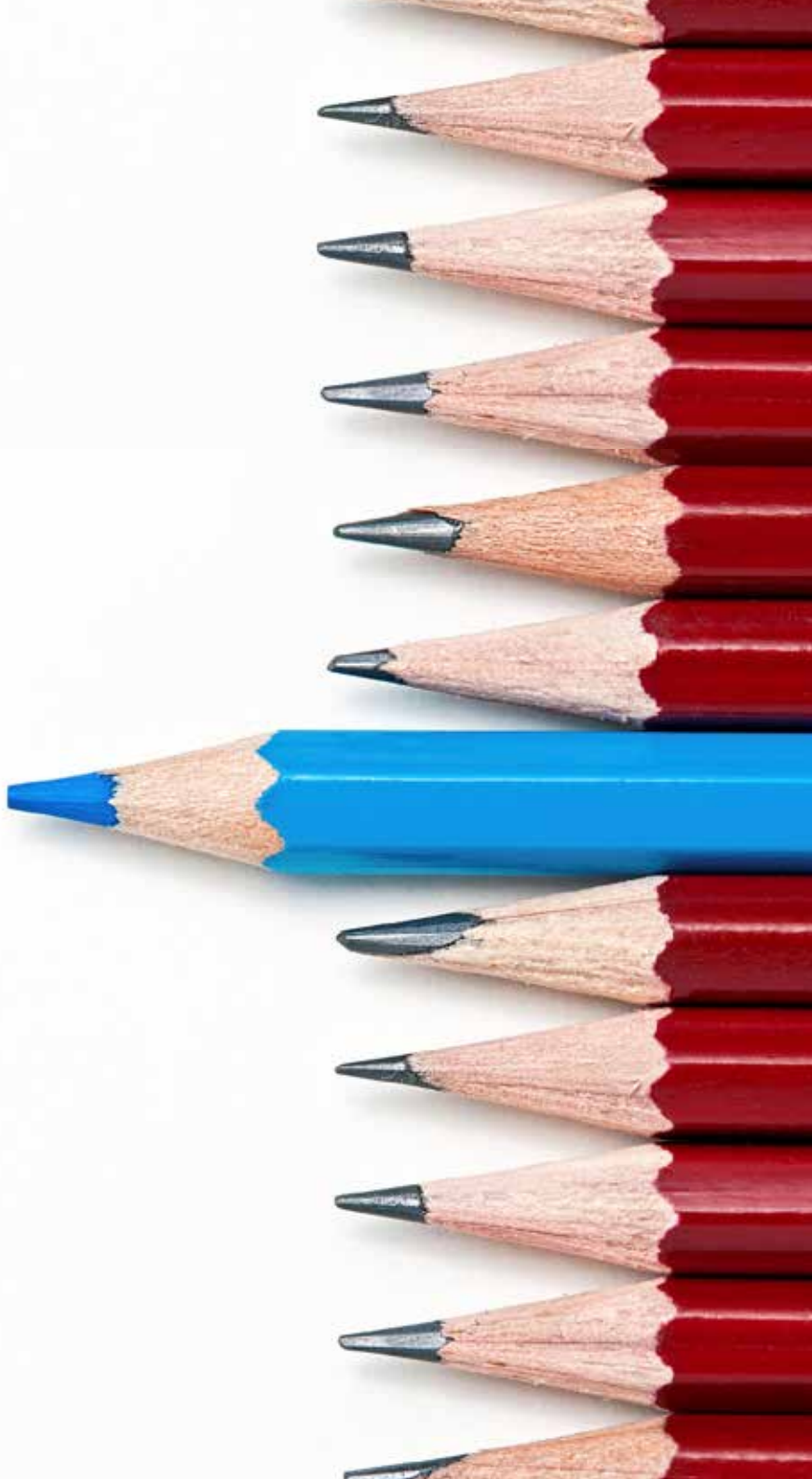
KPMG

IT Internal Audit Annual Conference Report 2015



Contents

Introduction

Andrew Shefford, Managing Director, IT Internal Audit, KPMG

As business risks proliferate, internal audit continues to be as crucial to the safeguarding of corporate reputations as ever. Within that, IT internal audit (ITIA) has probably never been more important. Technology has changed our world and the pace of change is only accelerating. These technologies bring new opportunities, but also new risks. We read almost weekly of cyber security incidents, which have claimed an ever-lengthening list of high profile casualties.

But it is by no means only a matter of cyber. KPMG's latest (2015) Technology Risk Radar[(1)], which analyses public domain reports of corporate technology issues, revealed that security incidents accounted for less than half of the total. Availability and quality issues each represented around a quarter of reported events.

Andrew Shefford, Managing Director

The complex interplay of relationships and dependencies that technology is creating mean that risk can come at an organisation from almost any angle – and the IT internal audit community needs to position itself as a primary influence on those that manage and mitigate risk.

All of this meant that there was a packed agenda at our fifth annual IT internal audit conference at the end of November 2015. Conference heard from a range of speakers across key issues including:

- The Audit Committee's perspective
- The cyber war – both attack and defence
- The data analytics opportunity
- The ITIA 'skills gap'

I hope you will find our report illuminating and thought-provoking as you seek to meet the rising demands that businesses are placing on their ITIA teams.

Note: (1) https://home.kpmg.com/content/dam/kpmg/pdf/2015/03/tech-risk-radar-second-edition.pdf
http://www.kpmg.com/UK/en/IssuesAndInsights/ArticlesPublications/Documents/PDF/Market%20Sector/Technology/tech-risk-radar-second-edition-corporates.pdf

What are Audit Committees looking for?

For IT internal auditors, the Audit Committee is clearly a key relationship. Whilst the Board needs to take ultimate responsibility for technology risk issues, the Audit Committee (and the Risk Committee if there is one) are prime players in providing risk oversight.

It therefore follows that ITIA needs to build strong ties with Audit Committees. But what, on their side, are Audit Committees looking for from ITIA?

Conference heard from Andy Pomfret, currently an Audit Committee Chair who holds several other non-executive positions and has previously been CEO of Rathbones and CFO at Kleinwort Benson Investment Management in a career in the City spanning some 30 years.

Andy set out key ways in which ITIA can interact with Audit Committees so as to develop a fruitful mutual relationship.

1. Education and awareness

Firstly, and fundamentally, it's a question of education. "Audit Committees and non-execs are quite capable of understanding technology risk issues," Andy said. "There are some very good non-execs out there and they want to learn – but they are all incredibly time-constrained. So it's really down to internal audit to find ways of educating them about the risks."

Technology risk may be rising up Boards' agendas – as was borne out by a show of hands at the conference in which the vast majority agreed this was the case – but there remains much more to do.

Andy cited a report* from the US-based Institute of Internal Auditors Research Foundation which found that two thirds of internal auditors surveyed agreed that Boards' awareness of cyber security risks had risen in the last couple of years. However, only 14% of Boards were actively involved in looking at cyber risks, whereas 58% of survey respondents thought they should be. "That's a huge gap," Andy observed. "It shows that education is absolutely key."

In an age where so many businesses are reliant on technology, it is perhaps a surprise that almost no Boards have a Chief Technology Officer on them.

"I would love to see a CTO on a Board or an Audit Committee," Andy said. "That said, some would not feel very comfortable sitting on one, or add much value. You've got to get the right individual, especially one who can present technology issues in a way that the Committee understands."

2. Short, medium and long term risks

Another key way in which ITIA can work with Audit Committees effectively is to break down the risks it presents to them into short, medium and long term elements.

Inevitably, short term risks will dominate. Issues around such areas as encryption of data, security of customer and client information, password security, and fraud in general, naturally loom large in Audit Committee discussions. "These risks are the stuff straight out of IA reports and are discussed day in, day out at Audit Committees around the country," Andy said.

However, there is less focus on medium and long term issues – with short term issues in danger of getting too much attention. "On cyber for example, all the headlines we keep seeing have done a lot to get Audit Committees worried and there is continual discussion around data security and hacking," Andy commented. "But the amount of attention these issues receive is perhaps to the detriment of other things. Longer term, strategic issues such as Blockchain for example could be even more threatening. Sometimes, Committees are just not looking far enough ahead."

ITIA needs to work hard to ensure medium term issues – such as projects to replace legacy IT systems - or longer timeframe industry issues like Blockchain (the underlying technology used by Bitcoin) have their place on the agenda alongside pressing short term items.

Note: *Institute of Internal Auditors Research Foundation (IIARF) – 'Cyber Security: What the board of directors needs to ask' © 2014

3. Offer alternatives

It is not enough, however, for ITIA to simply flag issues up. To really add value, they need to be suggesting some options too.

"It's all very well to talk about only being the third line of defence and that it's not IA's job to find solutions – but they've got to be doing more than that," Andy suggested. "They need to really help Audit Committees and be creative around alternatives to mitigate some of the issues that they're presenting."

4. Get a NED onside

It's all very well to flag up issues – but are they actually getting airtime at Audit Committee meetings?

All too often, IA issues are placed towards the end of the agenda and, as the meeting inevitably overruns through the sheer weight of discussion items, end up being squeezed into a few unsatisfactory minutes right at the end of the meeting. This is why it's crucial for IA to build relationships with Audit Committee members – preferably the Chair – so as to ensure that internal audit issues are given due prominence on the agenda.

"In one of my previous roles, I instituted a monthly catch-up between myself as Audit Committee chair and internal audit – and it proved incredibly useful," Andy said. "You don't even need a formal agenda, it's just an opportunity to talk and air issues. But IA shouldn't wait to be approached by someone on the Audit Committee – take the initiative and approach them."

A show of hands at conference found that there is more for ITIA to do here – only a minority said they have a monthly meeting with someone from the Audit Committee.

"It's about creating an ally on the Committee," Andy observed. "Some NEDs, quite correctly, are concerned about keeping the distance right, but I think a monthly conversation is fine. It's important for IA to find allies. Regulators, for example, can also be allies and can have the effect of raising certain issues up the agenda. Likewise, consultants can play an important role – they can help you benchmark yourselves against others. Audit Committees are often concerned because they're not sure how other organisations are approaching an issue, and consultants can provide some great insights here."

Cyber security – it's not Mission Impossible

Instances of high profile cyber attacks seem to be proliferating all the time. The risk is only increasing as several factors combine: attacker capabilities are growing; there are ever more resources available – often free or very low cost – on the public Internet (as well as the 'dark web'); the connectivity of devices is mushrooming through such concepts as the Internet of Things; the reliance on third parties and supply chains is growing; and cost pressures mean that most IT department resources are being reined in or reduced.

The result is what we might term a "readiness gap" in which the threat is increasing while companies' preparedness struggles to keep up.

And yet, clearly, it is a risk that every organisation quite simply must be armed against. Every institution needs to be able to detect and respond to the cyber security threat – and ITIA must be at the forefront of equipping the organisation in that battle.

So how can ITIA and other departments set about doing this? Thinking of the old adage "know your enemy", it can be extremely instructive to put yourself in the shoes of the cyber attacker – to understand how they work and what they are looking for.

KPMG

How hackers work: In the red corner

If you accept the premise that "you are under attack", then of course one of the first questions is – from whom?

So perhaps the first step is to think about the different types of cyber attacker out there, and which one(s) are most relevant for your organisation.

The main classes of attacker can be grouped as: criminal gangs (most interested in financial fraud in order to make a profit), hacktivists (perhaps motivated by an issue or cause), corporate competitors (looking to steal secrets or data), nation states (with similar aims), and disgruntled employees (often overlooked, but a potent threat as they often understand your systems and protocols).

Having thought about which group or groups you are most likely to be under threat from, ask yourself this: what are they likely to be targeting? Quite simply, what are your 'crown jewels'? What data or information do you hold that is most likely to be attractive to outsiders?

Then, put yourself in the shoes of your likely attacker, who is after your crown jewel of X – and consider: how are they likely to go about it? Even if your conclusion would be "no one is interested in us really", remember that cyber criminals cast a wide and automated net that could infect your systems with destructive malware.

Organised and systematic

One key thing to appreciate right from the outset is that cyber attackers are highly organised. It is their business after all. So they are likely to invest quite some time researching your organisation, its security posture, systems and employees. This could include researching individuals, perhaps via LinkedIn and other social media – who reports to whom, who has recently been hired, what linkages and dependencies are there between individuals and departments?

They will also be able to use publicly available search engines through which they can identify potentially vulnerable corporate devices, and exchange information with other groups of attackers. Tools available, such as open-source intelligence and forensics applications, enable them to then collate and analyse the huge amounts of data they have collected – the Big Data of hacking perhaps.

An attacker may also survey your physical premises, looking at access points to the building, how many people come in and out at what times of day and, crucially, what security pass system you have. They may be able to take a photo of or scan a staff or visitor pass and use it to print a fake one of their own. Don't overlook the physical threat – gaining access to your premises could be a quick way to gain access to your data.

Gaining access

Once the hacker has done their research and established their target, they will make a plan around how to reach it. Essentially, they will be looking to establish a virtual foothold within your organisation as a first base.

Likely methods of gaining this foothold include sending phishing emails to members of staff with links that have malware embedded or attached, or setting up a 'watering hole' – finding a site that is commonly used by staff and compromising it by embedding malware there.

Once they have tricked some victims, they can then digitally "move around" within your organisation and try to reach their target.

How to defend: In the blue corner

Having considered things from the attacker's point of view, you need to focus on shoring up your defences.

Just as for attackers, it's crucial to know your 'crown jewels'. What are they, and where are they located? Thinking about what it is you are defending also means thinking about the dependencies: what do your systems rely on, have you given copies to anyone externally or in the cloud?

Defending is essentially attacking in reverse – so map out possible routes of attack as a planning tool (known as creating an 'attack tree') and make a matrix of actions to defend against them. It helps here to think of the "five D's":

Detect, Deny, Disrupt, Degrade, Deceive

Deceiving could mean the creation of 'honeypots' – false targets (such as apparently vulnerable devices or applications) designed to lure attackers in to identify and catch them. Some organisations set up fake executive profiles on LinkedIn to get an early indication.

Pre-requisites

There are certain pre-requisites for a successful defence strategy.

You will need to be determined and have a resolve to win: winning the battle is not for the faint-hearted.

You will need to be able to capture all of your data in order to analyse and learn from it.

In the same vein, you will need to build a knowledge base – logging phishing emails for example, creating a database that you can interrogate and analyse.

It's vital of course to have the necessary in-house skills – a capable cyber security team, and perhaps the services of outside consultants who can be called in as and when necessary.

And finally, there is no getting around the fact that you will need to make the right amount of investment in order to do all of this – which means that getting the Board on side is essential.

Testing, testing, testing

Having done all of this, it's critical to put it into practice. Test your systems through drills and realistic attack simulations.

This may involve hiring a 'red team' of external attackers (such as from KPMG or another consultant) to put your systems through the mill and identify weaknesses and areas of priority – while your 'blue team' of defenders seeks to repel the attacks.

If you don't test your defences, then to a large degree you are simply closing your eyes and hoping.

But putting them into action will open your eyes as to where you really are and what you need to address – giving you the confidence that dealing with the cyber threat is not, after all, a case of 'Mission Impossible'.

Data analytics – where are you on the journey?

As technological capabilities continue to develop at pace, there's no doubt that data analytics (D&A) has become increasingly widely adopted across business areas.

A survey from KPMG published in 2015 – Going Beyond the Data[(a)] – showed that, from management's perspective, D&A has really entered the mainstream. Feedback from over 800 senior executives indicated that D&A was being used to manage risk in nearly every case, and was also prevalent across a whole series of other areas including financial management and Human Resources.

Another survey by KPMG found that D&A has entered the top 10 key focus areas for internal audit[(b)] – albeit only squeezing it at number nine. Other issues such as cyber security, regulatory compliance and anti-bribery ranked further up the chain – but when you consider that D&A is not just a focus area in itself but a capability that can support all of the other areas, its potential to become a powerful tool for the Internal Audit profession is clear.

How relevant is data analytics for Internal Audit?

1. Cybersecurity
2. Regulatory compliance
3. Antibribery/Anticorruption
4. International operations
5. Third-party relationships
6. Mergers, acquisitions and divestitures
7. Strategic alignment
8. Integrated and continuous risk assessment
9. Data analytics and continuous auditing
10. Talent recruitment and retention

But data analytics is not just a focus area itself, it is also a capability that can support all of the other 9 areas!

Note: (a) http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/going-beyond-the-data-turning-v1.pdf
(b) https://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/top-10-considerations-internal-audit-2015.pdf

KPMG

External audit powered by D&A

It may be helpful to look at IA's cousin, the external audit, where D&A has begun to make a deep impact. Increased data analytics, integrated with controls work, is bringing broader forward-looking insights and introducing automation that focuses procedures on key areas of risk.

For example, KPMG in the UK has cutting edge D&A capability that produces interactive dashboards for key transactional data such as cost of sale and revenue. A centralised approach means that for global clients operating in countries across the world, all data can be analysed centrally, potentially offshored. Smaller companies can reap the benefits too. For example, in one member firm smaller client who had an issue matching purchase invoices, KPMG's D&A tools were able to help, reducing risk and saving the client the equivalent of one FTE (full time equivalent).

KPMG in the UK has extended its capability further to cover high risk judgemental areas through its alliance with McLaren. For instance, KPMG and McLaren have developed an audit impairment tool that enables users to view the historical accuracy of management's forecasts, benchmark data, see the effects of assumption changes and export the results in a visual dynamic format.

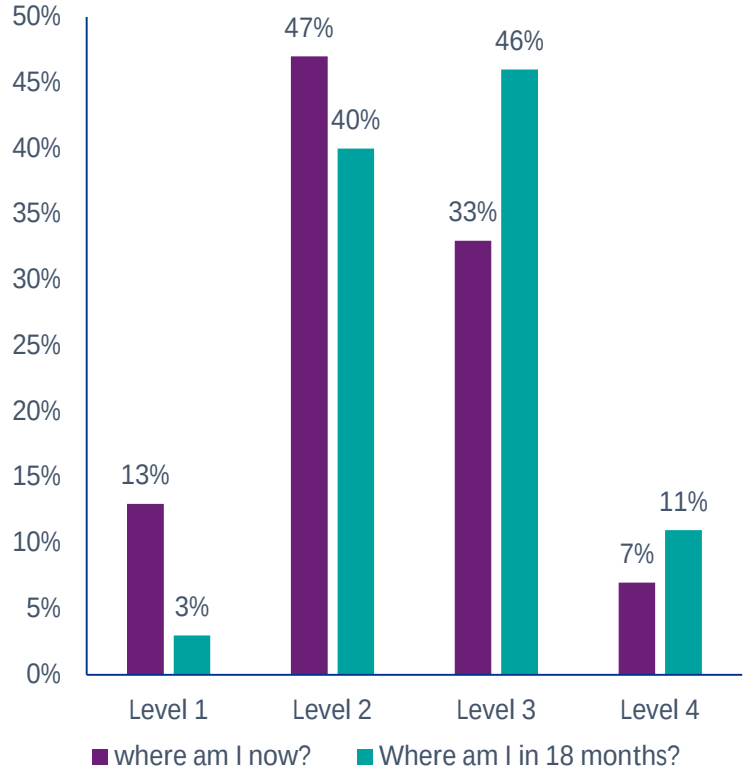
With more tools to come – which could be for anything from bad debt to estimating something as specific as oil rig decommissioning costs - there's no doubt that D&A has become central to the future of the external audit.

Can internal audit catch up?

With so much happening around D&A in the external audit, internal audit surely needs to do more to keep pace. Conference was asked to consider a number of questions to assess D&A maturity:

- Are you participating in conversations about using a single D&A capability across all three lines of defence?
- Are you providing assurance over the reliability of D&A systems developed by management?
- Are you clear on how IA can benefit from D&A?

When presented with a D&A maturity framework for internal audit consisting of four levels, a show of hands amongst delegates revealed that confidence around D&A is low. The majority of delegates hoped to move their IA function to either Level 2 or 3 within the next eighteen months.



Percentage of respondents by average maturity level

Developing the roadmap

So how can IA get there? Clearly, it's a journey that will take time: it can't be done overnight. For most, it will be a case of mapping out the vision first – beginning with the end in mind. It's important to be able to rigorously think through your goals and be able to articulate them very specifically, or there is a danger that you will end up with something that is not quite what you were aiming for – which could be both a frustration and a somewhat wasted investment.

Once your end-goals are clear, develop your roadmap to get there – remembering that it will be an evolution, process by process and business unit by business unit. After all, it's inherent to D&A that your requirements get clearer once you start analysing the actual data.

One critical component in the journey is to realise that D&A is not just about knowing how to use a technical tool. It's a skill as well, knowing how to scope the requirements and how to use the results. In the same vein, upgrading your D&A capabilities is as much about project management, stakeholder management and people development as it is about a technical implementation programme.

There are sure to be many challenges along the way. Dealing with a dynamic IT landscape with mixed maturity; integrating with business analytics and continuous control monitoring systems; data security issues; managing stakeholder expectations; alignment between the three lines of defence…there are plenty of aspects to juggle.

But for those that can move their IA function to a more D&A enabled footprint, the benefits will be great. A demonstration at the conference of tools available right now showed how D&A can help with real-time analysis across multiple issues including accounts payable, invoices, sales orders, credit risk, stock levels – all of it exportable into commonly distributable formats such as in spreadsheets.

Like the best journeys, the D&A transformation should certainly be worth it once you get there.

Speaker's Corner

Ensuring you have the right skills in the ITIA team – and getting the right mix between in-house and outsourced or co-sourced resources – is a key challenge in the industry. This is made all the more pressing by the rapid and indeed relentless development of new digital technologies, cloud-based solutions and mobile applications. A show of hands at conference indicated that at least half of delegates were concerned about skills gaps.

We asked a selection of Industry experts to speak to delegates about the issues they face and ways of bridging the gap. This is what they had to say:

Chris Wobschall, Group Chief Internal Auditor (HM Treasury and DECC)

For us, we need to think about what IT resources we keep in-house and what we co-source. We have seven firms on a contractor framework who we can draw on. In-house, it's about being an intelligent client business partner – we need people who understand the big picture and have strong relationship skills. We need people who are brave enough to speak to our client businesses, assess what the risk is at a point in time and make decisions about what actions we need to instigate. It's at the technical detail level – new developments around cyber for example, breaking technology trends – that we need to co-source. Given all the technology developments of the last decade, we do need more IT specialists – but even so I do wonder whether it is healthy for someone to be 100% an IT specialist only.

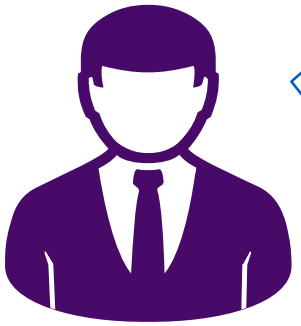
Outsourcing is less favoured than co-sourcing in FS, which is the opposite of what we see outside of FS.

Chris Gumn, Partner, KPMG

What we've found amongst our clients is that there are certainly challenges around recruitment and a shortage of graduates – the Big Four in the UK have also reduced their Internal Audit graduate intake in recent years, which has a knock-on effect. More broadly, analysing(1) a cross-section of KPMG clients we found that, overall, investment in IA in financial services has increased slightly while in other sectors it has slightly decreased. This may be because in non-FS sectors, companies are managing to create greater efficiencies through D&A where tooling is becoming more mature for ERP platforms. There is less use of D&A in FS because they rely on more specialist and bespoke systems. We expected to find an increase in focus amongst IA teams on emerging tech risks such as social media and the cloud – but in fact found an increased focus on more traditional areas. Emerging tech risk is still embryonic – indicating that IA needs to catch up here. Of course, this only increases the need to get the resourcing right.

Note: (1) KPMG analysis conducted in November 2015

In non-FS ITIA we see that the focus is on a wider variety of risks than in the FS area.



Daniel Flynn, Manager, ITIA recruitment, Barclay Simpson

As ITIA recruitment specialists, we've been analysing the market for over 25 years now. What we've seen this year is a continuation of the trend that there are two highly distinct markets: the London banking market, and everything else! Two thirds of vacancies this year have been in London and over 70% have been in financial services. The seniority of roles is rising as organisations seek people with greater specialisms who are able to deal credibly with senior stakeholders. Only around a third of positions are for generalists – we're seeing an increase in the need for specialists such as data analytics or security. There is huge competition for talent. Very few companies are training graduates from scratch and it's hard to find people with the desired experience (usually, 4 years plus). Some companies aren't helping themselves by being quite slow and traditional in their recruitment while more agile competitors will make offers more quickly and get in first.

Only one third of ITIA vacancies are for generalist roles and only one third of roles are outside of London

Justin Mycroft, Head of IT Internal Audit, SABMiller

Over the last five years or so, we've moved from a pure outsourcing model to more of a co-sourcing arrangement. We use KPMG as our co-source provider. But as the pressure is always there to do more for less, we have to look at ways of building capacity internally too. One thing I have started to do is make more use of financial internal audit teams. A lot of ITIA actually comes down to doing process reviews – which financial auditors are naturally very strong at. If you start them off doing some straightforward process reviews, it builds their confidence whilst at the same time they build the relationship with the IT team. It demystifies ITIA. There are some areas though where I wouldn't use an internal team – penetration testing for example. There wouldn't be enough regular work for an internal team, so that's one area where I use co-sourcing. It's a mixture of approaches to bridge the gap.

Mind the Skills Gap

Picking up the themes from the speakers, a panel session was convened to discuss what, if ITIA is facing increasing scope with static or falling resources, the way forward may be?

One panellist said "We're facing increasing challenges as the business becomes more digital and reliance on technology grows. We're also being more challenged by the Audit Committee, the business at large, and regulators. We need to find people that can keep pace with technology and who, crucially, can speak credibly about complex issues in a way that our business stakeholders can understand and engage with. Do you go for young people versed in technology or more old school technologists with more experience? Certainly, we need people who can think differently about the issues. It's not just a case of 'prevent and detect' these days but it's about responding too. It's very competitive – we're all fighting for the same resources. We also co-source from the firms on a case by case basis. We need to appeal to a wider talent base and convince them about the career path we can offer."

They were clear that it's sometimes about prioritising work and even turning some projects down. "We've got to be firm about what we want to look at," he said. "We've also got to find the most cost effective way of doing things – outsourcing process reviews, for example, to colleagues in lower cost regions, for example India."

For Justin Mycroft of SABMiller, an important aspect of ITIA's work now involves collaboration and delegation. "On data analytics, for example, other parts of the business such as Marketing are also active – so it's about finding out what they're doing and what we can re-use." On very technical issues, meanwhile, it's more about leveraging other investments from the IT function. "It's about getting a bigger team without paying for it!" Justin quipped.

Linking up more effectively with other functions was an approach stressed by Chris Gumn of KPMG. "You need to look at the whole risk universe. If external audit are doing more with D&A, that could enable some of their tools to be leveraged more easily by IA," he said. "It's about reducing duplication, breaking down silos and cutting the cloth better."

Tackling the skills challenge is also a question of addressing the image of ITIA. In the public sector, Chris Wobschall of Government Internal Audit acknowledged the challenge of attracting talent in an environment of low-growth or static pay. "It's about developing the brand. The Treasury for example has a very strong brand and attracts a lot of high fliers. That's something we would like to extend to the internal audit agency too."

The panellists were universally agreed that the profession needs people who can communicate clearly with a non-technical audience and "translate technology into English". But where will they come from? Daniel Flynn underlined how the profession must manage to reach young, technically literate people who "simply don't know that ITIA is an available career path."

Another panellist commented: "We've got to think laterally about the people we bring in and reach alternative pools of talent."

However, it can't be about just bringing in more IT-skilled people at the expense of others. "We need incremental, not substitutional change," as Chris Wobschall put it.

In the meantime, ITIA can help itself by ensuring its efforts are as effectively targeted as they can be. As Chris Gumn observed: "If ITIA is focusing on the right risks, the ones that really matter, then that could go a long way to freeing up resources."

Should ITIA be discouraged by the prevalence of the skills gap? Certainly, it is an issue that needs addressing and which does not have a quick fix solution. However, getting an effective and flexible resourcing model in place can go a long way to easing the problem.

There is also much that ITIA can do to help itself by operating more smartly in other areas, as we heard during the conference.

Getting the right relationship in place with the Audit Committee and individual non-execs means that IA issues should get the attention they deserve and the requisite management backing.

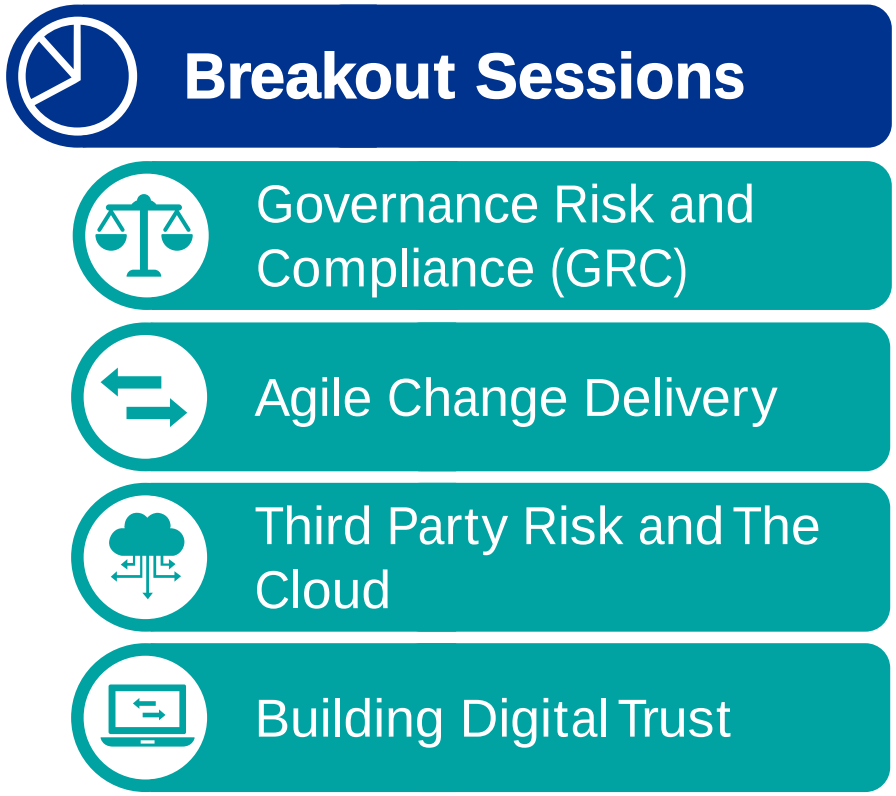
Greater use of D&A tools has significant potential to produce faster and more granular analysis – at a lower investment of man hours too.

While mounting an effective cyber security strategy will not only bring greater business resilience but could enhance the standing of internal audit within the organisation as a whole.

In short, if there are plenty of issues to be challenged by, there are also plenty of reasons for ITIA to look to the future with confidence.

Breakout Sessions

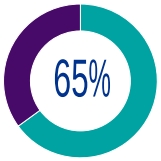
Delegates were given an opportunity to take part in one of four break-out sessions during the Conference. Each offered insights from KPMG experts into hot topics.



Governance Risk and Compliance (GRC)

More and more businesses across all sectors are assessing, implementing, extending or enhancing GRC tools and as with any change or key control process, internal audit need to be involved. The drivers for GRC can be regulatory (particularly in financial services and life sciences), an increasing need for transparency of risks, management's desire to urgently address audit weaknesses identified and, now more than ever, risk is on the CEO's agenda:

— 65% think risk management investments and disciplines are falling behind



— By 2020, more than 70% of companies (up from 25% today) will fully integrate IT risk management into an enterprise/operational risk management program

The potential benefits of a successful GRC project include:

— continuous controls, monitoring enhanced performance;
— major IT disruptions were avoided;
— risks anticipated, managed, predicted and reported;
— complete transparency and visibility of risks; and
— cost of compliance was reduced.

GRC can be very confusing! The scope of GRC is broad, GRC means different things to different people and there are a vast array of GRC tools in the marketplace across a number of different functional areas. Auditors have governance, risk and controls in their DNA and therefore need to be able to "see through the fog" and are expected to play a major part in helping the organisation improve.

Like any project, the earlier internal audit are involved in GRC initiatives the better. Internal audit can help shape the business case, enrich the benefits, check that issues raised in audits are addressed, validate progress and assess whether GRC benefits have been gained.

This session covered

— **What is GRC?**
An overview of GRC, a quick look at KPMG's GRC framework, what the main tools are in the market place.
— **Where is it heading?**
Key trend, including integration, data analytics, direction of tool providers and a view from GRC "gurus".
— **How do you use it to gain assurance?**
How to approach auditing GRC systems covering scoping, process, tool knowledge and reporting.

Agile Change Delivery

The objective of Agile is to satisfy the customer through early and continuous delivery of valuable software, to welcome changing requirements at any stage of development. In a corporate environment 'enterprise Agile' is referred to, indicating iterative methods which must dovetail into existing corporate control frameworks.

We covered

Agile change delivery methods introduces new risks to organisations. Accordingly programme assurance methods must be distinctly different to provide effective challenge in Agile environments:

- There is less emphasis on 'structural controls' such as the sign-off of Business Requirements;
- There is increased risk of 'scope creep' and of overruns if status reporting and planning controls are weak;
- Agile development places increased reliance on key managers (in both technical and business areas) and increases delivery risk if their experience and judgment is sub-optimal

As an emerging discipline, levels of knowledge, tools and understanding are frequently inconsistent and this increases risk, especially in organisations which swiftly introduce Agile into large/ complex change programmes.

Third Party Risk and The Cloud

There have been multiple high profile examples of failures of managing third party risks across all industry sectors which has resulted in the reputational loss, loss of consumer confidence in the products, monetary loss and regulatory scrutiny. This is a hot topic in the UK financial services sector due to huge regulatory pressure.

Many organisations have a limited perspective of how their supplier related risks impact on the end customer. In the Financial Services sector, the UK regulator has enforced monetary penalties in the form of 'capital charge' on a number of organisations who lack clarity on their outsourcing related risks. While businesses relationship with their third parties has evolved and become more complex, the governance and oversight hasn't.

We covered

In this breakout session we covered the evolving third party risk regime, with particular focus on:

— How the evolution of risk is changing the relationship with suppliers and managing the impact;

— The challenges being faced by organisations in relation to Third Party Risk Management;

— The leading monitoring practices observed in Financial Services and how other industries can learn from Financial Services.

Usage of cloud services is transforming the technology services industry and impacting all organisations. There are huge advantages in adopting cloud services i.e. reduction of costs, universal access, flexibility and high resilience. Despite the huge potential benefits, the adoption of cloud is being limited because of the risks it poses and lack of understanding of good controls.

For the large, more efficient organisations, confidence in the cloud is growing. In the past, cloud service providers were relatively secretive about what was happening – but today they're much more open about the types of controls they have and the reports they can provide companies with. Cloud computing also poses unique attributes and risks especially in the area of data integrity, recoverability and confidentiality, regulatory compliance, auditing and data offshoring.

Having a robust data strategy that can evaluate cloud service providers empirically is the key to mitigating these risks. That means understanding the value of information assets and the control you have over them.

We covered

In this session we looked at some of the challenges that organisations are facing in managing cloud service providers. In particular:

— What the challenges are that organisations face related to cloud computing;
— Building a robust data strategy to manage risks arising from cloud service providers;
— How to adopt a robust due-diligence process for cloud service providers;
— Leveraging cloud as a key delivery model for the evolution of IT in business innovation.

Building Digital Trust

Digital Trust is critical to the acquisition and retention of customers and shareholder value. This requires companies to focus on:

We covered

The challenges:

Zero Moment of Truth

Potential customers are choosing which businesses they use without directly interacting with those businesses – you need to be influencing consumers before their moment of truth

Personalisation

Customers expect their digital communication and interactions to be personalised – are you demonstrating that you know who your customers are

Feedback Culture

We make decisions based on the feedback provided by people we don't know and will never meet – the feedback customers provide on your digital services is critical

Regulatory Compliance

Regulatory failures are headline news, which directly impacts consumer trust, businesses need to comply with a broad range of existing and stay abreast of forthcoming technology and data protection legislation

Increased Expectations

Individuals are increasingly tech savvy and they have high expectations of the reliability, availability and user experience associated with the digital services they consume – many businesses are behind the curve

Delivered through:

Digital Risk Management

Establishing the mechanisms whereby you understand the risks associated with your use of digital and emerging technologies, to help you realise the benefits and avoid the pitfalls

Digital Architecture

The technological back bone of your digital services needs to effectively interface with your existing systems, processes and support arrangements, which is typically a complex undertaking.

Data Analytics

You need to effectively decipher data to provide you with a greater understanding of your customers, their preferences and ensure you provide them with the levels of personalisation they expect

Service Resilience

Preventing and responding to service disruption to minimise the impact to the digital customer experience is critical to ensuring confidence in your ability to deliver digital services.

Data Stewardship

You need to manage data assets appropriately to provide your business and consumers with high quality data that is easily accessible in a consistent manner.

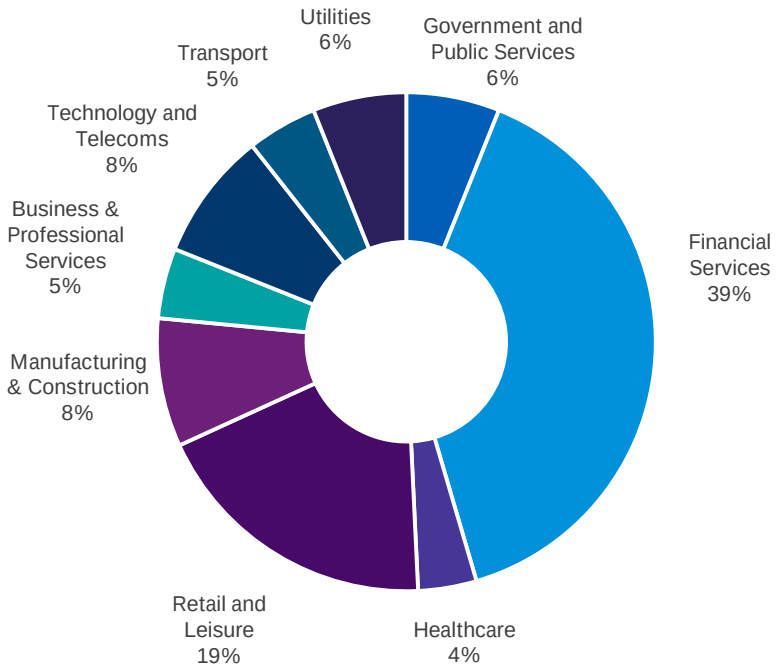
Security & Privacy

You need to understand the security risks and threats that impact your digital services and the protection of customer identity and data.

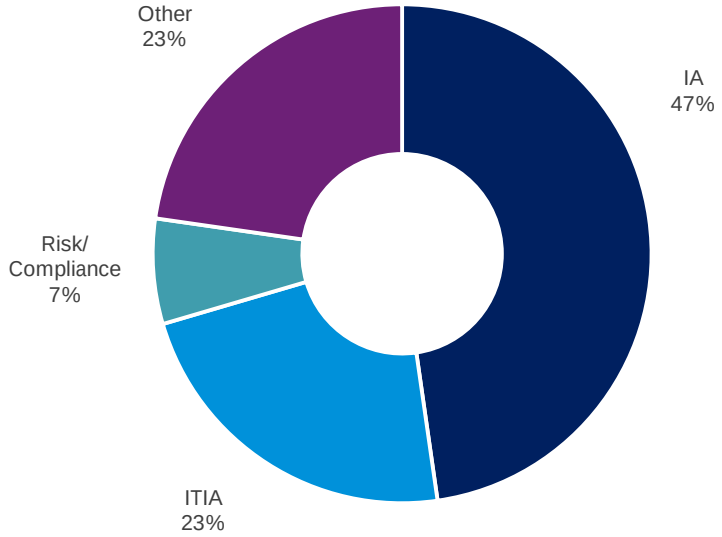
The Day in Numbers

This year's event was attended by delegates from the UK and beyond. There were over 130 attendees representing a diverse range of businesses:

Industry Representation



Role of Attendees



This report is based on KPMG's fifth annual IT Internal Audit conference held on 26 November 2015. Over 130 leaders in Internal Audit, IT Internal Audit and IT Risk took part in the Conference which included sessions on key areas they may need to address.

If you would like to be included in this network for future events, or would like any other information regarding KPMG's IT Internal Audit services, please use one of the contacts below:

Andrew Shefford
Head of IT Internal Audit and Head of Europe, Middle East and Africa IT Internal Audit Network
Mob: +44 7775 704 613
Email: Andrew.Shefford@KPMG.co.uk

Neil Osborne
Head of IT Internal Audit, Financial Services
Mob: +44 7920 290 226
Email: Neil.Osborne@KPMG.co.uk

Konrads Smelkovs
Cyber Defence Services
Mob: +44 7990 987 057
Email: Konrads.Smelkovs@KPMG.co.uk

Paul Holland
Director, Technology Risk and ERP Analytics Lead
Mob: +44 7786 703 405
Email: P.Holland@KPMG.co.uk

Chris Gumn
Head of Technology Risk
Mob: +44 7715 704 864
Email: Chris.Gumn@KPMG.co.uk

kpmg.com/socialmedia

kpmg.com/app

Designed by CREATE | CRT053397