Deloitte.

Planning ahead
Hot topics facing organisations in IT Internal Audit

2013

During Q4 2012, Deloitte surveyed Heads of IT Internal Audit at 22 global organisations to identify the key themes and topics which they see as their top IT risks for 2013.

Introduction

Welcome to the 2013 top 10 hot topics facing Heads of IT Internal audit.

In late 2012, Deloitte's UK practice performed a survey of 22 global Financial Services organisations to identify key themes and topics which they see as their top IT risks for 2013. It's been interesting to note that while rankings and priorities in the market in Australia may vary to some degree, the issues themselves have been relatively consistent. This is also true of what we have seen across industries outside FSI – the same issues, but some changing emphasis regarding priority.

'Third-Party Management' came in as the hottest topic for 2013, indicating greater acknowledgement of the increasing prevalence of outsourcing within institutions. It's not surprising this is high on the list of priorities in the FS Industry, who have long been considered market leaders in exploring the opportunities provided by increased globalisation and access to lower cost resources abroad. But it's a trend that has spread across many market segments, from telco's to utility companies, and is further evidence that digital disruption continues to be a game changer.

Third Party Management displaced 'Cyber Security' as the hottest topic for 2013 in the UK survey, but it is still very high on the agenda in Australia across a range of industries. Certainly, in terms of media attention, Cyber has dominated the press, and we've seen the flow on effect as it becomes a common topic for discussion at Board level, which has in turn driven increased attention and activity in IT risk management and audit functions.

Other notable changes in the survey included the continued rise of 'Data Governance & Quality', an area where institutions and regulators continue to focus; and 'Resilience', following both the recent consumer-impacting issues in UK Financial Services organisations which prompted censure by the regulators and natural disasters such as 'Superstorm Sandy' in the US. For Australia, there was a not unexpected spike in interest regarding Resilience in 2012, following the spate of natural disasters across the country. But the ongoing focus on Resilience in the current year has interestingly had ties to cyber security, as resilience and responsiveness to cyber attacks has begun to merge into broader business and IT resilience plans rather than being a stand alone security issue.

Finally, we see the entry of 'Cloud Computing' for the first time into the top 10 – perhaps a later addition to the top ten than we would have anticipated. Cloud has matured from an often ill-defined hype term to a genuine alternative to existing infrastructure and data management models. Organisations are using or considering adoption of cloud-based solutions, albeit with caution and often adopting in-house solutions at present. Even traditional late adopter industries like the public sector have begun to loosen the reins on considering these solutions, which has brought with it a renewed interest from a risk management perspective.

We hope you find the following information insightful, whereby we have set out the top 10 topics raised ranked in order of priority per the survey results.

Liz Brown
Partner

IT Internal Audit Hot Topics 2013

1. Third-Party Management (▲7)*

The use of third-party suppliers for some or even all IT and business operations within organisations is increasingly prevalent, as organisations look to focus on their core-business activity by increasing efficiency and reducing costs. Indeed, many organisations use third-party providers who in turn subcontract aspects of their services, creating a significant distance between the users and ultimate service providers. IT security continues to be the main risk for many organisations, with focus centring on the 'weakest link' in a control structure, which often lies with third-party suppliers. The relationship between the business, IT, Risk and Procurement is developing in this area, with significant focus on maturing risk assessments and reviewing processes across the organisation.

2. Identity & Access Management (▲3)

Access management remains a key focus area for organisations keen to avoid negative publicity associated with access breaches and fraudulent activities, as well as addressing the continued challenge of implementing effective segregation of duty controls. Internal Audit functions are increasingly expected to assess large and complex identity and access management systems and programmes, whilst also providing assurance on more traditional access provisioning and recertification processes. Untangling the matrix of system privileges and access rights can involve a significant amount of data analysis and we have seen mature Internal Audit functions in particular invest in access management tools and techniques to support their assurance activities.

3. Data Governance & Quality (▲1)

For organisations that process vast quantities of transactional data, they place huge reliance on the quality of their static data. Ensuring completeness and accuracy, appropriate restriction of access, and compliance with relevant regulatory requirements is of increased interest to executive management. Internal Audit functions have a role to play in assuring that the data is being governed appropriately and that the quality of data is fit for purpose. This is being reviewed at both a macro level, where certain organisations have significant programmes underway to address data quality top down, and through direct focus on individual audits. The use of data analytics, tools and techniques by Internal Audit to assess the quality of data is on the rise, albeit at a slow rate of progression.

4. Large Scale Change (▲2)

Large IT projects and a history of budget overruns, continue to elicit board-level attention, and this flows through the IT assurance function. We are also seeing an increase in the use of agile project development practices in contrast to the more traditional waterfall approach. Internal Audit functions are actively involved in providing assurance over change and project management activities and are engaging effectively with major IT change programmes to provide assurance that the required outcomes are being achieved. Given the widespread focus on cost cutting and implementing changes on time and within budget, the focus on release criteria and testing is becoming increasingly important.

5. Cyber Security (▼4)

The risks relating to the cyber security threat from 'hacktivists' continue to be a focus area, while attacks from state-sponsored hackers and organised crime are becoming increasingly sophisticated. A number of high profile cyber-attacks, which have caused financial and reputational damage to the organisations involved, have increased the profile of this issue at board level, as well as the government and regulatory bodies. Internal Audit has a significant role to play in assuring that the multi-layered people, process and technology controls in place can effectively prevent, detect and manage cyber-attacks. This is an area which received significant focus from Internal Audit functions in 2012, with many continuing to keep a 'watching brief' in 2013.

6. Resilience (▲New)

Recent natural and man-made disasters, along with business-impacting events across the globe, have increased corporate focus on business continuity and disaster recovery processes. Other high-profile system failures and outages have increased the pressure on businesses to consider resilience when changing or designing IT systems and processes – government departments are receiving similar levels of attention, such as from AGIMO. As a result, there has been an expectation on Internal Audit functions to provide assurance over the adequacy of resilience controls and processes and to promote awareness of resilience requirements across the organisation. The spate of natural disasters in recent years have challenged some of the previous norms around resiliency and location strategy.

7. Cloud Computing (▲New)

The use of cloud computing for remote data storage, along with the provision of software as a service and virtual desktop facilities, is increasing rapidly. This presents organisations with a challenge: balancing ease of access, time-to-market, flexibility and efficiency with concerns over data governance, security, availability and resilience. Internal Audit is being asked to assess cloud-based initiatives and to help provide assurance over the control structure. This includes managing and protecting the use of cloud computing solutions and assessing regulatory implications, such as the impact of cross-border data access restrictions. Although our findings suggest that this is the norm for some organisations, many are yet to adopt external clouds, instead electing to keep their cloud based solutions in-house.

8. Mobile Devices (▲2)

The proliferation of increasingly powerful smartphones and tablets has resulted in a significant increase in their use across organisations. In addition to being used as a customer channel through dedicated applications, they are also utilised as a mechanism for staff to access the corporate network, through initiatives such as 'Bring Your Own Device'. This, combined with nervousness around the security of such devices and the desire to maximise the availability of new technology, has increased IT Internal Audit's focus on ensuring that risks relating to the use of these devices are appropriately managed.

9. Complex Financial Modelling (▼7)

Regulatory changes require organisations subject to such regimes to develop and maintain complex financial data models. Internal Audit functions are required to provide detailed assurance over these models which highlights the need to nurture sophisticated data analysis skills as opposed to the more traditional 'black-box' approach. However, the sharp drop in priority that Internal Audit functions have placed on this topic reflects the higher level of attention this was given in previous years.

10. Social Media (▼1)

The growing adoption of social media by organisations to promote products and services has led to a greater need for control over social media interaction. In addition, the ability for consumers (and staff) to share their opinions about the organisation's products or services through social media channels has meant that, without an effective monitoring and communication strategy, the reputation and brand of a business can be rapidly undermined. Internal Audit functions are increasing their involvement in reviewing the steps taken by management to protect the organisation's reputation, whilst ensuring opportunities within social media are exploited and appropriately managed.

In addition to the top 10 noted above, other areas which were raised with reasonable frequency include:

• Effective implementation and use of GRC systems

• IT Governance

• Data Leakage Protection.

* The number in brackets indicates the movement since the 2012 survey.

Contacts

For enquiries relating to our IT Internal Audit services, please contact:

Sydney

Liz Brown
Partner – IT Assurance Product Lead
+61 2 9322 5372
ebrown@deloitte.com.au

Adam Barringer
Partner
+61 2 9322 5337
adbarringer@deloitte.com.au

Melbourne

George Stathos
Partner
+61 3 9671 6853
gstathos@deloitte.com.au

Brisbane

Craig Mitchell
Partner
+61 7 3308 7400
cmitchell@deloitte.com.au