risk inventory related to regulatory compliance is already laden with increased costs, decreased revenue, major operational and technology changes, vendor relations, potential fines, penalties, and restitution of charges to customers. However, to increase the intensity, one can also add strategic and reputation risk to the list. Regulatory compliance issues have been at the heart of class action lawsuits, investor lawsuits and proxy fights, consumer advocacy group demands, public memorandums of understanding from regulators, and pressure from boards of directors to resolve issues. The regulatory burden has caused some financial institutions to seek out merger partners because the burden has grown too large to address as a stand-alone entity.

2 Crowded Audit and Risk Committee Agendas

Audit and risk committee time has become a precious commodity as meeting agendas have continued to expand in order to address additional responsibilities coming from a multitude of sources. Shareholder and investor expectations continue to grow and regulatory expectations show no signs of diminishing. Boards of directors have turned to audit and risk committees to help them satisfy fiduciary responsibilities and provide some level of liability limitations against lawsuits and regulatory actions.

Audit and risk committee meetings continue to grow in both meeting frequency and duration. According to survey respondents, the financial sector has the highest average number of formal audit committee meetings compared to all other organization types, averaging 6.7 meetings per year (see **exhibit 3**).

In addition to the financial sector having a higher number of meetings, the time allocated to each agenda item shrinks as the number of items and presenters continues to increase. Issues to be addressed have increased in complexity, requiring lengthier discussions. Increased requirements for audit and risk committee member qualifications have resulted in members who ask more questions, which require more explanation and discussion in meetings. While increased engagement and interaction by audit committee members is generally a good thing, it does require more time and effort to accommodate increased interactions.

Exhibit 3 Average Number of Formal Committee Meetings Per Year

Type of Institution	Average Number of Meetings
Financial sector (privately held and publicly traded)	6.7
Publicly traded (excluding financial sector)	6.4
Not-for-profit organizations	6.2
Public sector (including government agencies and government-owned operations)	5.9
Other organization types	5.6
Privately held (excluding financial sector)	5.3

Note: Q78: Approximately how many formal audit committee meetings were held in the last fiscal year? CAEs only. *n* = 1,894.

The cast of characters at any given meeting has grown to include chief executive officers (CEOs), chief financial officers (CFOs), CAEs, chief risk officers (CROs), chief compliance officers (CCOs), chief technology officers (CTOs), chief privacy officers (CPOs), legal counsel, business unit managers for reports that are presented, loan review managers, security officers, BSA/AML officers, external auditors, and third-party advisors and consultants. Add standing executive sessions for the committees, along with private meetings with both internal and external auditors, and it is no wonder that meetings are jam-packed and often feel rushed.

To address the crowded agenda challenges, many financial institutions have added or increased sessions between meetings, set up calls between committee chairs and the CAE, and posted or sent out advance meeting packages so that committee members can prepare beforehand and help expedite the discussions. Meeting packages have exploded in size due to complex issues that require additional explanation.

CAEs continue to struggle with the challenges of writing audit reports directed at multiple audiences that each require different levels of detail. For example:

- Board members need reports focused on high-level strategic risks.
- Executive management needs more specifics to identify corrective actions.
- Operating management often needs extensive details in order to revise systems and processes to properly implement complex changes.

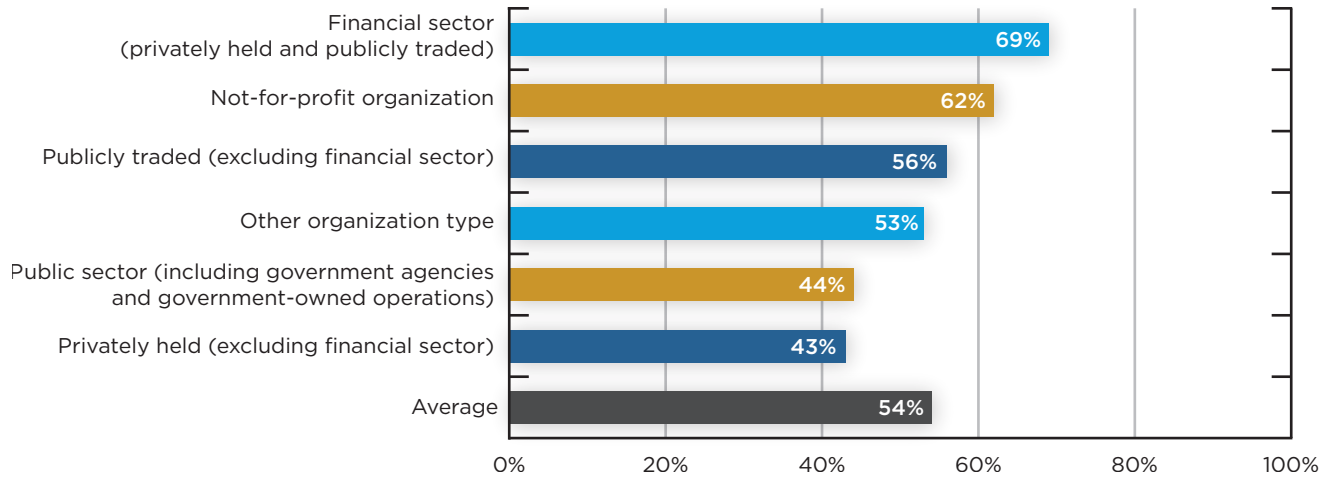
With the increased expectations, it is very difficult for audit and risk committees to be effective in today's environment. Additional time must be allotted to cover expanded meeting agendas and increased discussion time. It is imperative for CAEs to ensure that audit committee meetings focus on the most important topics and that risk-based audit plans are developed that address the issues of concern for management and audit committees. Succinct, impactful audit reports can contribute to efficient use of management and audit committee member time and facilitate more effective discussions in meetings.

3 Challenges Due to Elevation of Internal Audit

CAEs have long desired to be elevated in stature and recognition to facilitate independence, add weight and importance to audit recommendations, interact more frequently with executive management and board members, and obtain more first-hand knowledge and input to strategic initiatives. It appears the caveat about "being careful what you ask for" has become reality for many, bringing with it both opportunities and challenges. CAEs are finding themselves in the middle of almost every problem imaginable.

Expectations of management, directors, regulators, and external auditors have all raised the bar for internal audit performance. These internal audit stakeholders are often at odds with each other regarding their internal audit expectations, putting internal audit in the difficult position of serving multiple inconsistent masters. Internal auditors in financial institutions often must go beyond what the *Standards* requires in matters of governance, strategic involvement, reporting, and challenging management decisions to meet expectations. In addition, financial services auditors report directly to the audit committee much more often than internal auditors in other industries. According to survey respondents, 69% of financial services internal auditors report directly to the audit committee, compared to just 54% across all industries (see **exhibit 4**). Elevated expectations have increased internal audit workloads and audit schedules, stretching resources to even greater limits.

Exhibit 4 CAEs Reporting Functionally to Audit Committees



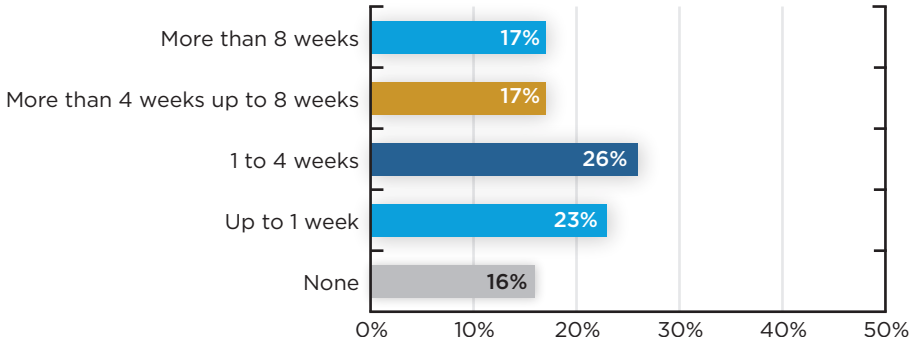
Note: Q74: What is the primary functional reporting line for the chief audit executive (CAE) or equivalent in your organization? CAEs only. *n* = 2,634.

Assistance Provided to External Auditors

Traditionally, internal auditors often devoted substantial resources to supplementing or assisting external auditors. This still occurs, but now internal audit groups must also supplement and assist regulatory examiners almost as much as or more than external auditors. In some cases, new accounting regulators have actually placed additional restrictions on relying on the work of internal auditors, resulting in additional external audit work and fees. This in turn can cause management and board members to question the resources allocated to internal audit while having to pay additional fees to external auditors and even regulatory agencies. According to survey respondents, when compared to all other industries, the financial and insurance industry classification is the most likely to provide support to external auditors, with only 16% reporting they provide no support to external auditors. Additionally, the financial services sector spent the most time supporting external auditors—34% spent more than 4 workweeks, while 17% of those spent more than 8 workweeks providing support (see **exhibit 5**).

Requirements to ensure audit recommendations are enacted have placed more emphasis on the formality of internal audit follow-up programs. Follow-up must go beyond simply asking management to confirm implementation of recommendations. Formal testing to validate timely implementation is becoming more important and adding to the audit workload, further taxing limited resources. Survey respondents indicate that other industries are more likely to have the process owner have primary responsibility for the follow-up action (25% on average, compared to 19% in financial services), while financial services internal auditors are more likely to share that responsibility with process owners (54%, compared to the overall average of 50%). (*Source:* Q52, *n* = 3,216.) Once again, internal audit resources in the financial services sector are stretched thin due to this additional responsibility.

Exhibit 5 Number of Weeks Per Year That Internal Audit Supports External Audit



Note: Q51: Approximately how many workweeks did the internal audit department at your organization spend last year on activities that supported external audit? CAEs only. Filtered by financial sector. *n* = 560.

Regulators Asking Internal Auditors to Challenge Management

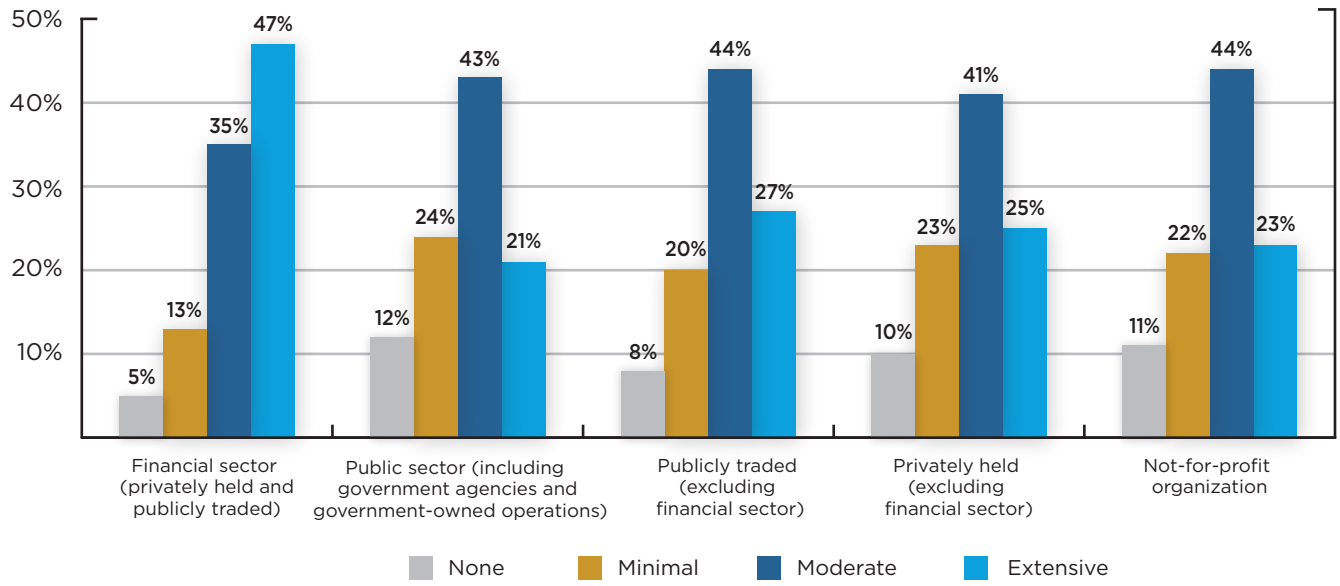
The regulators' elevation of internal audit's importance has expanded the scope of examinations from beyond simply looking at a few reports and workpapers to more comprehensive assessments of all aspects of internal auditing. In some cases, regulators almost seem to be trying to make internal audit groups an extension of the regulators themselves. Internal auditors have been asked to circumvent normal or traditional resolution processes in challenging management, reporting to the board, and even reporting issues directly to regulators. Many internal auditors worry that the results of their work will be used by regulators to cite additional deficiencies in regulatory examination reports. James Alexander, chief risk officer, Unitus Community Credit Union, Portland, Oregon, believes "a good follow-up system for audit report comments can lessen the potential for regulators to cite internal audit report comments as examination findings." Traditional disagreement resolution processes typically resolved many items prior to those items being reported to the board or regulators. Regulators' heightened expectations look for internal auditors to "challenge" management if differences of opinion exist and seek evidence that these situations are escalated to the audit committee or board.

The elevation of internal audit certainly has its benefits, but it is not without its challenges. With greater expectations and increased reporting and responsibilities come greater requirements for internal auditors to establish appropriate safeguards for independence, objectivity, due diligence, and communications with all parties.

4 Increased Technology Risks

Technological capabilities are growing faster than organizations can digest, interpret, assess, and control access to sensitive data. Using technology, criminals are able to respond and exploit vulnerabilities faster than organizations can protect and restrict access. Today's bank robbers come armed with technology instead of guns. They work behind the scenes and can be located anywhere in the world. Their attempts to inappropriately access a financial institution's sensitive data can be carried out electronically non-stop, twenty-four hours a day. As a result, internal auditors in the financial sector have much higher levels of activity for IT risks than other industry types (see **exhibit 6**).

Exhibit 6 Internal Audit Activity for General IT Risks



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: General information technology (IT) risks. *n* = 9,747.

> *Internal audit's competency in data analytics and performing proactive continuous monitoring is on the increase, and this is an area to consider in capacity planning.*
>
> —Jenitha John, CAE, FirstRand, South Africa

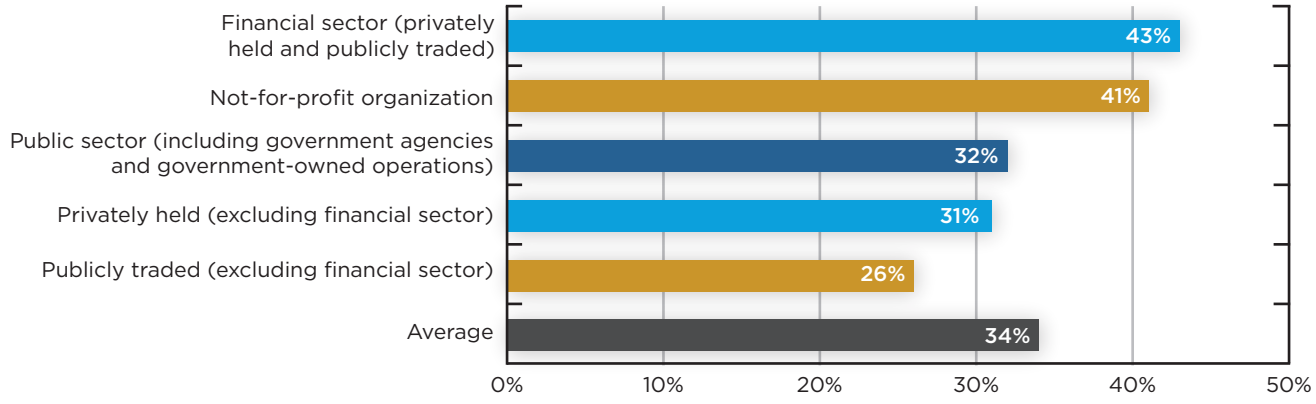
The Far-Reaching Impact of Cybersecurity Risks

Cybersecurity, advanced persistent threats, and privacy have become some of the hottest topics on internal auditors' risk radars. As noted in **exhibit 1** and **exhibit 2**, information technology (IT) risks rank fourth in both the top risks CAEs identified and the percentage of time devoted to audit these risks. And it is not just internal auditors who are focusing on these topics. We can add senior management, boards of directors, regulators, and investors to the list of those expressing concern over these risks. Due to heavily publicized data breaches, everyone is well aware of the reputation risk and negative impact that these breaches can generate. Recovery efforts can be costly, extremely time-consuming, and result in major organizational shake-ups. Many say that it is not "if you are breached" but "when you are breached," and that plans for remediation should be well developed and tested before a breach occurs. Financial sector internal auditors see the risk of a data breach as more extensive than those in other sectors: 43% describe the risk as extensive, compared to an average of 34% (see **exhibit 7**).

Preparedness and Recovery Activities

Business continuity, resumption, and recovery have become equally or more important than attempts to restrict or prevent data breaches. Broader, more holistic data and privacy controls and programs that cover the entire spectrum—from preparation, detection and analysis, containment, eradication and recovery to post incident activity—are necessary. Internal auditors' active involvement in testing preparedness plans can yield big dividends when the inevitable event happens. Preparedness testing has evolved from internal resources and a few vendors to include organizations such as the Financial Services Information Sharing and Analysis Center (FS-ISAC), a global financial service industry resource for cyber and physical threat intelligence analysis and sharing.

Exhibit 7 Risk of Data Breach Described as "Extensive"



Note: Q93: In your opinion, what is the level of inherent risk at your organization for the following emerging information technology (IT) areas? Topic: Data breaches that can damage organization's brand. *n* = 9,426.

Adding Big Data Risks to Audit Plans

Big data is creating challenges for organizations in how they store, manage, protect, and use this vast and ever-increasing resource. In 2013, it was reported that a full 90% of all the data in the world had been generated over the previous two years (ScienceDaily.com, May 22, 2013). Risk data aggregation and information governance are topics for internal auditors to consider when developing their risk-based audit plans.

Connectedness and Mobile Devices

New technologies are creating unique challenges for organizations and internal audit groups. Controlling access is no longer limited to locking down the workstation. The Internet, social media, mobile devices, remote access, and other devices or methods have opened many more entry points to control. Users throughout the organization are often able to introduce unapproved software without going through normal control channels. Coordinating new technology with legacy systems used by many financial institutions can present additional challenges in monitoring and controlling financial institution information.

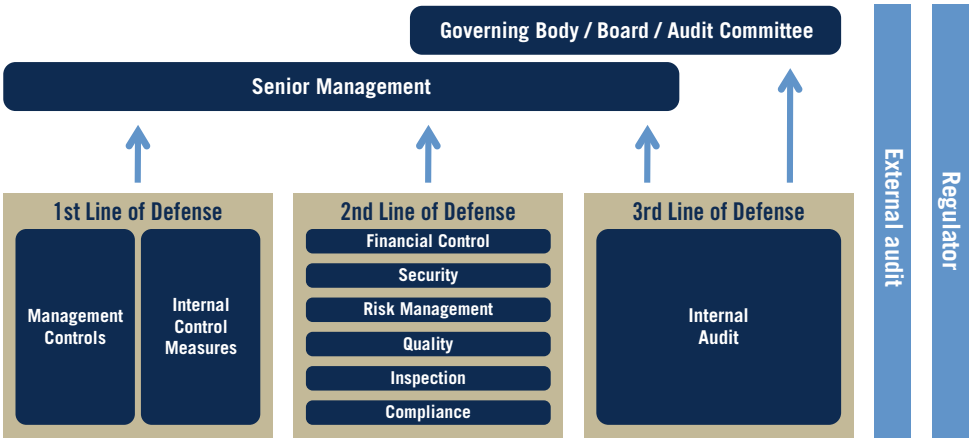
These technology challenges pose a number of issues for internal audit departments in the financial sector. Having the internal expertise on staff to address ever-changing technology risks is expensive and difficult to accomplish due to the limited number of experts in this area. Worldwide, only 10% of survey respondents say they have an information systems auditing certification, and only 3% have a certification for IT security (Q13, n = 12,540). Relying on consultants to perform technology audits can also be expensive and requires additional oversight and management. Due to the velocity of technological change, the technology risk profile of the institution is continually changing and morphing, requiring internal audit departments to audit a moving target.

5 Three Lines of Defense

The Three Lines of Defense Model (see **exhibit 8**) has gained popularity and widespread usage among internal auditors around the world. According to survey respondents, 78% of those in the financial sector worldwide say they follow the Three Lines of Defense Model, with internal audit as the third line of defense (see **exhibit 9** on the following page). This is a much higher percentage than other organization types. While the model is becoming more popular, understood, and accepted, questions about how flexible it should be have arisen. All three lines of defense should exist in some form at every financial institution, regardless of size or complexity. Risk management normally is strongest when there are three separate and clearly identified lines of defense. In practice, particularly at some small and mid-sized institutions, a blended approach has been implemented. For example, some institutions have consolidated or combined some second lines of defense with internal audit.

Internal auditors may be asked or assigned responsibility to provide compliance audits when a separate compliance department does not exist, execute loan reviews without a separate loan review department, coordinate enterprise risk management (ERM) activities, or handle physical and/or IT security. Some CAEs are looking for answers on how to appropriately and effectively implement the Three Lines of Defense Model.

Exhibit 8 The Three Lines of Defense Model



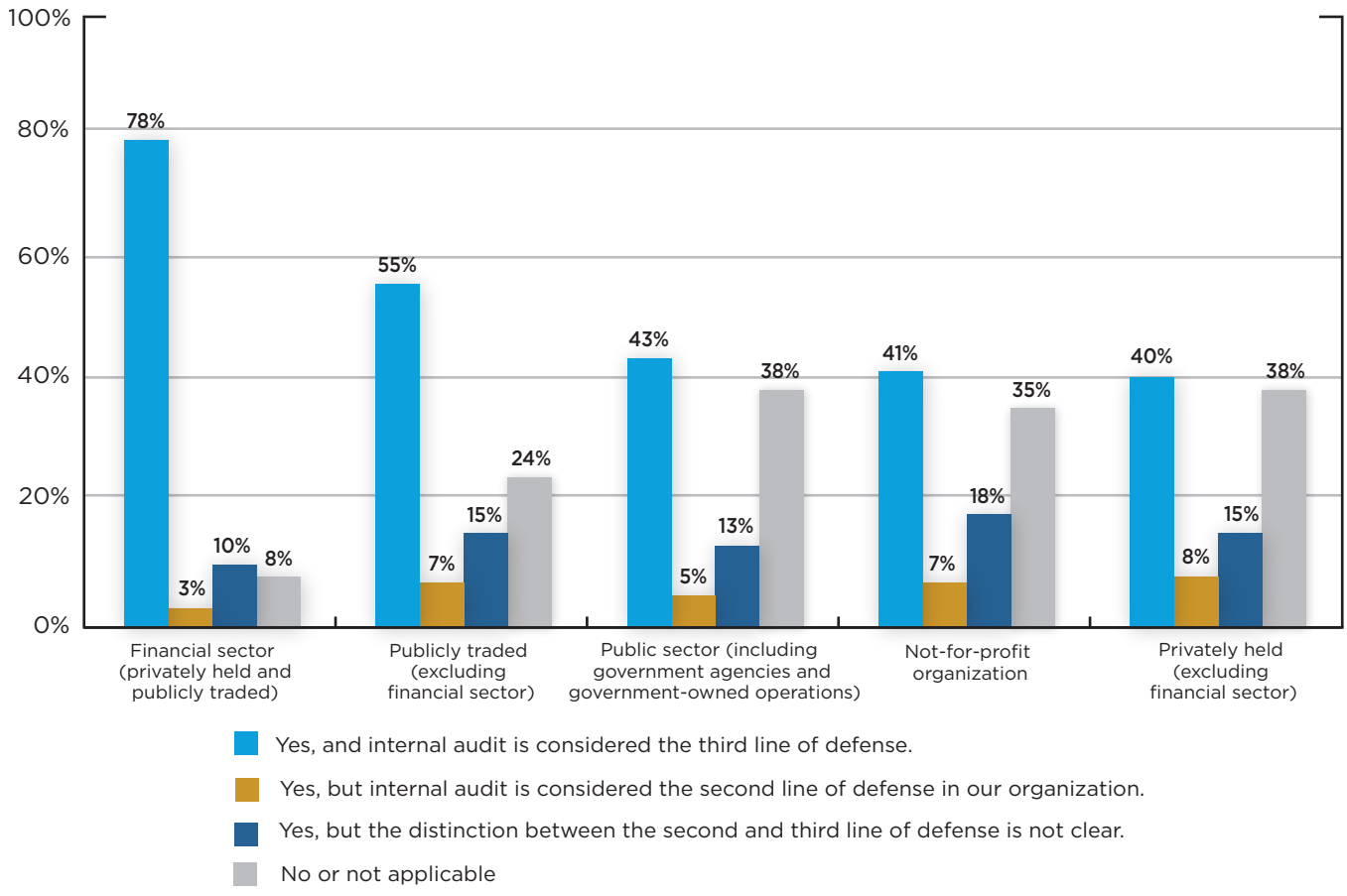
Note: Adapted from ECIIA/FERMA Guidance on the 8th EU Company Law Directive, article 41, as shown in The IIA's Position Paper, The Three Lines of Defense in Effective Risk Management and Control, January 2013.

Safeguards for a Blended Three Lines of Defense

It is important for internal audit to be able to perform its duties with objectivity and not be unduly influenced by managers of day-to-day operations. Some organizations may have all internal assurance groups, including internal audit and some portions of the second line of defense, administratively report to a single executive. A blended administrative reporting relationship should be designed so as to not interfere with the CAE's functional reporting directly to the institution's audit committee.

It is important to ensure internal audit functionally reports directly to the audit committee when different elements of the three lines of defense report administratively to the same executive. Additional safeguards can also be established to help maintain internal audit's independence and objectivity; quality assessments of internal audit; third-party reviews of compliance, loan review, security, and ERM; providing

Exhibit 9 Usage of the Three Lines of Defense Model



Note: Q63: Does your organization follow the three lines of defense model as articulated by The IIA? Those who responded "I am not familiar with this model" were excluded from these calculations. Due to rounding, some totals may not equal 100%. *n* = 9,093.

access to board committees for managers assigned to compliance, loan review, and security, etc.

Ensuring that these groups do not have operational or management decision-making responsibilities with proper disclosure and transparency in the internal audit charter, reports, and other communications can support independence and objectivity in a blended administrative reporting relationship under the Three Lines of Defense Model. In the highly regulated financial services industry, regulatory examinations that review these blended reporting arrangements, and the safeguards in place to foster independence and objectivity, can be used to help validate the appropriateness of the structure.

Having an executive to whom all internal assurance groups report directly can also act as a safeguard that may strengthen independence and objectivity for all these groups. This approach can foster greater communication and coordination among multiple assurance groups so information can be leveraged and duplicate work minimized, resulting in more efficient and effective programs.

The IIA's Position Paper, The Three Lines of Defense in Effective Risk Management and Control, acknowledges that, "Because every organization is unique and specific situations vary, there is no one 'right' way to coordinate the Three Lines of Defense." The paper also states, "...in exceptional situations that develop, especially in small organizations, certain lines of defense may be combined. In these situations, internal audit should communicate clearly to the governing body and senior management the impact of the combination. If dual responsibilities are assigned to a single person or department, it would be appropriate to consider separating the responsibility for these functions at a later time to establish the three lines."

CAEs should ensure that information is shared and activities are coordinated for effective management of each organization's risks and controls. Development of formal policies and procedures can assist in this effort.

6 Internal Audit Resources

> *"In light of financial services audit functions' need to evolve their focus from financial risks to more operational risks, the backgrounds of those we are recruiting are also evolving. We now seek candidates with college majors such as finance, organizational strategy, statistics, and supply chain management."*
>
> —Mark Howard, Senior Vice President and CAE, USAA, San Antonio, Texas

Expectations of management, board members, and regulators for internal auditors have increased beyond the typical accounting and financial knowledge that was traditionally the hallmark for all internal auditors. Now they are expected to have knowledge related to technology, business operations, financial services, communications, regulatory compliance, cybersecurity, privacy, vendor management, business continuity, legal matters, quantitative analysis, and so forth. In most organizations, it is not possible to simply keep hiring more people to acquire these skills. According to CAE survey respondents, the financial services industry has different skill priorities than other industries, with more emphasis on industry-specific knowledge, finance, risk management, and IT (see **exhibit 10**). Interestingly, there is less emphasis on accounting skills. Individual auditor skill

Exhibit 10 Top Skills Financial Sector CAEs Seek for Staff

Skill	Financial Sector	Nonfinancial Sectors	Gap
Analytical/critical thinking	66%	64%	2%
Communication skills	52%	51%	1%
Risk management assurance	48%	41%	7%
Industry-specific knowledge	45%	33%	12%
Information technology (general)	43%	37%	6%
Accounting	36%	45%	-9%
Data mining and analytics	32%	31%	1%
Finance	30%	21%	9%
Business acumen	26%	27%	-1%
Fraud auditing	21%	23%	-2%
Cybersecurity and privacy	16%	13%	3%
Forensics and investigations	13%	15%	-2%
Legal knowledge	10%	12%	-2%
Quality controls (Six Sigma; ISO)	4%	8%	-4%
Other	3%	4%	-1%

Note: Q30: What skills are you recruiting or building the most in your internal audit department? (Choose up to five.) CAEs only. *n* = 3,288.

sets must be developed so that multi-talented auditors can be used to audit diverse disciplines.

Developing internal auditors with these new skill sets is not without its challenges. For example, it was reported at The IIA's 2015 General Audit Management Conference that unemployment numbers for auditors and accountants in North America are at all-time lows and fewer students are electing degrees in accounting. CAEs are expanding recruiting searches and considering educational backgrounds other than traditional accounting.

Generational differences are reshaping work environments and creating challenges with traditional compensation and management approaches. Work and life balance considerations rate higher for benefit considerations for younger generations. Flexible work schedules and more generous leave time are becoming more common. Fortunately, technology has allowed for more work-from-home opportunities for audit staffs.

Technology skills are now mandatory for any auditor entering the workforce. Technology is also an area where organizations frequently need to obtain outside or third-party resources to supplement staff resources. New systems or software tools may also be needed to supplement internal audit resources. Increased budgets and training may be needed to effectively implement expanded technology audits.

Rotational CAEs who serve as the head of internal audit for a limited time, while expanding audit approaches and methods, are also creating challenges such as continuity in audit approaches, independence issues, and even whether rotational CAEs understand or even care about IIA *Standards*, quality assessments, etc. Commitments for internal audit training and certifications could be lacking. Organizational developments can affect timing and opportunities for favorable exits or rotation back to operating units for rotational CAEs. However, a number of benefits can be derived from rotational CAE engagements, such as proven leadership with an existing seat at the table, expanded business insights, and existing business relationships that can be leveraged to add value and increase confidence in the audit function.

Conclusion

There will always be challenges for internal auditors in the financial services industry. While the challenges may be grouped in common categories with similar themes over the years, there will always be unique twists to test the creativity and ingenuity of those tasked with addressing the challenges. The environment will continue to change and present new opportunities to develop innovative strategies to address the challenges.

Internal auditors who step up and effectively address the challenges they face can demonstrate their positive contributions to the organizations they serve. They will be recognized as effective leaders and, in turn, continue to elevate their stature and reputation in the workplace. Along with this recognition, they are likely to get additional challenges as their role in the organization continues to grow in importance. The most successful internal auditors will learn from the lessons of the past and continue to strive for improvement through innovative techniques and practices, professionalism, continual development, and dedication to the profession of internal auditing.

About the Authors

Jennifer F. Burke, CPA, CRP, CFF, CFS, is a partner in Crowe Horwath's Financial Services Risk practice and has more than 25 years of experience serving financial services clients, including 19 years with Crowe. She leads projects at strategic multi-billion-dollar financial institutions, providing internal audit, compliance, loan review, and enterprise risk management (ERM) services. She serves on The IIA's Financial Services Advisory Board and the North Carolina State ERM Initiative Advisory Board. She is a nationally and internationally recognized speaker on banking issues, internal auditing, and ERM. Before joining Crowe, she served as senior vice president and CAE for a multibillion-dollar, 10-bank holding and trust company.

Steven E. Jameson, CIA, CFSA, CRMA, CPA, CFE, is executive vice president, chief internal audit and risk officer for Community Trust Bank where he is responsible for the internal audit, ERM, loan review, compliance, and security functions. He has more than 28 years of experience as an internal audit professional in the financial services industry, three years in public accounting, and four-plus years with The IIA as assistant vice president, Professional Practices Group. He served on the Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) steering committees for the development of *Internal Control – Integrated Framework* (2012) and *Enterprise Risk Management – Integrated Framework* (2004).

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

Contact Us

The Institute of Internal Auditors Global Headquarters

247 Maitland Avenue

Altamonte Springs, Florida 32701-4201, USA

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.

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

James Alexander (United States)
Despoina Chatzaga (Greece)
Kıvılcım Günbattı (Turkey)
Cassian Jay (United States)
Jenitha John (South Africa)
Michael Parkinson (Australia)
Deborah Poulalion (United States)
Nicola Rimmer (United Kingdom)

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.