IT Internal Audit: Multiplying risks amid scarce resources

KPMG International

kpmg.com

As information technology and systems become ever more complex, those technologies are changing ever more rapidly and we are beginning to see the deployment of artificial intelligence systems; this means entities must audit based on the increasing risk they face and find ways to overcome resource and budgetary constraints to achieve this.

Contents

Foreword

IT Internal Audit (ITIA) is coming under increasing pressure to measure the management and mitigation of technology risks that are proliferating. Resources are stretched and demands are ever increasing. As technology risks multiply, ITIA is being asked to do more. For some, budgets are rising, but not for all. IA professionals are rising to the challenge, but nonetheless this latest survey of the market shows there are significant gaps in resources and capabilities.

To bridge the gap, ITIA must redouble its efforts to enhance the skills of existing personnel, to partner with third parties and to hire talented professionals where necessary. It is becoming critical to present a forward-looking and compelling business case for more resources, where needed, to the Board and senior management.

Andrew Shefford
Global Head of IT
Internal Audit

The findings in this report are based on a survey of 250 ITIA professionals around the world. Insights are also included from KPMG's 2016 IT Internal Audit conference. It is the third report of its kind (the previous ones were published in 2009 and 2013).

I would like to thank all of the respondents who participated in the survey, including many of our member firms' clients. I hope that you will find it a valuable and insightful assessment of the state of ITIA globally, providing you with information that broadens your understanding of the critical contribution ITIA can make to the business.

At a time when demands placed on ITIA are steadily growing, we expect this report will stimulate your thinking and provide fresh perspectives.

Introduction

Technology risk is pervasive and continually changing. It is a critical time for IT professionals and internal auditors (IA) of IT, who must build plans to provide assessments of, and insights into, the most important technology risks and how to mitigate them. ITIA must keep abreast, and wherever possible anticipate, fast-moving developments in technology. In particular, ITIA must plan, deliver and, when necessary, flex its audit plan in such a way that it responds to these changes in the most appropriate, efficient and effective manner. And it must do so within the budgetary constraints imposed by the organization, facing competition (both internal and external) for resources.

To find out how ITIA is responding to these challenges, KPMG surveyed ITIA representatives of 250 organizations, both large and small, that are operating in a wide range of industries around the world (see demographic breakdown on page 19). The survey took place between October 2016 and February 2017. Based on our analysis of the survey results, the main findings include the following.

— ITIA is currently focusing on core operations risks, such as unauthorized access or changes to critical business applications. But respondents anticipate a significant shift in attention in 2018 toward emerging risks, such as robotics and the Internet of Things (IoT) (connecting devices to the internet and to each other). ITIA will need to build holistic assurance over these new risks across the organization to cover key components such as cyber defenses around data, applications and infrastructure.

— ITIA faces the task of obtaining the appropriate skilled and qualified resources to assess fast-changing risks and to increase the use of tools and technologies such as data analytic technology and automated workflow tools.

— Forty-three percent of respondents say their ITIA budgets are likely to be stable and 8 percent say they may fall between 2017 and 2018. Thirty-eight percent say they may rise. If budgets are not, at least, maintained, there is a danger that ITIA will not be able to perform its job of providing adequate assurance over all the different kinds of risks, not just those affecting core operations.

— The chief area of concern is whether ITIA has the skills required to provide assurance over the most important technological risks to the organization. ITIA respondents say they face talent shortages in many risk areas they are auditing. The biggest resource gaps are in cyber security, followed by data and analytics (D&A), and privacy.

— One area of need is the ability to use D&A for various purposes in ITIA. Only a quarter of respondents say they use analytics for continuous auditing, monitoring and assurance techniques; the remainder use it in an ad hoc way.

— Assurance is typically delivered through direct internal and external audits, rather than by leveraging the assurance work done by the organization's independent assurance specialists. The implication is that many organizations lack an integrated approach to assurance.

ITIA focus will shift to robotics and IoT.

51%
say budgets won't rise

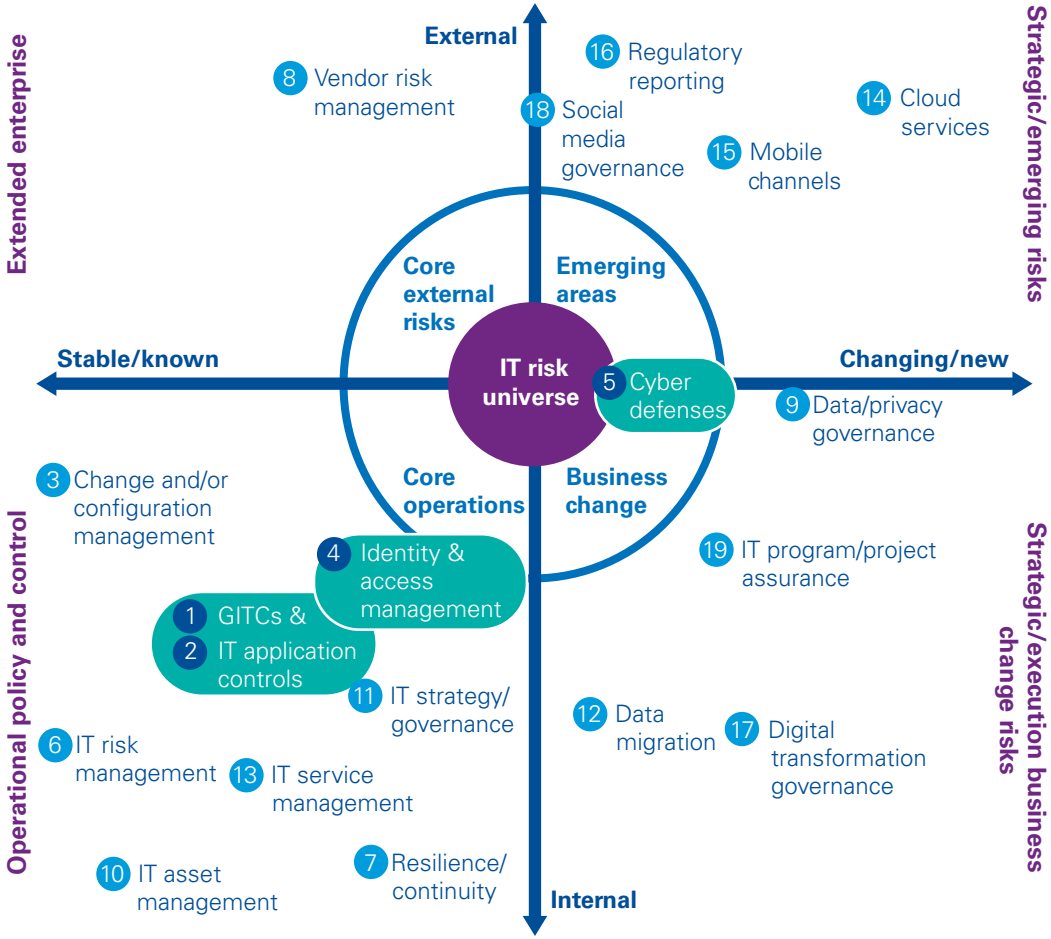
Key areas of risk

The questionnaire asked organizations to pick from 19 risk areas that their ITIA has reported on within the previous 12 months or has plans to review in the next 6 months. The areas chosen most frequently are: general IT controls (GITCs) and application layer controls. The prominence of these two areas reflects ITIA's ongoing assurance over these key controls, under regulations such as those pertaining to the Sarbanes-Oxley Act in the US.

IT risk universe

Based on KPMG's experience of advising clients on managing IT risk, key risk areas have been placed in an IT risk universe, portrayed in this chart and the one on page 6. The horizontal axis depicts the pace of change, from static at the left to fast moving on the right. The vertical axis indicates whether the focus of control tends to be external (above the horizontal axis) or internal (below it).

Areas ITIA has reported on within the previous 12 months



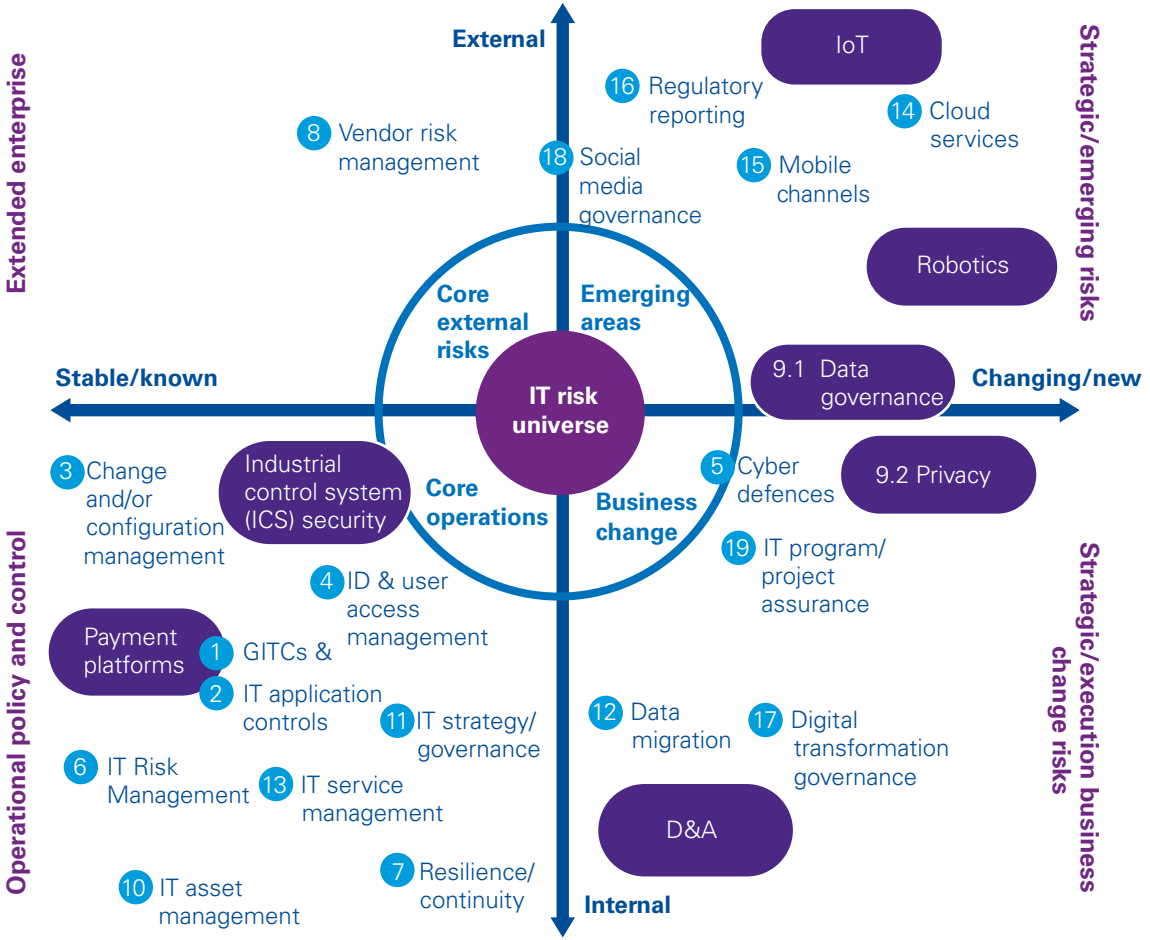
Source: IT Internal Audit: Multiplying risks amid scarce resources, KPMG International, 2017

The next most frequently cited areas are cyber defenses and the management of identification and user access. Other risk categories fall some way down the level of importance, such as change and/or configuration controls, IT risk management, resilience and continuity, and vendor risk management.

GITCs, application controls, cyber defenses and data protection were frequently cited risk areas in 2013 and form the traditional core operations risks. In the latest survey these risks are joined by areas such as: the IoT and robotics and machine learning (computers performing routine tasks previously done by humans). These are seen as emerging risks that will grow in importance in the coming months. In these cases, the risks include the governance and change management associated with their integration into business processes, as well as their compatibility with other IT systems and the culture of the organization. These new risks present challenges for ITIA to understand and provide assurance over, as well as opportunities to enhance, its capabilities.

In summary, there are some stark differences between this chart and the one on page 5. There is a marked shift in focus to emerging areas, such as robotics and IoT. Yet at the same time, organizations cannot afford to neglect the basic areas of risk, including service management areas, access management, industrial control system security and IT disaster recovery.

Areas ITIA plans to review in the next 6 months



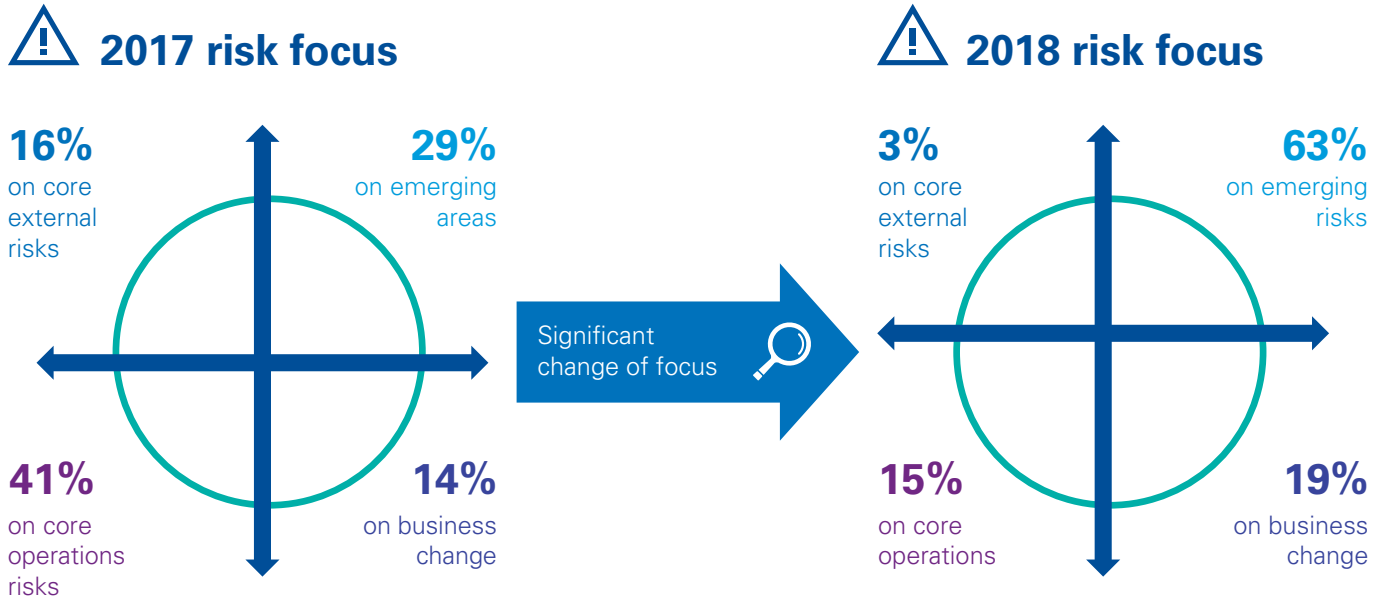
Source: IT Internal Audit: Multiplying risks amid scarce resources, KPMG International, 2017

Focus shifts from core operations to emerging risks

The survey found that ITIA is currently focusing on core operations risks (41 percent). Emerging areas of risk (29 percent) (such as robotics and the IoT) plus risk arising from business changes (such as digital transformation and IT project delivery) and core external risks (such as vendors hosting IT data centers) receive considerably less attention (see chart below). But the focus is expected to change significantly in 2018: respondents say emerging risks will receive by far the most attention (63 percent), whereas core operations will fall to only 15 percent, lower than business changes.

The implication of these findings is that organizations will need to gain access to new skills and potentially invest to leverage new tools to tackle these emerging areas. In addition, companies will have to come up with alternative approaches to reporting that take place in real time, reflecting the pace of change of the risk environment.

Focus of ITIA functions



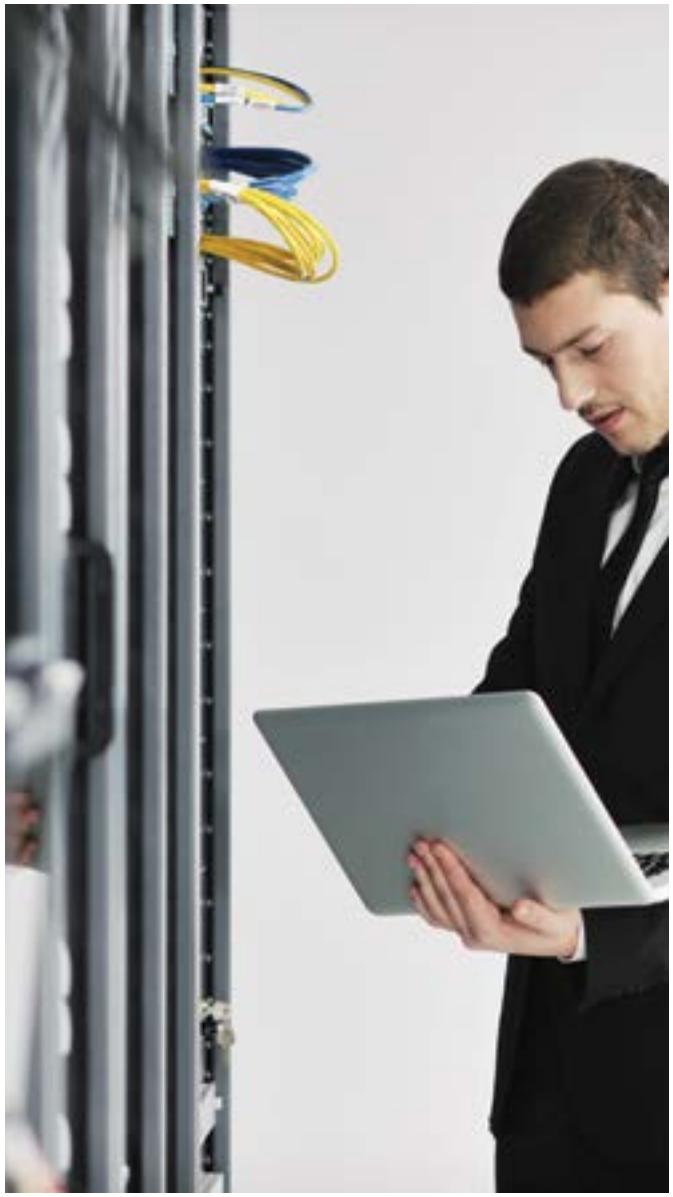
Source: IT Internal Audit: Multiplying risks amid scarce resources, KPMG International, 2017

Within core operations, the survey shows that risks arising from GITCs and application layer controls are pervasive. This is reinforced by such rules as those related to the Sarbanes-Oxley Act. In addition, cyber risks affect core operations in many different ways, too. Identity and access management risks sit within core operations risks. Cyber risks can affect many aspects of IT infrastructure and applications, as well as targeting access points, such as mobile devices. They also arise through fast-changing interconnections in computer networks and automated processes. Core operations risk will therefore remain important.

Management cannot ignore cyber defense risks, which bridge business change and emerging areas. Cyber defense risks reflect the increasing sophistication of network attacks, the importance of setting the right cyber controls in IT projects and programs, and of building the right IT control environment over emerging technological areas such as IoT and robotics.

ITIA needs a robust risk assessment for its organization that should be conducted at least annually and preferably more frequently, to support those cyber components that most need addressing. The risk assessment needs to consider the organization's expected controls for each component and to define who in the organization is to provide assurance over them. Without this, the organization might have a false sense of assurance, for example, wrongly assuming there is one homogeneous cyber risk and failing to understand what is required to provide adequate assurance over all the different elements of cyber risk.

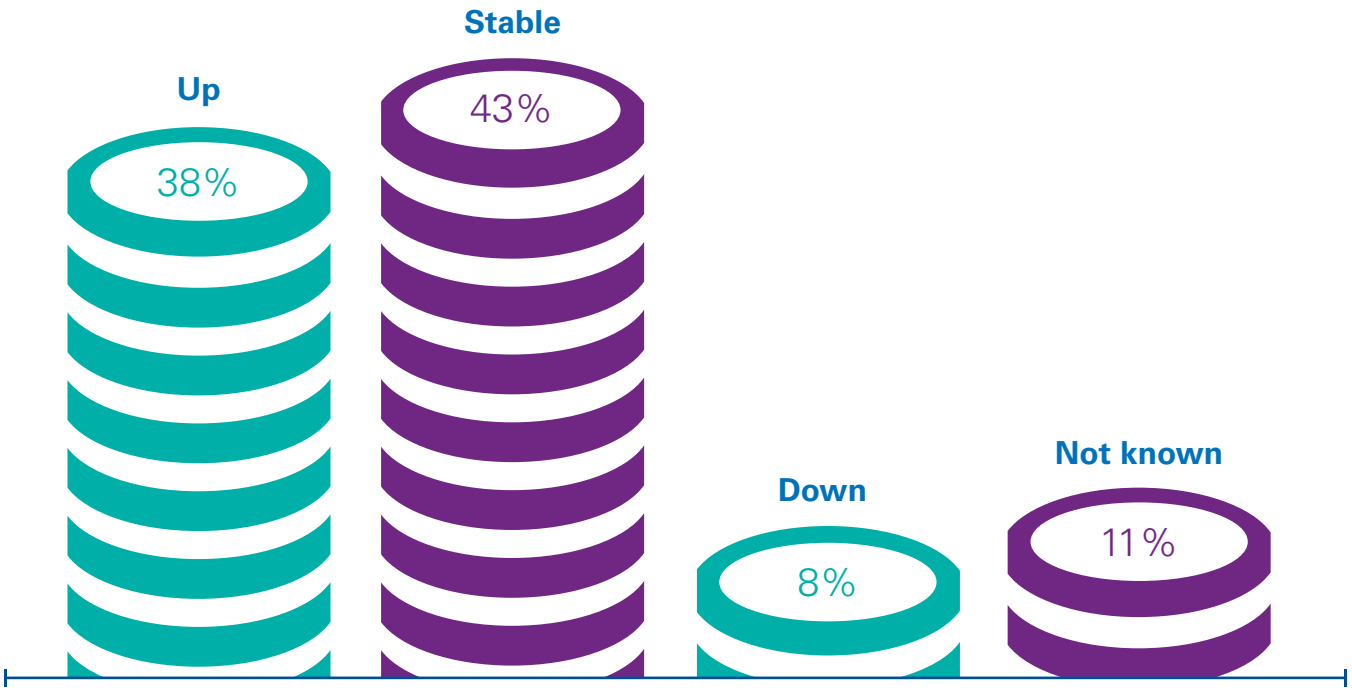
In view of the expected shift of focus to emerging risk areas, ITIA faces the task of obtaining the appropriate skilled resources and level of automation to assess fast-changing risks. It will also need to optimize the use of tools for D&A and automation. This will be connected to business IT systems ('audit of IT') and will run audit workflow ('audit by IT'). To ensure ITIA receives the resources it needs, it must argue its case cogently before senior management and the board, supported by evidence of the emerging risks relevant to the parent organization and the state of assurance over them.



Needs and budgets

The quality of assurance will partly depend on the size of the budget for ITIA and it is becoming increasingly important to make budgets go further. Fifty-one percent of respondents say that their ITIA budgets are likely to be stable (43 percent) or fall (8 percent) between 2017 and 2018. Thirty-eight percent say budgets will rise.

Directions of 2018 ITIA budget



Source: IT Internal Audit: Multiplying risks amid scarce resources, KPMG International, 2017

These budgets are needed to keep pace with technology risks and to be able to deploy more integrated audit tools across the full audit lifecycle. The resources are also required to implement and integrate D&A in a continuous, systematic fashion in audits. Stretching the budget can be achieved in a number of ways. These include the automation of audit workflow and the deployment of highly skilled and experienced audit resources that can work efficiently.

These improvements will help enhance efficiency. But given the pace of change of risks, ITIA functions have a duty to bring to the attention of their Boards the limits to the assurance they are able to provide under current and forecast budgets. If audit plans are driven by cost rather than risk, ITIA may fail to fulfill its role adequately. Focusing on historic risk areas will not provide adequate assurance over emerging risks. IA can perform more tasks by using business and IT tools, but investment in the right specialized skills is key.

Resource constraints vary by size of organization. Nearly half the respondents in organizations with smaller headcounts say that their current ITIA budget is US$65,000 a year or less. This makes it severely challenging to provide their organizations with an effective view of core operations, external, business change and emerging risks.

ITIA at small organizations should be making a strong argument in favor of much higher budgets, approaching the budget levels of US$650,000 and above reported by other small organizations.

Among mid- and large-headcount organizations respondents typically report ITIA budgets of between US$65,000 and US$650,000 (58 percent of respondents in the mid-size headcount category and 56 percent of the larger organizations). In any size of organization the ITIA budget needs to be matched to the risks over which assurance is needed, and this is driven by a robust annual risk assessment.

The survey points to a compelling case that ITIA can make to their management and boards for a higher budget to support specialist resources and to invest in tools to address the range of risks faced. Even in a small-headcount organization, an IT risk event can have such severe business consequences that it should be worth rigorously calibrating the ITIA budget during the annual risk assessment. The result of this calibration is likely to provide a strong case in favor of increasing the ITIA budget.

Where the skills gaps are

The chief area of concern, in terms of human resources, is whether ITIA has the skills required to provide assurance over the most important technological risks to the organization. ITIA respondents say they face talent shortages in many risk areas they are auditing. The biggest resource gaps are in cyber security followed by D&A and privacy. Taken together, these three areas are prioritized by more than half the respondents.

Skills shortages

1. Cyber security
2. D&A
3. Privacy
4. Risk management
5. ERP systems
6. Compliance
7. Change management
8. Software development lifecycle
9. Data quality
10. Independent project assurance
11. Other

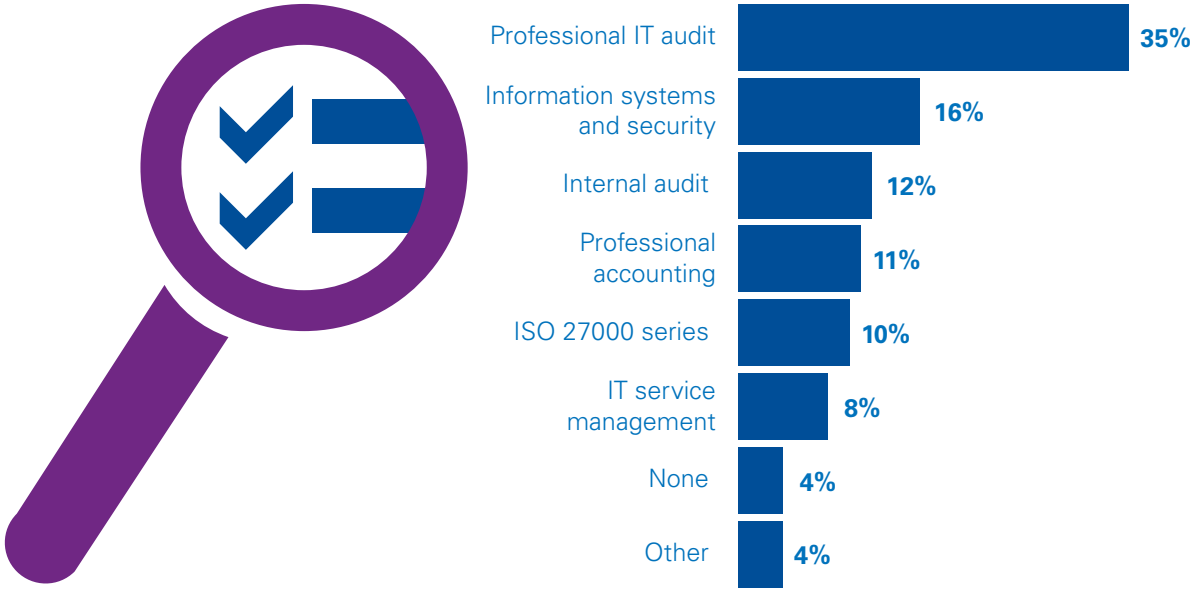
Source: IT Internal Audit: Multiplying risks amid scarce resources, KPMG International, 2017

IT audit skills shortages are reported across all sizes of organizations who responded. They are seeking additional skills to assess risk management and ERP systems followed by compliance, change management, software development lifecycle and data quality. Surprisingly, skills shortages in program assurance were of least concern, which may be in part due to the limited extent of reliance on program assurance by ITIA teams. In addition, assurance may be potentially sought from elsewhere.

Respondents were asked which areas are difficult to upskill from ITIA's existing repertoire of skills. Their answers show that organizations of all sizes reveal a similar pattern of skills shortages, with the gaps most acute in cyber security and D&A. However, a significantly bigger proportion of large organizations report skills gaps in cyber security and D&A than do respondents at smaller organizations. Clearly, the former are competing for talent against other big organizations, government agencies and consultants in the same limited pool of specialists.

Privacy risks should be among the highest ranking for ITIA to assure when their organizations are considering or implementing measures to shift data to the cloud; and these resources needed to assess privacy risks add to the staffing issues seen in cyber security and D&A (see KPMG's report). The prominence of data privacy is highlighted by the EU's General Data Protection Regulation, which could levy fines of up to 4 percent of a company's annual revenue.

Qualifications organizations look for



Source: IT Internal Audit: Multiplying risks amid scarce resources, KPMG International, 2017

In other areas of shortage, there is competition for risk management skills, even though they are less technology-focused than the skills deployed in cyber security and D&A. ERP skills, by contrast, have to be continually updated to keep pace with innovations in the field. Many of the large organizations have highly centralized ERP systems and can manage with smaller teams. Even so, ITIA has to compete to attract such specialists, who may only be needed for parts of the audit plan.

Organizations, understandably, place a high priority on the certification of their IT internal auditors: 96 percent of respondents call for it. Irrespective of organization size, 35 percent seek candidates with a professional IT audit qualification and 16 percent require an information systems and security qualification.

Priorities vary for other qualifications, depending on the organization's size. Professional accounting skills are preferred by smaller organizations. Mid-sized organizations look for internal audit qualifications. In consequence, small- and mid-sized organizations may place a reliance on non-IT auditors, unless they have support from third-party specialists in their delivery model. Larger organizations focus on more specialized IT qualifications such as cyber and IT service management. Consequently, those larger organizations gain a greater level of assurance over IT risks than the small- or mid-sized organizations.

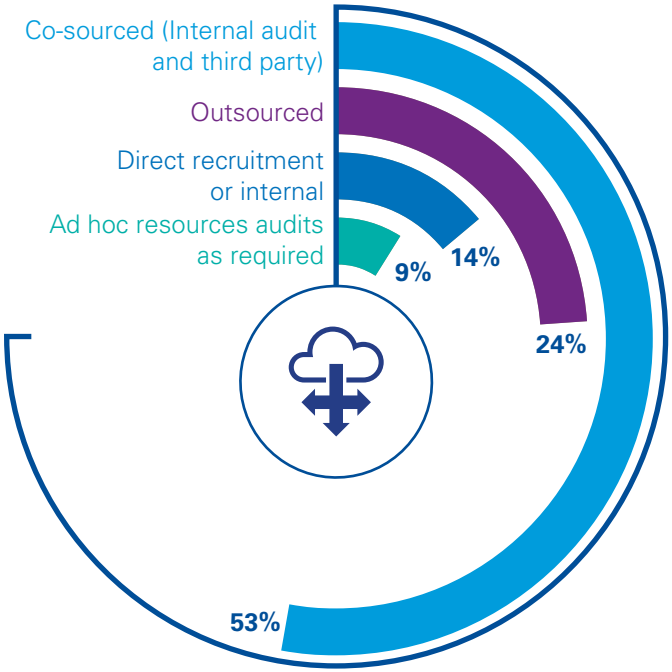
Use of third parties

Almost no organization has all the ITIA resources it needs because of the sheer breadth of skills required and the cost of maintaining, training and developing in-house resources to cover all the bases. Over three quarters of survey respondents rely on either co-sourced or full out-sourced ITIA delivery models. The balance of co-sourced versus fully out-sourced shifts depending on the size of organization. The smaller organizations have a higher preference for fully out-sourced ITIA, while larger organizations report a higher preference for co-sourcing. The difficulty of maintaining specialist internal resources to leverage a co-source model is seemingly too great for those smaller organizations. The larger organizations seem more attracted to leveraging the co-source model (for example to access technical knowledge transfer). But even those larger organizations need to re-evaluate whether their technical knowledge transfer is keeping pace with emerging risks.

According to the survey, the main reasons for outsourcing is a lack of people and a deficit of technical skills, the same reasons given in the 2009 and 2013 surveys. In view of the increasing range of risks and the lack of qualified staff, it is not surprising that ITIA turns to third parties to fill in the gaps.

Although compliance with legal requirements is a highly technical skill for ITIA, the survey shows that it is one of the least important reasons for hiring third parties. Given the ever-growing level of regulations around the world, organizations should carefully assess whether they need to think again about regulatory risk.

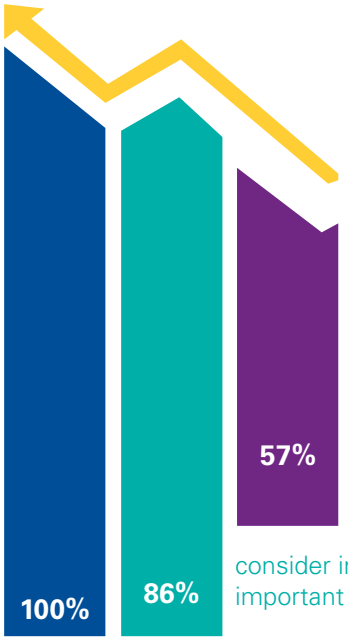
Delivery models



Source: IT Internal Audit: Multiplying risks amid scarce resources, KPMG International, 2017

Audit of IT and by IT

One of the most important skills for ITIA is the ability to harness D&A to deliver insights in key risk areas. Respondents were asked about the degree of importance of D&A for ITIA. All say D&A is a useful way of generating additional insights such as trends or anomalies, rather than the outcomes from traditional audits in which simple transaction checking occurs. Eighty-six percent see the importance of D&A for widening the scope of audit to cover such things as identifying the appropriateness of all actions to a critical database, or ensuring all changes to a critical IT system are appropriately approved.



consider the importance of using D&A for fraud as either important or very important.

consider increasing audit coverage important or very important.

want to be able to generate insights over and above data — with 85 percent marking this as either very or extremely important.

The reliance on D&A presupposes that the data is of high quality; 85 percent of respondents consider data quality to be very or extremely important. The survey asked what D&A tools are used. Excel was the most popular (30 percent), followed by ACL. The frequency of use of visualization and D&A tools increases as the size of organization grows, with sophisticated applications more popular among large organizations. In organizations with fewer resources, therefore, consideration should be given to leveraging their co-source or full out-source delivery models to learn from third parties as to which tools it would be worth investing in.

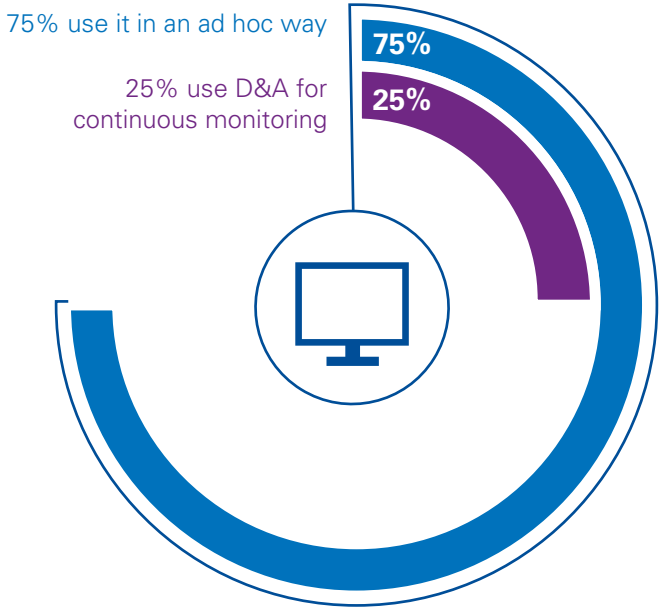
Even if organizations are deploying more sophisticated tools, this does not mean they are being used in a systematic way. Only a quarter of respondents say they use D&A for continuous auditing, monitoring and assurance to support ITIA; the remainder uses it in an ad hoc way. Larger organizations are running continuous D&A tools more frequently than smaller ones and are covering a wider range of areas, including integrated continuous auditing and continuous monitoring.

Source: IT Internal Audit: Multiplying risks amid scarce resources, KPMG International, 2017

It is important to know when tools are used, as well as how. The survey finds that many organizations deploy audit methodology/workflow tools across the full spectrum of their audit lifecycles. Data analysis is the prime area of focus, followed by working papers management, planning, risk and control analysis, recommendations and reporting. Very few respondents report that they use IT tools for assignment management and resource control, despite the fact that this would help optimize the allocation of scarce resources, especially that of skilled personnel.

The results show that organizations still have a long way to go to reach a high level of maturity in ITIA's use of D&A. But, as KPMG's 2016 ITIA conference highlighted, the emergence of business applications of artificial intelligence (AI) and machine learning is going to make it even more challenging for ITIA to ensure that IT risk is being measured, managed and mitigated. The survey shows that ITIA organizations intend to address emerging risk areas such as AI more fully next year and yet they have not yet developed their conventional data analytics capability. What is clear is that AI is going to be quickly incorporated into systems and processes, and so ITIA will have to develop rapidly a strategy for assuring the risk associated with it.

How data is analyzed



The survey finds that organizations deploy audit methodology/workflow tools across the full spectrum of their audit lifecycles.

Very few use IT tools for assignment management and resource control.

Source: IT Internal Audit: Multiplying risks amid scarce resources, KPMG International, 2017

Sources of assurance over key risks

When asked about the sources of assurance over key risks that are drawn on by ITIA, nearly 70 percent of respondents say they currently rely on direct internal and external audits. Only 30 percent look to the results of management's cyber security audits, ISO27001, standards compliance and independent project assurance results.

When looking specifically at IT project and program risks, KPMG research[1] indicates that between 30 and 60 percent of IT projects (depending on project types such as infrastructure, applications or data) have successful outcomes. Strategic IT programs and projects should therefore be a critical starting point for examining how risks over data, applications and infrastructure are controlled by the business.

This problem appears to be recognized by organizations, as survey respondents say that they will focus more in 2018 on business change risks, which include program and project assurance. Even so, the change in priority is only slight.

For the future, 40 percent of ITIA respondents said they have no program assurance activities commissioned or planned for a major IT enabled program their organization has planned or is undergoing. Of the 60 percent of respondents who report they have future program/project assurance planned, nearly half say they will rely on ITIA to deliver that assurance. A further quarter rely on their wider internal audit plan for some assurance over those IT programs/projects. The other quarter report they rely on sources outside the IT or wider audit plan.

Good practice suggests that an independent program assurance function will help mitigate the risk of program or project failure. We typically expect between two and five percent of an overall IT program budget to be spent on IPA, which could provide a rich source of assurance for organizations. Yet we see in our survey organizations tell us they conduct their own ITIA audits of risks and do not rely on the outputs of management's assurance activities. Where ITIA relies on its own audit activities there may be some duplication of efforts with management's own assurance activities. Conversely, some organizations may be relying on ITIA audits and not conducting much of their own management assurance. Some organizations may be missing the value of management assurance that could help them report more fully on key risk areas. If ITIA rely more on other assurance sources it could help direct scarce ITIA resources onto other risk areas. But the recipients of management and ITIA assurance are different. ITIA audits report ultimately through to the Board, whereas management's assurance reports up to Executive Management. These lines must be preserved. That should not stop ITIA acting as a catalyst to achieve an integrated approach to assurance in their organizations. Then a cohesive picture of the organization's stance on risks is available to both the Board and Executive Management. And both ITIA and management can optimize and where possible share their scarce resources. As we saw earlier in our survey report, skilled personnel are scarce. So, as part of the budget agreement, organizations should be led by ITIA in tackling the opportunity for integrated assurance.

Since most ITIA organizations do not draw on IPA and 40 percent have no program assurance activities planned it is likely that they rarely consider they have a shortage of skills in this area. Indeed, only 4 percent of respondents reported such a talent gap.

Qualifications relevant to IPA are not prioritized in recruitment, according to survey respondents. This is not necessarily a significant drawback. Although these qualifications are useful, they are not a substitute for employing practitioners with experience in project and program delivery. When such skills are missing in-house, the best option is to draw on the experience of third parties as a means of independently assessing IT projects and programs.

An independent program assurance function will help mitigate the risk of program or project failure.

[1] The Creative CIO, The Harvey Nash/KPMG CIO Survey 2016

KPMG's Global Enterprise Transformation Tool (GETT)

Used to define the approach and workplan for the IPA

Out of scope for initial review

In scope for initial review

Sources of assurance over key risks

Conclusion

This report has examined the fast-growing array of IT risks and highlighted the need for ITIA to meet the challenge by calling for more resources and tools, where needed. Overall, this entails developing an ITIA strategy that judiciously combines training, IT investment, outsourcing and co-sourcing in a way that is aligned with the organization's overall strategy — not just for today, but next year and the year after. This strategy would consist of the following three main points.

— It is imperative for ITIA to address emerging risks, as the business continues to seize the commercial opportunities of new technology and hackers find new ways to penetrate organizational defenses. ITIA stands to benefit from automation and D&A to make its work more efficient and insightful. But the problem remains that budgets, staff skills and delivery models are not adequate to assess emerging risks, if ITIA remains stuck inside its comfort zone of assuring core operations risk.

— ITIA must present a compelling and coherent business case to senior management and the board to support investment that address skills shortages, the need for continuous monitoring and assurance, and for new delivery models. This requires highly developed communication skills that avoid appearing to 'cry wolf', while presenting a prioritized set of resource requirements.

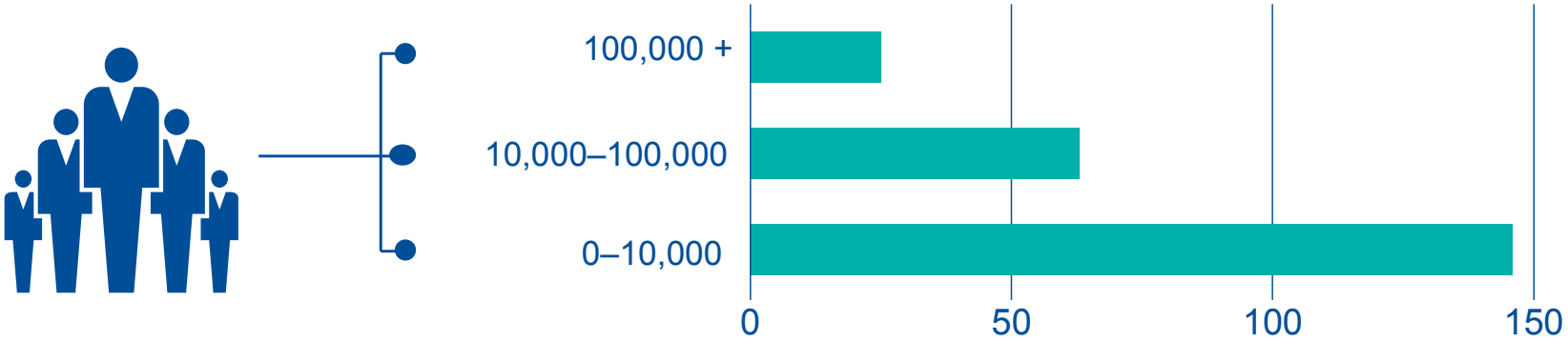
— ITIA must play a key role in aligning all sources of assurance to risk, relying increasingly on these sources to optimize their own ITIA program. The sources of assurance are on the front lines, across all relevant functions and at each level of the organization. The relevant standards must be set and then checked to ensure the controls meet the standards. Ultimately, these steps create a risk-aware organization. Everybody from the board and senior management to the bottom rung knows their roles and responsibilities in managing risk, while operating within an efficient and effective framework designed with the help of ITIA.

> ITIA must present a compelling and coherent business case to senior management and the Board to support requests for increases in the ITIA budget.

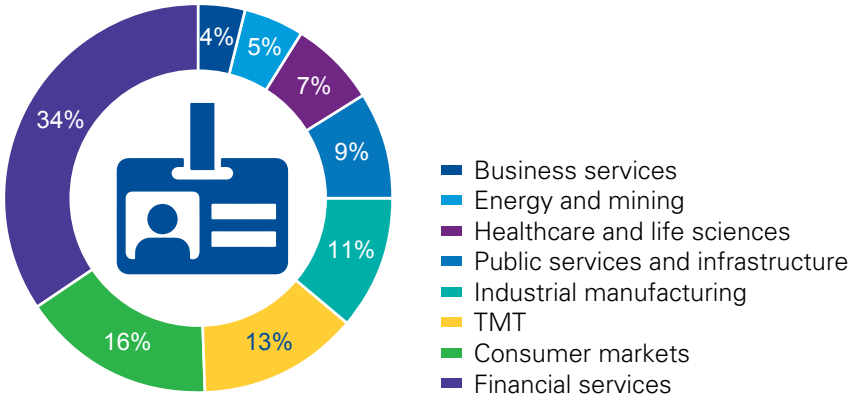
Survey demographics

Number of employees

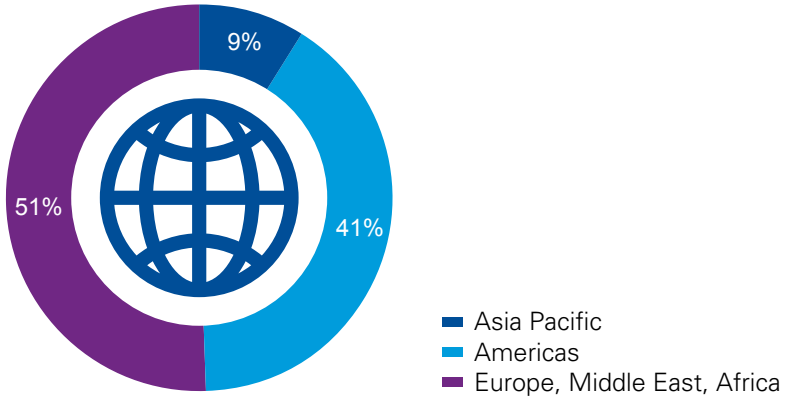
250 organizations in total



Operating in 8 sectors



Located in 3 regions



Source: IT Internal Audit: Multiplying risks amid scarce resources, KPMG International, 2017

Contacts

KPMG d.o.o. Beograd
Kraljice Natalije 11
11000 Belgrade
Serbia
www.kpmg.com/rs
E: itadvisory@kpmg.rs

Dušan Tomić
Partner, Head of Financial Institutions & Services
E: dtomic@kpmg.com
T: +381 11 20 50 521
M: +381 60 20 55 521

Nebojša Janković
Manager, IT Advisory
E: njankovic@kpmg.com
T: +381 11 20 50 603
M: +381 60 20 55 603

kpmg.com/socialmedia

Designed by Evalueserve.

Publication name: IT Internal Audit: Multiplying risks and scarce resources

Publication number: 134524-G

Publication date: July 2017