



REUTERS/Erik de Castro

# STATE OF INTERNAL AUDIT SURVEY 2014 – ADAPTING TO COMPLEX CHALLENGES?

Michael Cowan, Helen Camfield, Stacey English and Susannah Hammond





# TABLE OF CONTENTS

- 4 EXECUTIVE SUMMARY
- 5 INTRODUCTION
- 5 THE FINDINGS
- 11 KEY RISKS FOR INTERNAL AUDIT FUNCTIONS
  - 12 CORPORATE GOVERNANCE
  - 13 CULTURE/CONDUCT RISK
  - 15 INCREASED PERSONAL LIABILITY
  - 17 RESOURCE RISK
  - 19 UNDERTAKE A SKILLS AUDIT
  - 20 FUTURE REGULATORY DEVELOPMENTS
  - 21 IT RISKS
- 22 ADAPTING TO COMPLEX CHALLENGES: IS CHANGE HAPPENING AT THE RIGHT PACE?
- 23 NEXT STEPS FOR INTERNAL AUDIT



## EXECUTIVE SUMMARY

---

Thomson Reuters Accelus' annual State of Internal Audit Survey provides an insight into the experiences and expectations of internal audit professionals around the world. More than 900 internal audit practitioners across 50 countries participated in the 2014 survey sharing their views across a range of subjects, issues and concerns. The experiences shared in this report are intended to help internal audit functions and senior management benchmark the myriad of challenges faced and enable them to leverage the approach taken by their peers.

The survey has demonstrated that the world and work of internal audit continues to be as complex, and challenging as ever. Both the volume and diversity of issues that internal auditors need to understand and assess continues to increase globally and across all industries.

In fact, at a high level the results of the Thomson Reuters Accelus State of Internal Audit Survey have remained relatively unchanged for the last few years.

This year the results confirmed that the vast majority (81 percent) of internal auditors' focus remains on providing assurance on the efficacy of internal control process. While assurance work is the traditional mainstay of internal audit there are a wide range of other areas and issues for internal auditors to consider, including:

- Nearly a quarter (24 percent) of internal auditors expect their personal liability to increase in 2014. The adequacy of internal auditors' skills, focus and approach is firmly on the radar of regulators worldwide. It is no surprise, therefore, that internal auditors expect their own personal liability to increase in the near future.
- Nearly half (49 percent) of all internal auditors have had no involvement in assessing their firm's culture. There are distinct regional variations with respondents from South America reporting that three-quarters (77 percent) of internal auditors have not assessed the culture of their firm.
- Just over a quarter (27 percent) of internal auditors have had no involvement in assessing their firm's corporate governance;

regionally this figure looks most concerning for North America, with 32 percent of internal auditors having no involvement.

- Internal auditors spend 45 percent of their time on IT security and risk. Nearly half (48 percent) of respondents said that it should be a top priority for their organization and 35 percent said it would be a top challenge for boards of directors in 2014.
- Nearly half of the respondents (48 percent) expect to be spending more time reporting to senior management and tracking remedial actions. This is in addition to almost a quarter (24 percent) of internal auditors anticipating a need to focus on the implementation of industry-specific legislation.
- Nearly half of internal auditors interact with risk management (44 percent) and compliance (47 percent) on at least a monthly basis. While these figures are a slight improvement on last year it remains an area where improvements could be made.
- It is interesting that areas not considered a priority for internal audit included customer outcomes (6 percent), whistle-blowing (5 percent) and capital and liquidity (4 percent).
- Internal auditors' perception of priorities for the board are not aligned with their own. The key challenges for internal auditors are greater complexity of issues and focus on risk and control, as well as changing business models. In contrast, boards' priorities are corporate strategy, strategic risk management and legal and regulatory risk.

The growing focus which policymakers and regulators have been placing on culture, corporate governance and risk management has emphasized still further the need for a strong, well-resourced independent audit function operating, and in particular reporting, in close coordination with other risk and compliance functions, all with visible support from the top of the organization. Yet the results show a relatively unchanged picture in these areas from previous years. As the risks increase so does the need for internal audit to react to those changes.

# INTRODUCTION

*“Unfortunately, over the decades, we’ve seen multiple cycles in which company management and internal and external auditors simply didn’t get it right in the area of internal control, resulting in failures to effectively define, understand, implement and assess internal control.”*

**Jeanette M Franzel, board member, U.S. Public Company Accounting Oversight Board, March 26, 2014**

but their views are crucial in helping peers benchmark their own firms’ practices and experiences and assess whether their resources, focus and expectations are in line with those in the wider industry.

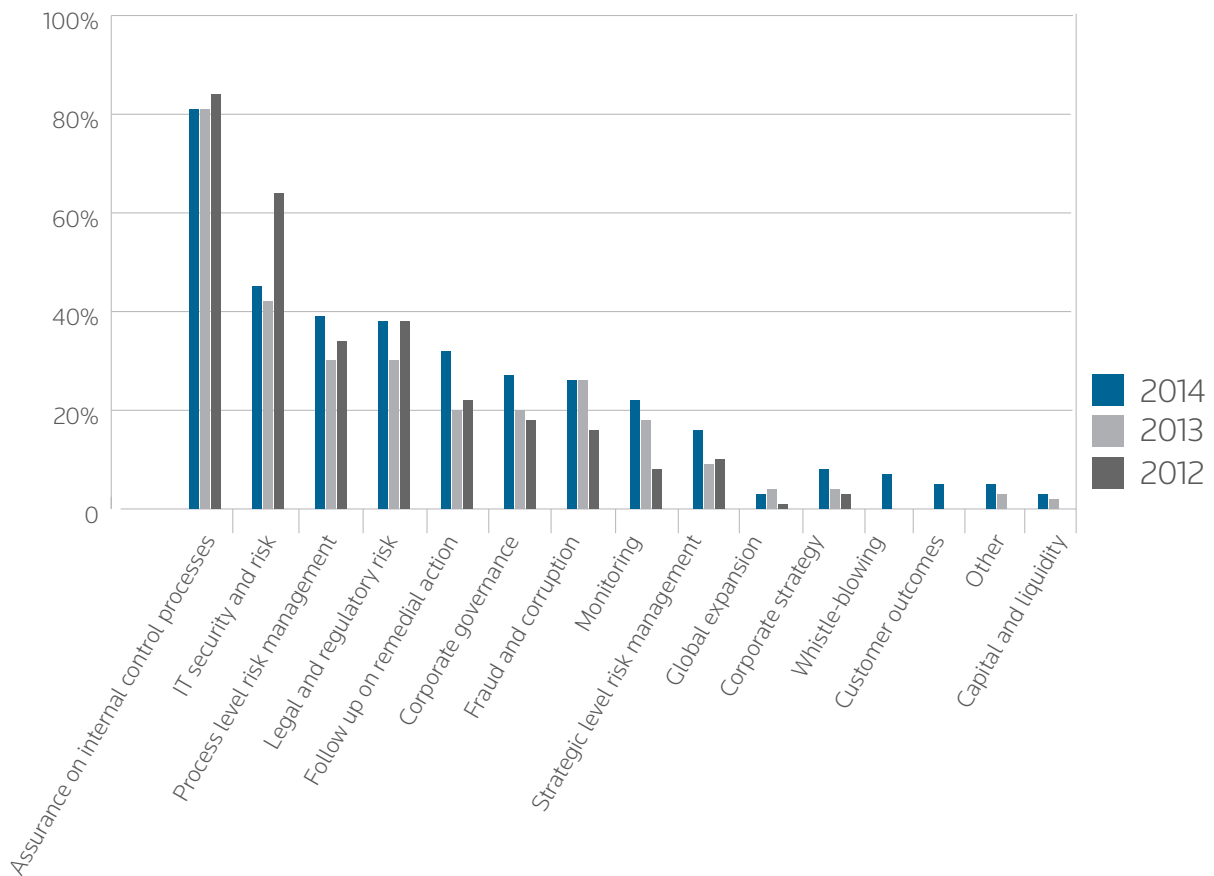
The responses received covered 50 countries worldwide including those from Europe, the Americas, Australasia, Asia, Africa and the Middle East. They represent firms from industries such as financial services, manufacturing, government, education, life sciences, energy and other highly regulated industries. Feedback came from internal audit departments of all sizes, ranging from those whose departments comprised fewer than five auditors to global conglomerates with departments exceeding 100 auditors.

The report is intended to help internal auditors with future planning, resourcing and focus and has been driven by the high level of industry participation. Participants remain anonymous

# THE FINDINGS

The annual State of Internal Audit survey provides readers with a broad view of how the world of internal audit has developed and changed over the past year.

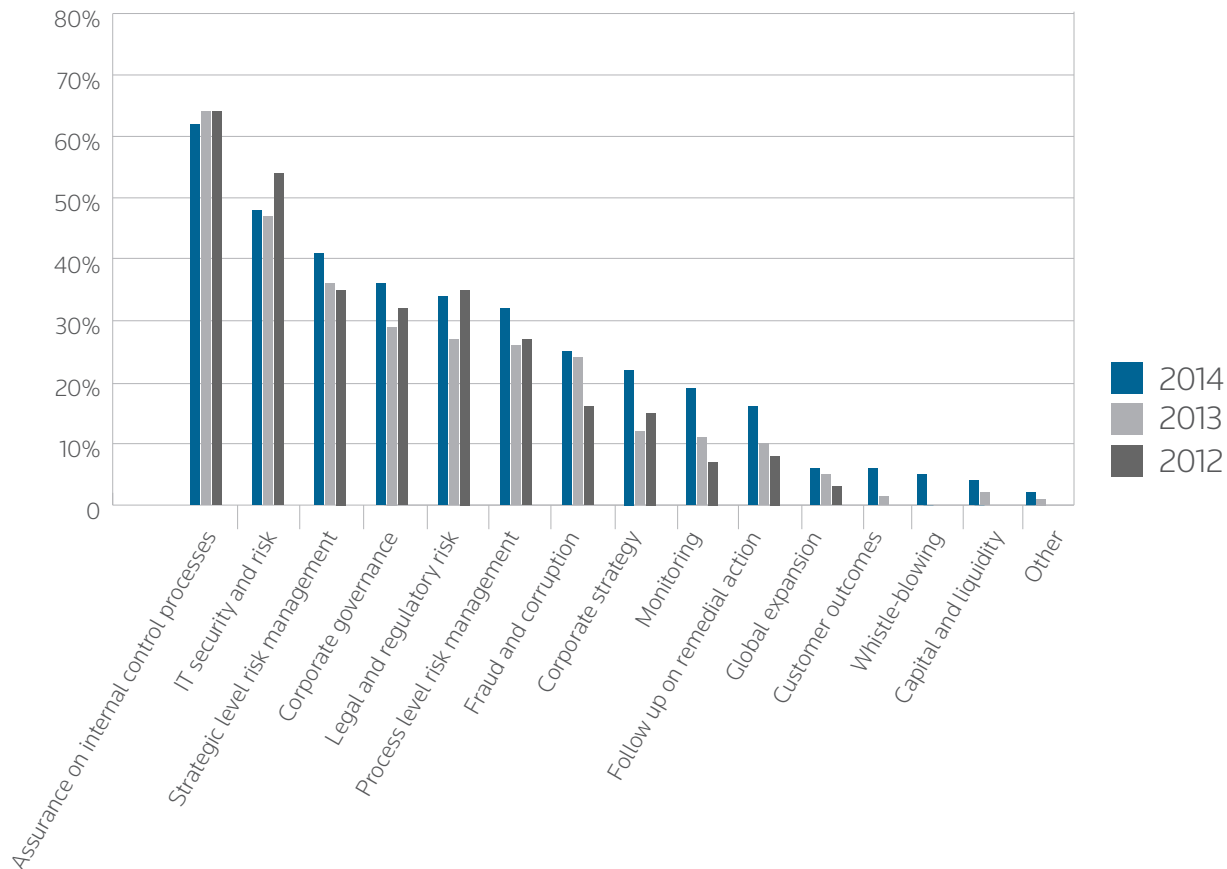
## IN YOUR ORGANIZATION CURRENTLY, WHAT ARES INTERNAL AUDIT’S TIME AND RESOURCES PRIMARILY APPLIED TO?



This year, as in previous years, respondents unsurprisingly highlighted assurance on internal control processes as the area to which internal audit's time and resources were primarily applied. Overall, 81 percent of respondents listed assurance as a top-three activity. IT security and risk were ranked second in the list of priorities by 45 percent of respondents. Similar to previous years, process-level risk management (39 percent) and legal and regulatory risk (38 percent) featured prominently. There has been an increase in focus on other areas such as corporate

governance: 27 percent of respondents selected it this year, growing from 20 percent in 2013 and 18 percent in 2012. That said, just over a quarter (27 percent) of internal auditors have had no involvement in assessing their firm's corporate governance. Good corporate governance is vital for effective compliance and risk management within firms and it sends a clear message that, in line with regulatory expectations, it is growing as an area of focus for internal audit.

### IN YOUR OPINION, WHAT SHOULD BE THE TOP PRIORITIES FOR YOUR ORGANIZATION'S INTERNAL AUDIT FUNCTION?



As well as asking internal auditors to name the top three areas where they primarily focused their time and resources, the survey also asked about what they thought these priorities should be. The gaps between what internal auditors were doing and what they thought they should be doing varied by both region and issue, but there were some clear trends. In three of the seven global regions, for example, the biggest disconnect was in relation to corporate governance.

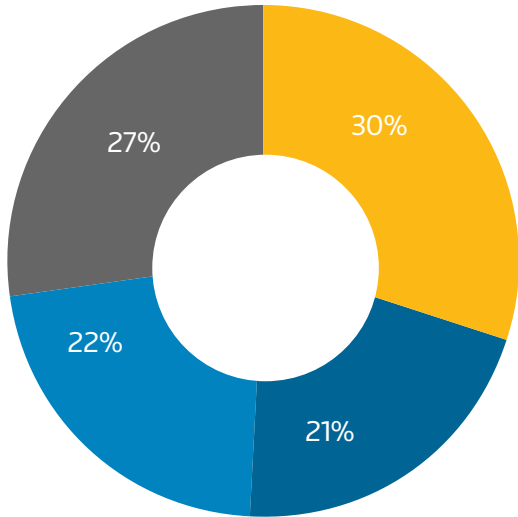
Assurance over internal control processes and IT security and risk are consistently viewed as top priorities both for what internal audit is focusing on and what it should be focusing on, and yet survey responses demonstrated some divergence between the actual focus for 2014 and what auditors believed should be their focus for the year ahead. Strategic level risk management

remained the third priority at 41 percent, an increase from 36 percent in 2013, and corporate governance was fourth at 36 percent, an increase from 29 percent in 2013.

While internal audit's top priorities from a regional perspective largely correlate with the overall picture — assurance remains the top priority — there are some distinct regional variances. Internal audit functions in Australasia, Europe and North America all considered that they should be spending more time focusing on IT and security risks associated with their firm. In Africa, Asia and South America, meanwhile, the primary areas of disconnect related to corporate governance, with internal auditors in these regions considering this an area in need of more attention. In contrast, internal auditors in the Middle East thought they should be spending more time on fraud and corruption risks.

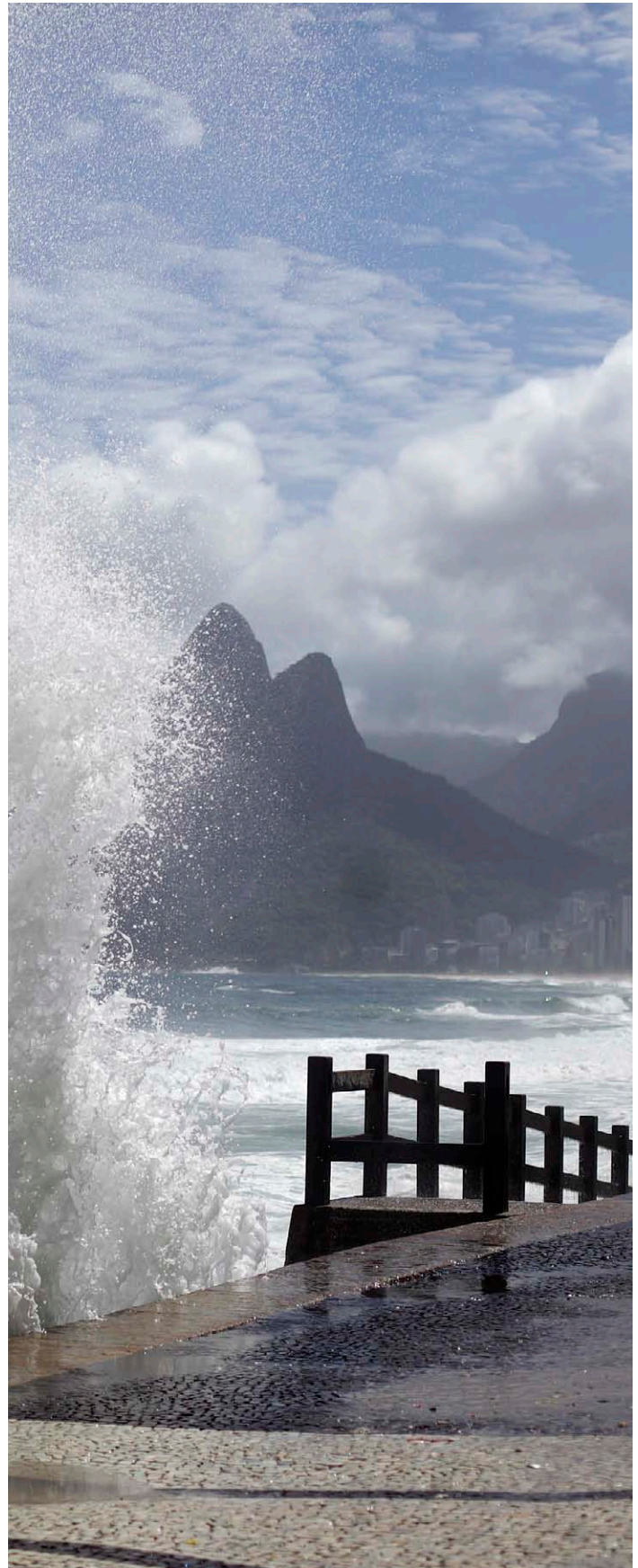
While the top priorities are in line with previous years, it is worth highlighting that corporate strategy has seen a 10 percent jump from 2013 to 22 percent this year. Areas that perhaps should be more of a priority for internal audit are customer outcomes (6 percent), whistle-blowing (5 percent) and capital and liquidity (4 percent).

**TO DATE, WHAT INVOLVEMENT HAVE YOU HAD IN ASSESSING YOUR FIRM'S CORPORATE GOVERNANCE?**

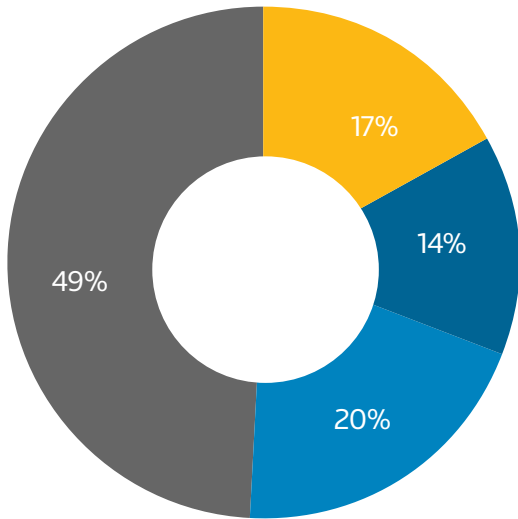


- Effectiveness is reviewed as part of monitoring program
- Have been consulted on design and effectiveness
- Have highlighted it as a key risk to be assessed
- No involvement

Corporate governance and culture have moved into the mainstream as a result of the financial crisis and now as the global recovery takes hold governments, regulators and firms are all keen to ensure the appropriate lessons are learned. It is clear, however, that despite the increasing profile of corporate governance with regulators, shareholders and customers, and the effect it has on the health and reputation of firms, it is still an area in which many internal auditors lack a high level of involvement. Just over a quarter of internal auditors have had no involvement in assessing their firm's corporate governance; regionally, this figure was most concerning for North America, with 32 percent of internal auditors having no involvement in assessing corporate governance. This figure dropped to 18 percent for European respondents.



**TO DATE, WHAT INVOLVEMENT HAVE YOU HAD IN ASSESSING YOUR FIRM'S CULTURE?**



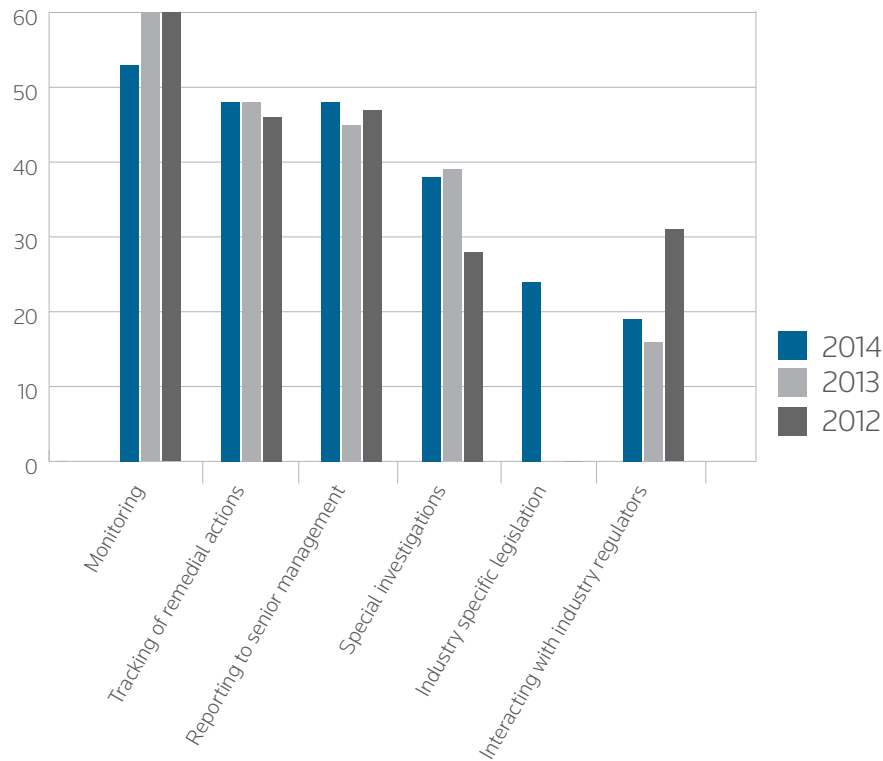
- Effectiveness is reviewed as part of monitoring program
- Have been consulted on design and effectiveness
- Have highlighted it as a key risk to be assessed
- No involvement

Culture is a vital regulatory priority around the world and the embedding of what is seen as a good culture has become the new normal. It is therefore worrying that nearly half of all internal auditors have had no involvement in assessing their firm's culture. This figure is of most concern in South America where three-quarters of internal auditors have reported no involvement in assessing their firm's culture. The financial services industry appears to be leading the way in driving the enhanced focus on culture as a means of improving corporate behavior. The UK Financial Conduct Authority has not specifically defined culture but has said that it will assess it by looking at areas of a firm's business and behavior and drawing conclusions there from. The FCA's approach can usefully be applied to all business sectors and seeks to use a range of different measures such as:

- how a firm responds to, and deals with, regulatory issues;
- what customers are actually experiencing when they buy a product or service from front-line staff;
- how a firm runs its product approval process and what factors it takes into account;
- the manner in which decisions are made or escalated;
- the behavior of a firm in certain markets;
- remuneration structures.

There has been a high-profile focus on culture in the UK and Europe but even so 49 percent of internal auditors have not assessed their firm's culture. In Asia, Australasia and North America, this figure is higher, with more than half of respondents reporting no involvement.

**WHICH OF THE FOLLOWING AREAS ARE YOU EXPECTING TO SPEND MORE TIME ON IN THE COMING YEAR?**





In line with findings from previous internal audit surveys, more than half of the respondents expected to be spending more time on monitoring in the coming year. This is slightly down from previous years (60 percent). Nearly half of the respondents expected to be spending more time reporting to senior managers and tracking remedial actions. A key feature of this year's responses is that almost a quarter of internal auditors anticipated having to focus on the implementation of industry-specific legislation, which does not fit well with the finding that internal auditors reported a distinct fall over the last two years in the time spent interacting with regulators. This could perhaps be attributed to the fallout from the financial crisis when all firms, regardless of sector, were placed under intense regulatory

scrutiny. The successful implementation of regulatory change relies however on building and maintaining strong working relationships with all relevant regulators.

As an example, in the financial services sector, last year saw a 43 percent increase in the volume of regulatory alerts published globally. This heightened level of regulation is placing an enormous strain on already stretched resources within many control functions.

It is another cause of potential stretch for internal auditors that in Australasia (72 percent), Asia (49 percent) and Europe (48 percent) they also expect to be spending more time reporting to senior managers alongside their monitoring duties.

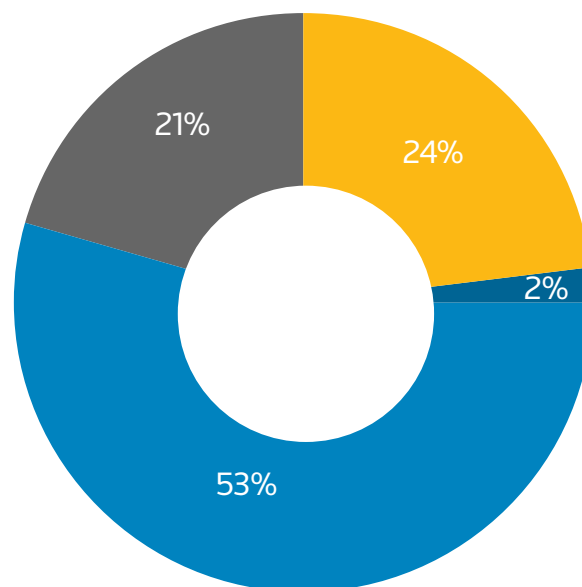
**ON AVERAGE, HOW OFTEN DO YOU INTERACT WITH THE FOLLOWING ASSURANCE GROUPS?**

On average, how often do you interact with the following assurance groups?									
	Risk Management			Compliance			Legal		
	2012	2013	2014	2012	2013	2014	2012	2013	2014
Weekly	32%	18%	22%	32%	25%	25%	13%	15%	14%
Monthly	24%	19%	22%	27%	18%	22%	22%	19%	24%
Quarterly	14%	15%	14%	14%	10%	11%	16%	13%	12%
Annually	3%	5%	4%	3%	4%	2%	3%	4%	2%
Ad hoc	22%	29%	28%	19%	25%	27%	37%	40%	41%
Not sure	5%	14%	10%	6%	18%	13%	8%	9%	7%

As in previous surveys, respondents have indicated that significant interaction is undertaken on an ad hoc basis with other assurance groups. As a matter of good practice consideration should be given to formalizing these meetings to help to ensure that nothing is missed or overlooked. This year, internal auditors have signaled a slightly improved level of interaction, with nearly half interacting with risk management (44 percent) and compliance (47 percent) on at least a monthly basis. Interaction with legal is slightly lower than risk and compliance (38 percent) but it is still an improvement on previous years. This is positive but there is still room for improvement, with around a quarter of internal auditors either meeting on a quarterly or annual basis with other assurance groups or more worryingly not being sure when they are meeting at all.

Although internal audit must retain its independence it does need to be closely aligned with the compliance, risk and other control functions. The current, and increasingly complex, operational environments, as well as the greater focus on the quality of risk management information, will mean that the most effective firms will be those that have audit, risk, legal and compliance functions which have aligned work programs, share risk issues and communicate internally and externally on a consistent basis.

**IS YOUR JOB-RELATED PERSONAL LIABILITY LIKELY TO CHANGE IN 2014?**



- Increase
- Decrease
- No change
- Don't know

As part of the remedial regulatory reforms implemented following the financial crisis there is a greater focus on ensuring that senior individuals in financial services firms can be held accountable personally for wrongdoing. Although not all industry sectors have adopted this level of culpability, it is clear that internal auditors are aware of the trend, with nearly a quarter of them expecting their personal liability to increase this year.

# KEY RISKS FOR INTERNAL AUDIT FUNCTIONS

## BOARD OF DIRECTORS' TOP CHALLENGES



## KEY CHALLENGES FOR THE YEAR AHEAD



Although this year's survey results showed limited change from those of the 2013 survey, in general, those changes indicate that the "direction of travel" for internal audit functions is correct although more change may be needed to address all the risks fully. In addition, the word clouds above demonstrate that there are some differences between the priorities internal auditors perceive for themselves for the coming year and those they anticipate for the boards of their organizations. From the board's perspective, internal auditors predicted that corporate strategy, strategic-level risk management and legal and regulatory issues

would be the top priorities for the year ahead. Underpinning all these areas is corporate governance, and some of the risks and controls surrounding corporate governance are explored below.

For internal auditors themselves the top three areas came out as complexity of issues, increased focus on risk and control and changing business model issues. Some of the risks and controls associated with these areas are explained further below, and the resource issues raised in the survey, e.g. cost, availability and management support, are also examined.

## CORPORATE GOVERNANCE

The survey showed just over a quarter of internal auditors have had no involvement in assessing their firm's corporate governance. In the UK, listed companies are required to comply with the UK Corporate Governance Code which is administered by the Financial Reporting Council. In April 2014 the FRC issued a consultation to make changes to the code; these changes included:

- greater emphasis be placed on ensuring that remuneration policies are designed with the long-term success of the company in mind, and that the lead responsibility for doing so rests with the remuneration committee;
- companies should put in place arrangements that will enable them to recover or withhold variable pay when appropriate to do so, and should consider appropriate vesting and holding periods for deferred remuneration;
- companies should explain when publishing annual general meeting results how they intend to engage with shareholders when a significant percentage of them have voted against any resolution;
- companies should state in their financial statements whether they consider it appropriate to adopt the going concern basis of accounting and identify any material uncertainties to their ability to continue to do so;
- companies should carefully assess their principal risks and explain how they are being managed and mitigated;
- companies should state whether they believe they will be able to continue in operation and meet their liabilities, taking account of their current position and principal risks, and specify the period covered by this statement and why they consider it appropriate. It is expected that the period assessed will be significantly longer than 12 months; and
- companies should monitor their risk management and internal control systems and, at least annually, carry out a review of their effectiveness, and report on that review in the annual report.

This consultation follows previous consultations during 2013 on directors' remuneration (October 2013) and risk management, internal control and the going concern basis of accounting (November 2013). In the light of this it may be helpful to explore some of the significant elements of corporate governance from an internal audit angle:

- **Board composition and effectiveness** The code states: "Every company should be headed by an effective board which is collectively responsible for the long-term success of the company." In brief, internal audit needs to provide assurance that: the board is made up of the appropriate mix of executive and non-executive directors; the board meets regularly; relevant sub-committees (e.g., audit and risk committees) are in place; there is appropriate delegation and apportionment of responsibilities; appropriate records (e.g., minutes of meetings) are kept and retained; there is a rigorous formal process for appointing members to the board; training for board members is in place and appropriate; and regular (annual in the UK) assessments of the performance of the board are undertaken.

- **Risk management** The code states: "The board is responsible for determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives. The board should maintain sound risk management and internal control systems." For internal auditors this means ensuring that: the internal audit function has a reporting line into the audit committee; the three lines of defense model to control risks throughout the organization is operating effectively, e.g., appropriate controls and monitoring are in place in the first line and that second-line risk functions are undertaking their roles effectively; and the scope, completeness and accuracy of reports to the board is sufficient for them to carry out their responsibilities.

An important factor here is the relationship internal audit has with other control functions. The survey showed that internal audit is still spending relatively little time interacting with other assurance groups. In fact this supports a study undertaken by the London School of Economics published in September 2013 which suggested that there were tensions between the first and second line and that these tensions should be managed through awareness rather than potentially entrenched positions that the model may lead to. This may also be true for the second and third lines where, to be effective, a collaborative, two-way interface needs to be maintained, but the formality of the three lines of defense model requires a level of independence behind which, perhaps, both sides hide. Internal audit needs to find a way to interact effectively with other control functions while maintaining its organizational independence.

- **Directors' remuneration** The code states: "Levels of remuneration should be sufficient to attract, retain and motivate directors of the quality required to run the company successfully, but a company should avoid paying more than is necessary for this purpose. A significant proportion of executive directors' remuneration should be structured so as to link rewards to corporate and individual performance." Internal auditors need to ensure that: appropriate remuneration committees are in place and formalized processes and procedures operate around them; formal remuneration policies are in place and monitored throughout the wider organization; and remuneration structures are free from conflicts of interest (see below).
- **Relations with shareholders** For listed companies the code states: "There should be a dialogue with shareholders based on the mutual understanding of objectives. The board as a whole has responsibility for ensuring that a satisfactory dialogue with shareholders takes place." Internal auditors should make sure that: communications are appropriate and have been through the necessary approval process; AGMs have been established and arrangements are satisfactory; and there are policies and processes to make the relevant disclosures in annual reports and on websites.

## CULTURE/CONDUCT RISK

Regulators, especially in the financial services industry, have stressed, and will continue to pursue, their culture and conduct reforms. At times what the regulators want is unclear but the survey results showed that internal audit functions are not being involved with this area, a significant risk that perhaps should be more closely analyzed.

It is entirely possible that internal audit functions do not have an audit or a series of audits that are badged “culture” or “conduct.” It may be that this area is covered by other pieces of work that are more indirectly associated with culture or conduct, but what are the individual areas that internal auditors may more readily recognize as the component parts of culture or conduct? Here are some examples:

- **Customer outcomes** The survey showed that while internal auditors (6 percent) and boards (11 percent) of organizations were showing an increase in customer outcomes as a priority for the organization, the percentages remained low. Customer outcomes are fundamental to an organization’s culture and conduct and getting them right goes a long way to minimizing an organization’s conduct risk.

It is important that internal auditors identify the areas where the organization is exposed to the greatest customer risk and provide assurance that effective controls are in place. Customer outcomes should be an essential part of an internal auditor’s risk assessment of an organization’s corporate governance, from the board setting the right tone from the top on customer outcomes to whether senior managers are receiving appropriate and adequate information on the delivery of customer outcomes. Internal audit needs to consider the controls throughout an organization’s approach.

Other operational areas that may present risks from a customer outcomes perspective include sales processes, complaints procedures, customer service areas or customer interfaces with IT systems. The Accelus Conduct Risk Survey 2013 found that organizations measured good customer outcomes in a number of ways. These included, the analysis of complaints, compliance monitoring and mystery shopping. Internal auditors may also wish to consider these areas when undertaking risk assessments.

- **Whistle-blowing** The presence of an appropriate, adequate and trusted whistle-blowing process can be seen as a positive attribute of a healthy culture and to this end both the whistle-blowing process and the outputs of specific whistle-blowing allegations should be seen by internal auditors as an important area where strong controls are needed.

The number of instances of whistle-blowing is growing. For example, the U.S. Securities and Exchange Commission reported that in Fiscal Year 2013, 3,238 whistle-blower

requests were received. By comparison, for Fiscal Year 2012, the Commission received 3,001. Since April 2013, the UK Financial Conduct Authority has seen a 38 percent rise in whistle-blowing reports. Reports averaged around 338 a month in the previous year, whereas the FCA has seen around 467 a month in the past year. Regulators continue to strengthen and widen the scope of whistle-blowing legislation. For example, in March 2014, the U.S. Supreme Court ruled that the whistle-blowing provisions in the Sarbanes-Oxley Act of 2002 should be expanded to include employees of private contractors and sub-contractors of public companies. In Europe, the European Commission approved the UCTIS V Directive for fund managers that introduced secured whistle-blowing reporting mechanisms through supervisors at national and pan-European level.

The role that internal audit should play in an organization’s approach to whistle-blowing has been debated in the last year. In the UK the Chartered Institute of Internal Auditors has developed a position paper on whistle-blowing policy, “Whistle-blowing and Corporate Governance – the role of internal auditing in whistle-blowing”. The position paper allows for two scenarios. First, where internal audit is directly involved in the procedures for whistle-blowing, the board should ensure there is an independent mechanism to provide assurance on the effectiveness of those procedures, and secondly, where internal audit is playing an indirect role it should provide assurance on the effectiveness of the system and procedures to the board.

- **Conflicts of Interest** Conflicts of interest can mean many things to many different people. At the heart of its meaning is the notion that someone with authority stands to gain from a decision that it is within their authority to make. Hence a risk occurs and this could be an important risk for organizations, and one that should be at the forefront of internal auditors’ minds when undertaking most audits.

Again, while there might not be a review specifically entitled “conflicts of interest” in the audit plan, the areas that constitute the greatest risk to an organization’s conflicts may still be included for example:

- o Remuneration process, e.g., can performance targets be manipulated to increase bonus or other personal incentives?
- o Compliance with anti-bribery and anti-corruption legislation, e.g., how vulnerable is your firm to the receipt of bribes and other inducements?
- o A third-party arrangement, e.g., is your firm doing business with someone who has a close relationship with an employee?
- o Sales processes, e.g., does the sales process benefit the customer or the sales representative?
- o Financial approvals and mandates, e.g., how sure are you that mandate holders do not have a vested, personal interest in holding that mandate?

## INTERNAL AUDIT RECOMMENDATIONS IGNORED IN LONDON WHALE TRADES CASE

*"The Financial Conduct Authority (FCA) fined JPMorgan Chase Bank N.A. £137,610,000 (\$220 million) for serious failings related to its Chief Investment Office (CIO). JPMorgan's conduct demonstrated flaws permeating all levels of the firm: from portfolio level right up to senior management, resulting in breaches of Principles 2, 3, 5 and 11 of the FCA's Principles for Businesses - the fundamental obligations firms have under the regulatory system ... Firm senior management did not take sufficient steps to ensure that all crucial information reached the appropriate decision-makers; findings made by internal audit were not escalated to senior management and therefore not considered."*

**UK Financial Conduct Authority, September 2013.**



## INCREASED PERSONAL LIABILITY

*"Internal audit's independence is as important as that of the chief risk officer and the head of group compliance, and its preservation should similarly be the responsibility of a named individual non-executive director, usually the chairman of the audit committee. Dismissal or sanctions against the head of internal audit should also require the agreement of the non-executive directors."*

**UK Parliamentary Commission on Banking Standards, "Changing Banking for Good" (Vol1), June 2013**

The world is a dangerous place, even for internal auditors. In the survey, 24 percent of respondents said that their personal liability was likely to increase in 2014. Increased complexity was also a key finding in this year's survey, and with a higher level of global regulation and a move toward stricter enforcement of rules and regulations, internal auditors (and indeed other senior managers in firms) are more than ever at risk from prosecution and enforcement when things go wrong.

So what can internal auditors do to minimize these risks and prepare themselves for any potential repercussions? Here are some suggestions:

- Be aware of external legislation/regulations, their reporting requirements and how the organization manages them. Make sure that compliance arrangements are strong enough to ensure that all legislation/regulatory information is considered, such as supranational or cross-border regulatory changes, the lessons to be learned from enforcement actions against firms undertaking similar business activities and the messages from speeches and other regulatory publications.
- In association with chief risk officers, heads of compliance and other relevant senior managers discuss all key relevant regulatory changes with the relevant supervisor to understand the likely impact on the firm and its customers.
- Maintain comprehensive notes of the discussions with regulators and others and keep a record of any documents or other information exchanged. In particular any requests or expectations stated by the regulator should be noted and as a matter of best practice confirmed in writing to ensure clarity of understanding. It goes without saying that all information provided to the regulator must be accurate and able to be substantiated, and that all actions and timescales agreed must be met and reported on both internally and externally.
- If a firm does not already have a lobbying programme in place it may want to consider investing in its ability to influence the external regulatory environment. While lobbying is a medium-to long-term investment it is important that areas pertinent to heads of internal auditors' personal positions, as well as the

wider implications as part of a senior management team, are included in any lobbying that occurs.

- Ensure that discussions on culture, risk appetite and setting the tone from the top have happened at a suitably senior level and, critically, that consensus has been reached. It is not necessarily a given that all senior individuals will agree on what "good" looks like for the firm. Indeed, anecdotally there have been some widely differing opinions and views aired at board meetings where the subject was raised. Any discussion, challenge and constructive criticism should be documented and the final agreed position needs to be given, and be seen to be given, support from all senior managers.
- Provide assurance that the mechanism for dealing with regulatory approvals and registrations is appropriate and maintained; in a large international firm this will also need visibly adequate resourcing. For example, it is imperative that the employee structure chart is kept up-to-date. The vast majority of regulatory bodies around the world have the concept of authorized or registered persons and it is essential that there is an accurate central record for all employees in all firms. This is particularly true of international groups where employees may hold a number of directorships and/or registrations in a number of different legal entities in a number of different jurisdictions.

Firms may wish to ask certain regulators for a full list of all registered persons to check that the records at the firm and the regulator can be reconciled; it is not, for instance, unheard of for a regulator to fail to update its own records, having been informed of changes. It is far better for both the individual and the firm to be active in undertaking such checks rather than discrepancies coming to light as part of, say, an intrusive supervisory visit and there being a mismatch of understanding as to which senior manager is registered where, and responsible for what.

- Make sure that job descriptions are up-to-date and accurately reflect actual responsibilities. Job descriptions are often only considered in detail when someone is new in their role and even then it is all too often a high-level and general document. Almost nowhere is the interlinking between roles, job descriptions and accountabilities routinely considered. One immediate area for consideration might be for all senior managers to review and document exactly what their role covers and how those obligations are discharged. This activity needs to be done on a firm-wide basis to ensure that the resulting aggregation of all the (much) more detailed job descriptions come together into a seamless whole. For the whole process to be effective it then needs to be kept up-to-date.

Compliance officers and other senior individuals could do worse than use the policy recommendations of the Financial

Stability Board, whose work on risk governance under the aegis of the G20 has set the benchmark for the expectations on senior managers. From the principles for an effective risk appetite framework (RAF) the FSB has set out the roles and responsibilities of the board of directors, the chief executive officer, the chief risk officer, the chief financial officer, business line leaders and legal entity-level management as well as internal audit.

For internal audit these were:

- o routinely include assessments of the RAF on an institution-wide basis as well as on an individual business line and legal entity basis;
  - o identify whether breaches in risk limits are being appropriately identified, escalated and reported, and report on the implementation of the RAF to the board and senior management as appropriate;
  - o independently assess periodically the design and effectiveness of the RAF and its alignment with supervisory expectations;
  - o assess the effectiveness of the implementation of the RAF, including linkage to organizational culture, as well as strategic and business planning, compensation, and decision-making processes;
  - o assess the design and effectiveness of risk measurement techniques and the management information system (MIS) used to monitor the institution's risk profile in relation to its risk appetite;
  - o report any material deficiencies in the RAF and on alignment (or otherwise) of risk appetite and risk profile with risk culture to the board and senior management in a timely manner; and
  - o evaluate the need to supplement its own independent assessment with expertise from third parties to provide a comprehensive independent view of the effectiveness of the RAF.
- Routinely collect and maintain the evidence to show they discharged all their obligations and responsibilities. When roles change, detailed documented handovers need to become the norm to ensure that all concerned can manage their personal regulatory risk. It could easily be seen as a cottage industry but the greater level of documentation around job descriptions is an essential part of enabling senior managers to demonstrate the appropriate discharge of their responsibilities.
  - Engaging in a rolling training programme that includes relevant legislation and regulation. Build and maintain their own personal archive of evidence to demonstrate the full and complete discharge of their responsibilities. For some quantitative elements that is likely to be a relatively simple process but there are often challenges when culture is added into the mix. One quick win could be to gather all board and other meeting minutes which provide evidence of challenge and engagement by the individual. For an appreciation of the scope of the evidence to be gathered, heads of internal audit could do worse than to look again to the FSB which put together a list of "indicators" for senior managers under which they can demonstrate that they:

- o Are committed to establishing, monitoring, and adhering to an effective risk appetite statement that underpins the institution's risk management strategy and is integrated with the overall business strategy.
- o Have a clear view of the risk culture to which they aspire for the institution, systematically monitor and assess the prevailing risk culture and proactively address any identified areas of weakness or concern.
- o Promote through actions and words a risk culture that expects integrity and a sound approach to risk. The board and senior management should promote an open exchange of views, challenge and debate, and ensure that all directors have the tools, resources and information to carry out their roles effectively, particularly their challenge function.
- o Have mechanisms in place, such as talent development and succession planning, which help to lessen the influence of dominant personalities and behavior.
- o Systematically assesses whether the espoused values are communicated and adhered to by management and staff at all levels to ensure that the "tone at the middle" and throughout the institution as a whole is the same as the "tone at the top".
- o Have mechanisms in place to assess whether the risk appetite statement, risk management strategy and overall business strategy are clearly understood and embraced by management and staff at all levels, and effectively embedded in the decision-making and operations of the business.
- o Have established a compensation structure that supports the institution's espoused core values and promotes prudent risk-taking behavior.
- o Demonstrate a clear understanding of the quality and consistency of decision-making throughout the business, including how decision-making is consistent with the financial institution's risk appetite and the business strategy.
- o Have clear views on the business lines considered to pose the greatest challenges to risk management, such as unusually profitable parts of the business, and these are subject to constructive and credible challenge about the risk-return balance.
- o Systematically monitor how quickly issues raised by the board, supervisors, internal audit and other control functions are addressed by management.
- o Have processes in place to ensure that failures or near-failures in risk culture, internal or external to the firm, are reviewed at all levels of the organization and are seen as an opportunity to strengthen the institution's risk culture.
- o Assess and communicate lessons learned from past errors which are seen as an opportunity to strengthen the institution's risk culture, and to enact real changes for the future.



## RESOURCE RISK

*“The Review team understands that the internal audit function is not fit for purpose in terms of capabilities, information gathering, analysis and dissemination and prioritisation of topics.”*

**Paul Myners, The Co-operative Group, Report of the Independent Governance Review, May 2014**

In a number of categories the survey results showed resource to be less of a risk than last year, although management support was flagged as a worry for internal auditors. This may stem from the previous point, increased personal liability. Nevertheless, these two findings together suggest that internal auditors need to be aware of the issue and the need to manage resource risk carefully.

There are a number of factors to consider when determining the nature of resource for an organization’s internal audit function:

- location;
- risk universe and control environment;
- extent of audit plan;
- business strategy;
- business change/stability;
- experience of existing employees;
- availability of resource in the market place;
- other elements, such as past regulatory history, levels of complexity in business model, risk infrastructure, mix of preventative and detective controls.

Given these criteria, what can heads of internal audit do to manage the difficulties between ever-tightening budgets and the need to keep quality of results high? Here are some examples:

- **Use of third-party/outsourcing/co-sourcing arrangements**

There are some undoubted benefits to outsourcing or co-sourcing the internal audit function. These include a higher level of specialist knowledge, on-demand resource and lower costs. There can, however, be some important risks to consider. These include:

- o **Weak governance** Careful governance is needed in the management of third-party arrangements. Among the areas to focus on are:

- Before engaging with a third-party supplier it is important that a thorough procurement process has been undertaken to identify the most suitable partner. Adequate due diligence should be undertaken and third-party firms interviewed about how they intend to fulfil the objectives of the engagement. These objectives should be clear and comprehensive.
- Appropriate and regular reporting and communication facilities need to be put in place. Monthly (or more regular) meetings need to be established between both senior representatives of each party but also including the operators at the coal face.
- The organization needs to understand the management information being provided and be able objectively to analyze and question the third-party firm on exceptions or slippage to contract arrangements.
- Formal lines of approval need to be established at a suitably senior level in an organization to agree changes to contract, policy and process. Policies and processes used by the third party need to be reviewed and agreed by the organization. The organization needs to own the policies and have final sign-off on the processes used.
- The control functions – compliance, risk and internal audit – should view this arrangement as in-house and treat the third-party provider as another department. Their responsibilities should not change just because a function has been outsourced.
- The contract should have clear and explicit rights for termination and redress should things not work out as intended, and management should not be afraid to discuss invoking these rights with each party.

- o **Breach of regulatory requirements** In the UK, the systems and controls section of the two financial services sector regulators' the Prudential Regulation Authority and FCA Handbook, SYSC 8, sets out the appropriate rules. The responsibilities associated with outsourcing are defined as critical or important operational functions or any relevant services and activities. It does not cover the provision to the firm of advisory services, and other services which do not form part of the relevant services and activities of the firm, including the provision of legal advice to the firm, the

training of personnel of the firm, billing services and the security of the firm's premises and personnel. The SYSC rules require that the firm retains responsibility for those activities which are being outsourced; that due care and skill should be observed when entering into an outsourced contract; and that controls for monitoring/supervising performance should be established.

- o **Underestimating monitoring arrangements** Monitoring and supervising arrangements are essential to the success of a third-party engagement. The three lines of defense model is still appropriate even when applied on an engagement-by-engagement basis. For example, in the first line, management need to monitor and challenge management information regularly to be able to assess the successful achievement of the engagement. Management may also feel the need to put in place first-line "auditing" arrangements including file checks and process reviews to gain the assurance they need that all is going well.

In the second line compliance and risk need to be able to work together to assess the risks and controls inherent in the process and advise and provide independent assurance that senior management require.

In the third line internal audit need to be given access to the third-party firm and on a periodic basis need to give comprehensive assurance that the overall risks, both at the third-party supplier and in-house, are being managed appropriately. In third-party arrangements it is important that the control functions work together and provide a consistent message about the arrangement. Their findings and conclusions may lead to the termination of the contract and it is vital that this is done with irrevocable evidence that is agreed, internally, that it is a breach of the contract.

- o **Scope creep** There is a tendency with third-party suppliers to look for further "sales" opportunities within firms. This could lead to additional requests to perform further work either as an extension to the contract or as part of a separate engagement. As mentioned above the objectives of an engagement should be clear and comprehensive from the beginning, but understandably there may be issues that were not known at the beginning which come to light further down the line. Scope creep can therefore be both good and bad: good in that it can pick up material issues that were missed during the initiation of the contract and bad in that it could lead to increased cost, a realignment of focus away from the original issue and confusion on both sides, making management difficult. Control is absolutely vital. Firms should be in control of their third-party contracts, not the reverse. If the firm believes that an amendment to scope is beneficial then that is acceptable. A process needs to be in place with the third-party supplier to be able to weed out unnecessary areas of scope creep.



## UNDERTAKE A SKILLS AUDIT

*"The second review was commissioned following an ARROW letter from the regulator in June 2012, in which it asked senior management to provide assurance on the effectiveness of the internal audit function. The regulator judged the IIA standards to be insufficiently rigorous and argued that the function should instead be compared to that of its peers. This second review, conducted by a different firm in late 2012, was highly critical. It is also worth noting that one of the first acts of the new (interim) head of internal audit appointed in October 2012 was to restructure the team completely, replacing the majority of its staff in early 2013."*

**Sir Christopher Kelly, Report of the independent review into the events leading to the UK Co-operative Bank's capital shortfall, April 2014**

There are many attributes an internal audit team need from its employees: negotiating, interviewing, investigating and auditing knowledge; initiative; IT literacy; diligence; thoroughness; the ability to adopt a professional approach; project management; multitasking skills; relationship management and managing stress, and there are many more. To ensure that the team possesses these characteristics and to establish where further

improvements need to be made in the team, it is worth undertaking a skills audit.

A simple structure to use when undertaking a skills audit may be:

- identify existing skills and knowledge in the team;
- identify the future skills and knowledge required in the team;
- undertake a gap analysis, weighting each characteristic as to the level of importance to the team;
- assess the gaps and develop a recruitment and development plan for the team and each individual.

*"Internal audit staff should have the requisite collective skill levels to audit all areas of the institution. Therefore, auditors should have a wide range of business knowledge, demonstrated through years of audit and industry-specific experience, educational background, professional certifications, training programs, committee participation, professional associations, and job rotational assignments. Internal audit should assign staff to audit assignments based on areas of expertise and, when feasible, rotate staff within the audit function."*

**Board of Governors of the U.S. Federal Reserve System, supplemental policy statement on the internal audit function and its outsourcing, January 2013**

## FUTURE REGULATORY DEVELOPMENTS

### FAILURE TO ACT ON EVIDENCE

*"The Financial Conduct Authority (FCA) has fined Coöperatieve Centrale Raiffeisen-Boerenleenbank B.A. (Rabobank) £105 million for serious, prolonged and widespread misconduct relating to the London Interbank Offered Rate (Libor) ... a JPY Libor submitter informed Rabobank's internal audit group that his submissions were based on direct instructions from traders, yet the bank failed to address the issue."*

**UK Financial Conduct Authority, October 2013.**

Legal and regulatory risk was identified as a major area of risk in the survey. It accounted for 38 percent of things that internal auditors spent time on (8 percent above last year) and 34 percent thought it was a top priority, with 35 percent believing it was a challenge for the board of directors in 2014. Twenty-four percent said that they were expecting to spend more time responding to the implementation of industry-specific legislation and 19 percent expected to spend more time interacting with regulators.

Putting all this together the conclusion is that legal and regulatory developments are still an issue for internal auditors. What can internal auditors do to manage this risk?

- **Ensure compliance functions are adequate** The responsibilities of a compliance function should include surveillance of the horizon for forthcoming regulatory issues, analyzing and assessing the impact of these issues on the firm, communicating issues and risks to senior and operational management and facilitating any external feedback or commentary to appropriate organizations. Internal audit should provide assurance that the compliance function is undertaking its responsibilities fully and diligently and that nothing is being overlooked to minimize the risk to the organization.
- **Being aware of regulations and any actions and implications** There may be a limit to the scope of a compliance function's responsibilities when monitoring the regulatory landscape and this may not include looking for accounting or audit developments that would affect the internal audit function directly. Internal auditors should satisfy themselves that their own personal risk is being covered by the compliance function and, where it is not, devote time to monitoring audit and accountancy websites for any relevant future material. For example, recent surveillance may have picked up the external audit case in Hong Kong where EY had been ordered by the High Court to hand over papers relating to a Chinese client. The Hong Kong Securities and Futures Commission petitioned for the papers but EY claimed that Chinese law prohibited the mainland partner of the firm from passing on documents.

- **Discussions with regulators** In the UK, the financial services regulators will hold regular meetings with heads of internal audit as part of their supervisory process. These, and any similar meetings in other industries, give the internal auditor the opportunity to ask about forthcoming regulations and the risks that those regulations pose, and to discuss internal audit's approach to those regulations. As a matter of good practice detailed minutes should be taken of all meetings with regulators.
- **Liaison with compliance and risk functions** Survey responses indicated a slight increase in the amount of time internal audit spend interacting with other assurance functions. With regard to preparing both the organization and themselves for new regulations it is vital that internal audit maintain a healthy and regular communication with compliance and risk functions. These relationships pose an interesting challenge for all parties: on the one hand trying to maintain the kind of workable independence that the roles demand while on the other trying to work in harmony for the good of the organization. It is important that the attitudes towards independence are not too entrenched on all sides; some flexibility needs to be displayed for the good of the organization. For example, defensive stances to proposals or disagreements regarding points of detail may only disadvantage the objective of the relationship.

### INTERNAL AUDIT DID NOT FIND FULL EXTENT OF PROBLEM.

*"State Street UK has been fined £22,885,000 by the Financial Conduct Authority (FCA). State Street UK's Transitions Management (TM) business had developed and executed a deliberate strategy to charge clients substantial mark-ups on certain transitions, in addition to the agreed management fee or commission. These mark-ups had not been agreed by the clients and were concealed from them. State Street's Corporate Audit Function was based in Boston and had responsibility for internal audit oversight of the UK TM business. Two audits of the UK TM business were undertaken in the Relevant Period. The first covered PSG front office arrangements, while the second covered the operational functions supporting PSG. Although the audits identified some control issues (for example the manual nature of the fixed-income processes), they did not identify a number of the weaknesses that existed in the relevant period. Both audits received a satisfactory rating."*

**UK Financial Conduct Authority, January 2014.**

## IT RISKS

*“Cybersecurity is a huge area of concern, ranking near the top of nearly every list of business risks for about a decade. But the risk levels are higher than ever this year ...”*

**Richard Chambers, president and CEO of the U.S. Institute of Internal Auditors, April 2014.**

“Cyber risk” is any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems. This affects all types and sizes of organizations including small businesses as there is growing evidence that criminals are targeting the less protected organizations. There are many examples (and names) of the types of cyber risk but a non-exhaustive list might include mobile devices, malware, social engineering, cloud computing, hacking, web application attacks and corporate and government espionage. As well as those areas mentioned above, internal auditors may wish to consider some other areas of IT risk:

- **Data privacy and security** Underpinning effective control of cyber risk are the basics the internal audit should look for, e.g., physical security arrangements, system access controls (passwords, log ins, etc.), data storage arrangements, remote access, data management, compliance with data protection legislation.
- **Social media** To tweet or not to tweet ... The risk of uncontrolled use of social media could be irreparable damage to an organization’s reputation. With the current environment encouraging comment and opinion in this form it is vital that organizations know what activity about them is being broadcast across social media. Organizations need to put in place appropriate governance and control arrangements including policies, guidance, monitoring and reporting arrangements. In particular, access and identify controls and suitable arrangements for approving content need to be established.
- **Business continuity/disaster recovery** Internal audit must consider how the organization would manage if presented

with a situation where normal operations could not be enacted. The concepts of business continuity and disaster recovery have been around for a while but still remain high risks to organizations. Internal audit need to embrace this risk and make sure that the arrangements organizations put in place are appropriate for continuance of operations in the light of a disaster. In summary, internal audit need to ensure that organizations understand and analyze their business sufficiently so that they can then assess the risks. Plans to ensure the key areas of the business can continue should be put in place and communicated effectively to all employees, and thorough and regular testing of those plans then needs to be undertaken.

- **Third-party risk/outsourcing** Internal audit should be aware that cyber risk is not just an issue for the IT team. Risk management functions must also have a detailed understanding of the risks and the practical tools and techniques that are available to offset them. This poses the problem of whether non-IT departments can recruit and retain the necessary skilled resource to challenge IT strategies. This is especially relevant in organizations with a small internal audit team where budgetary pressures mean that auditors need to multi-skill across a number of specialized areas. This may lead heads of internal audit to consider outsourcing as a way forward.

Some pros and cons of outsourcing have been discussed above but the risk to organizations is particularly acute from an IT perspective. The issues above still apply but where IT systems, processes and responsibilities are outsourced, internal audit need to place special focus on due diligence and procurement processes when appointing an outsourced provider. Issues to consider include: contract and communication arrangements; service level agreements; monitoring of the service (is it frequent and detailed enough?); resolution arrangements (are they prompt and effective?); business continuity arrangements in times of a disaster; clawback and recourse arrangements where service levels are not met; resourcing; and skill levels of the outsourced provider.

# ADAPTING TO COMPLEX CHALLENGES: IS CHANGE HAPPENING AT THE RIGHT PACE?

---

The future risk and control landscape for internal audit is evolving and in some areas is beginning to change quickly. Against that background it is notable that the results of the Accelus State of Internal Audit Survey, at a high level, have remained relatively unchanged for the last few years. Is there a risk that internal audit is being left behind, relying on outdated mind sets, historic practices and old methodologies? It is too early to tell, but there is no doubt that remaining unchanged in a changing world does no one any favors – not the firm, not the customer and certainly not the internal auditor.

In common with other risk and control functions in a firm, internal auditors have a difficult job that is not helped by an increasing need to adapt to many different, complex challenges. The internal audit function is increasingly expected to cope with regulatory change, the shifting expectations of regulators, boards and senior managers and more intense scrutiny of their work at a time of still-tight budgets, increasing competition for skilled risk resources and changing reporting requirements. Change takes time but the world of risk and control is changing fast.

The fastest change is happening in the financial services sector and this is setting the agenda for all other firms. There is a clear direction of travel with internal auditors being asked to step out of their traditional comfort zone and into the more qualitative worlds of culture and corporate governance. Internal auditors must engage with the change and there is evidence that this is happening, but the survey results show this process is slow.

The downside is that unless they are aware of, and embrace, the changing operating environment, internal auditors will not be in a position to support their firm appropriately and assist the board in discharging its obligations. Specifically, the internal audit function needs to assess the impact of the raft of changes, what

it means in terms of resources, required skill sets (for themselves and others such as the audit committee), reporting obligations and work programs. Potentially new areas such as culture, regulatory complexity, personal liability for senior managers, corporate governance and the detailed elements of cyber risk all need to be considered.

What good looks like for internal audit is shifting, and one-size most definitely does not fit all. The internal audit function needs to continue to work closely with its firm's audit committee and board to ensure a clear and common understanding of the skills, roles, remits and, increasingly, personal liabilities for anyone at a senior level. A key feature of internal audit work of the future will be not only to assess the efficacy of internal control processes but also to provide an opinion as to whether the corporate governance infrastructure is fit for purpose and operating effectively. The precise nature and shape of any corporate governance assurance work will need to be tailored precisely to the business activities under consideration but review measures might include, say, unannounced attendance at meetings, assessment of the quality of the argument on risk as evidenced in the minutes of key committees, a sense-check of the practical ramifications of the "tone from the top" in terms of culture and risk awareness and a detailed assessment of the quality and coherence of risk and other management information.

Last but most certainly not least for internal auditors is the perceived and genuine increase in potential personal liability. It is well understood that internal auditors need to have the independence and authority to report all material findings, risks and weaknesses without interference and undue pressure to alter or omit points. This position becomes even more important when the personal liability of the internal auditor is brought into the mix. That said, this potentially greater liability should have its compensations as internal audit continues to evolve into a vital, business-critical function which sits at the heart of not only risk management within a firm but also of the exercise of effective corporate governance, and the cascade of a positive risk culture.

# NEXT STEPS FOR INTERNAL AUDIT

---

We hope you found this year's report valuable. Many of our customers tell us these reports are useful for benchmarking, and also for building internal business cases to support greater investment in the internal audit function. Something we know is important to you.

## **PARTNER WITH THE EXPERTS**

Thomson Reuters Accelus delivers a range of integrated solutions designed to help address the challenges you face daily and better manage the ever-changing risk and regulatory landscape.

## **MAXIMIZE THE INSIGHT YOUR INTERNAL AUDIT TEAM DELIVER TO YOUR ORGANIZATION**

Internal audit teams are as individual as the organizations they are a part of. Yet, most are now facing a common set of challenges that are emerging from the difficult economic environment, an enhanced need for corporate dynamism, and increased regulatory pressure. These trends are coalescing into a triple set of pressures on audit teams:

- to increase the amount of strategic value and insight that a single team can deliver to the business;
- to engage proactively with a broader set of stakeholders across the business;
- and to simultaneously provide independent and objective assurance on risk management, corporate governance, and internal controls.

Meeting these pressures head-on, and then rising above them to achieve a truly successful audit function, requires fresh thinking. It is not possible to deliver on these objectives while using traditional, manual audit processes. Nor is it possible to achieve success using a point solution.

## **DRIVE EFFICIENCY AND PRODUCTIVITY**

Thomson Reuters Accelus solutions for internal audit help you standardize, automate and manage key aspects of your audit process – including the sharing of audit findings, key risk areas and recommendations across compliance, IT, internal controls and risk management processes. Designed by auditors for auditors, our comprehensive audit management solutions can help with risk assessment, audit planning, scheduling, working

paper preparation, time and expense entry, report generation, and issue tracking. Utilizing these powerful audit solutions, you avoid redundant efforts and save valuable time, money and resources. In addition, your auditors spend less time identifying and testing internal controls and can place greater emphasis on measuring risks, investigating material threats and controlling weaknesses.

## **CHOOSE THE INTERNAL AUDIT SOLUTION THAT BEST SUITS FOR YOUR BUSINESS**

Thomson Reuters Accelus provides a choice of internal audit solutions tailored to your organization's size and specific business requirements. You can choose the delivery of your solution to fit your firm's unique internal IT, infrastructure, and budget requirements.

## **ENABLE ENTERPRISE GRC**

Governance, risk and compliance activities are, by nature, interconnected and rely on common sets of information, taxonomy, methodology, processes and technology. The Accelus Enterprise GRC platform delivers connectivity that enables organizations to take an integrated approach to GRC.

By facilitating connectivity between the various assurance functions, the front office and the board, Accelus informs and simplifies GRC complexity, supporting analysis and decision-making, translating risk into opportunity and enabling organizations to run their businesses in a more principled, effective and productive fashion.

## **ENGAGE WITH THE RISK AND COMPLIANCE FUNCTIONS**

The need for more communication and interaction with their organization's risk management and compliance teams emerged as a key takeaway for internal auditors in this year's report. Accelus Risk Manager and Accelus Compliance Manager make it easier for risk and compliance teams to work more closely with the third line of defense, aligned around a common approach to GRC.

To speak to an advisor about how we can help you meet the challenges ahead, please contact your local Thomson Reuters office or email us at [accelus@info.accelus.thomsonreuters.com](mailto:accelus@info.accelus.thomsonreuters.com).

## THOMSON REUTERS ACCELUS

The Thomson Reuters Governance, Risk & Compliance (GRC) business delivers a comprehensive set of solutions designed to empower audit, risk and compliance professionals, business leaders, and the Boards they serve to reliably achieve business objectives, address uncertainty, and act with integrity.

Thomson Reuters Accelus dynamically connects business transactions, strategy and operations to the ever-changing regulatory environment, enabling firms to manage business risk. A comprehensive platform supported by a range of applications and trusted regulatory and risk intelligence data, Accelus brings together market-leading solutions for governance, risk and compliance management, global regulatory intelligence, financial crime, anti-bribery and corruption, enhanced due diligence, training and e-learning, and board of director and disclosure services.

Thomson Reuters has been named as a category leader in the Chartis RiskTech Quadrant™ For Operational Risk Management Systems, category leader in the Chartis RiskTech Quadrant™ for Enterprise Governance, Risk and Compliance Systems and has been positioned by Gartner, Inc. in its Leaders Quadrant of the "Enterprise Governance, Risk and Compliance Platforms Magic Quadrant." Thomson Reuters was also named as Operational Risk Software Provider of the Year Award in the Operational Risk and Regulation Awards 2013 and 2014.

**For more information, visit [accelus.thomsonreuters.com](http://accelus.thomsonreuters.com)**



THOMSON REUTERS™