



Planning ahead

Hot topics facing Financial Services organisations in IT Internal Audit



During Q4 2012, we surveyed Heads of IT Internal Audit at 22 global Financial Services 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 the Financial Services Industry.

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 the rankings and priorities in the market in Australia may vary to some degree, the issues themselves have been relatively consistent with what we've seen locally.

The promotion of 'Third-Party Management', which displaces 'Cyber Security' as the hottest topic for 2013 is the most notable change in rankings from the 2012 survey results, indicating a greater acknowledgement of the increased prevalence of outsourcing within institutions and the continued regulatory focus in this area.

Cyber still retains a significant spot in the top 10. 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 include 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. In Australia, we had a 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 just a stand alone security issue.

Finally, we see the entry of 'Cloud Computing' for the first time into the top 10. Many Financial Services organisations are using, or considering adoption of cloud-based solutions, albeit with caution and often adopting in-house solutions at present.

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 Financial Services 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 industry.



2. Identity & Access Management (▲3)

Access management remains a key focus area for Financial Services organisations keen to avoid negative publicity associated with access breaches and rogue trader 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 invest in access management tools and techniques to support their assurance activities.



3. Data Governance & Quality (▲1)

Financial Services organisations process vast quantities of transactional data and 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, especially given the spotlight on regulations such as Basel III and Solvency II. 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 institutions 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)

Regulatory programmes, such as FATCA, Recovery & Resolution Planning, Dodd-Frank and Solvency II, continue to elicit board-level attention and are driving significant levels of change in many Financial Services organisations, both in terms of the volume of change and the cost and size of the changes. 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 regulatory programmes to provide assurance that the required outcomes are being achieved. Given the volume of change now being undertaken across the industry, in addition to the focus on cost cutting and implementing these 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 FSA and other 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 led to regulators increasing the pressure on businesses to consider resilience when changing or designing IT systems and processes (including a 'Dear Chairman' letter from the FSA). 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. Events such as 'Superstorm Sandy' in the US in October 2012 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, are 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 Financial Services institutions. In addition to being used as a customer channel, through dedicated applications such as mobile banking, 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, such as Basel III and Solvency II, require organisations 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:

- High Frequency Trading
- Effective implementation and use of GRC systems
- Cash Payment Controls
- IT Governance
- Data Leakage Protection.

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

Contacts

For enquiries relating to this survey, please contact:

David Bettsworth

Partner

020 7007 8644

dbettesworth@deloitte.co.uk

Dan McDonough

Senior Manager

020 7007 9706

dmcdonough@deloitte.co.uk

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

Sydney



Liz Brown

Partner – Product Lead

61 2 9322 5372

ebrown@deloitte.com.au



Adam Barringer

Partner – FSI

+61 2 9322 5337

adbarringer@deloitte.com.au

Melbourne



George Stathos

Partner – FSI

+61 3 9671 6853

gstathos@deloitte.com.au

Brisbane



Craig Mitchell

Partner – FSI

+61 7 3308 7400

cmitchell@deloitte.com.au

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively the “Deloitte Network”) is, by means of this publication, rendering professional advice or services.

Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/au/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte has in the region of 200,000 professionals, all committed to becoming the standard of excellence.

About Deloitte Australia

In Australia, the member firm is the Australian partnership of Deloitte Touche Tohmatsu. As one of Australia’s leading professional services firms, Deloitte Touche Tohmatsu and its affiliates provide audit, tax, consulting, and financial advisory services through approximately 6,000 people across the country. Focused on the creation of value and growth, and known as an employer of choice for innovative human resources programs, we are dedicated to helping our clients and our people excel. For more information, please visit Deloitte’s web site at www.deloitte.com.au.

Liability limited by a scheme approved under Professional Standards Legislation.

Member of Deloitte Touche Tohmatsu Limited

© 2013 Deloitte Touche Tohmatsu.

EDC_984_04/12