Deloitte.

Under control
2015 Hot topics for IT internal audit in financial services

An Internal Audit viewpoint

Introduction

Welcome to our fourth annual review of the IT hot topics for IT internal audit in financial services. The survey was conducted in August and September 2014 through discussions with Heads of IT Internal Audit of UK financial services organisations.

This year internal audit priorities have shifted from the hot topics we identified in our 2014 results, although not as markedly as in previous years. Internal audit departments in the financial services industry continue to operate against a backdrop of heightened regulatory scrutiny, emerging best practices and increasing stakeholder expectations. Not surprisingly, this has resulted in a number of fundamental control areas featuring in this year's top-10 hot topics. The list of high profile items is led by 'Cyber Security' on the back of continued government initiated cyber exercises and board-level appreciation of the impact a breach can make. Similarly, 'Disaster Recovery and Resilience' has re-emerged as an important topic as organisations focus on minimising customer impacting system outages. For the first time, we see 'Enterprise Technology Architecture' emerge as a hot topic, which reflects the challenge many financial services organisations have with large legacy estates and complex architectural maintenance demands.

There was again a consistent theme of audit attention focused on 'Large Scale Change' which reflects the growing expectation for and recognition of the advantages from, proactive pre-implementation involvement of internal audit across the large change programmes. 'Information Security' remains in the top 5, underlining it as complex area which management find hard to address successfully and where internal audit often identify high-impact control weaknesses.

More broadly, we continue to see greater reliance on IT internal audit functions to support ever increasing analytics activity and to help assess data governance and data quality in support of broader business audit review.

We hope you find the top 10 topics, presented in priority order, a useful resource to help benchmark your own IT audit plans for 2015 against.

Mike Sobers
Partner

More broadly, we continue to see greater reliance on IT internal audit functions to support ever increasing analytics activity and to help assess data governance and data quality in support of broader business audit review.

IT Internal Audit Hot Topics: 2012-2015

The table compares the top-10 IT internal audit hot topics over the past four years as identified through our annual survey of Heads of IT Internal Audit in the financial services industry. It depicts some interesting trends across focus areas over time. The table also highlights the core, high-profile topics that have appeared consistently in the top-10 of IT internal audit functions.

Rank	2015	2014	2013	2012
1	**Cyber Security**	Large Scale Change	**Third-Party Management**	**Cyber Threat**
2	Disaster Recovery and Resilience	IT Governance and IT Risk Management	Identity and Access Management	Complex Financial Models
3	Large Scale Change	Identity & Access Management and Data Security	**Data Governance and Quality**	Data Leakage
4	Enterprise Technology Architecture	**Data Governance and Quality**	Large Scale Change	**Data Governance and Quality**
5	Information Security	**Third-Party Management**	**Cyber Security**	Rogue Trader and Access Segregation
6	**Third-Party Management**	**Cyber Security**	**Resilience**	Regulatory Programmes
7	Digital and Mobile Risk	Digital Risk	Cloud Computing	Financial Crime
8	**Data Management and Governance**	Service Management	Mobile Devices	**Third-Party Management**
9	IT Governance and IT Risk Management	**Disaster Recovery and Resilience**	Complex Financial Modelling	Social Media
10	Service Management	Cloud Computing	Social Media	Mobile Devices

IT Internal Audit Hot Topics 2015

1. **Cyber Security (▲ 6)**
   Cyber security remains high on the agenda for many organisations and this year was the most commonly reported topic that internal audit functions are looking to address in their plans for 2015. In our view, this is largely driven by increased appetite and awareness at board-level to ensure that cyber risks can be managed. Across financial services, board appetite has been influenced, at least in part, by the increased regulatory scrutiny and government-backed exercises to assess the readiness of firms to respond to cyber threats. In particular, an industry-wide ethical security test (CBEST), which aims to test the stability of the UK financial system has received board-level attention in many organisations leading internal audit functions to continue their focus on assessing the various layers of cyber defence, including intelligence and monitoring capabilities alongside processes to detect, prevent and importantly manage the impact of cyber-attacks. Many internal audit functions report they face a challenge in having the skill sets necessary to audit the 'in-depth' approaches which organisations are taking to address cyber risk.

2. **Disaster Recovery and Resilience (▲ 9)**
   High-profile system outages for high street banks and other firms across financial services have increased corporate and regulatory focus on disaster recovery processes and systems resilience. Despite "Dear Chairman" letters having been issued to financial services firms, outages impacting ATM and branch networks, payment systems and ultimately customer access to services continue to cause regulators and organisations to focus great attention on the stability of their systems. Internal audit recognises it has an important role in providing assurance over the adequacy of resilience controls and processes, the effectiveness of change controls and the maintenance programmes which firms have in place to keep their systems running (see topic 4). It is often a challenge for internal audit functions to assess resilience across their complex technology estates. However, whilst technology skills are at the heart of the disaster recovery (and indeed cyber) topics, internal audit functions increasingly find the impact of these reviews is significantly enhanced by engaging business stakeholders, in areas such as communications, public relations and crisis management.

Note. The number in brackets indicates the ranking of the topics in our 2014 survey

3. **Large Scale Change (▼ 1)**

Investment in change across financial services is significant with large capital, redress and control programmes being driven across all of the organisations we surveyed. As a result, internal audit functions are devoting substantially more time and resource than they have previously to providing assurance over the large-scale change in which their organisations are investing to meet regulatory demand and drive growth. We are seeing examples of up to 40% of the total audit plan effort being focused on change programme assurance. Given the high technological content of change programmes in areas such as Solvency II, Basel III, COREP and IFRS 9, IT specialists have a significant contribution to make to multi-disciplinary internal audit teams in delivering appropriate and robust challenge. Internal audit is increasingly expected to assess whether required outcomes are being achieved by large-scale change programmes, as well as whether programme governance controls are operating effectively. We have seen numerous examples whereby internal audit functions are providing the check and challenge on programme boards to help assure whether regulatory expectations and control requirements are being met as part of programme delivery. In our experience, many functions will need to develop their approaches and range of reporting tools to deliver flexible, timely assurance in these areas.

4. **Enterprise Technology Architecture (NEW)**

The complexity of the technology architectures typically in place across financial services may cause significant challenges for IT management, particularly post integration with other environments or where there is a high reliance on legacy systems. Legacy systems can pose a number of risks, such as security vulnerabilities, shortage of skills to manage and externally support the systems effectively, increased complexity caused by add-on interfaces to core systems and limited interoperability. Given these risks, there are clear linkages and cross-overs with the, previously highlighted, cyber-security and resilience hot topics which have increased the level of focus internal audit functions are placing on technology architecture. It is imperative that internal audit work closely with stakeholders in IT to understand the technology architecture and ensure they can achieve sufficient audit coverage of legacy platforms, interfaces and information flows. We are also seeing internal audit functions participate in programmes related to changes in the technology operating model allowing them to provide an early view and independent opinion on the suitability and viability of the target state.

5. **Information Security (▼ 3)**

Information and access management predictably continues to be a very important area of focus for organisations across financial services. The avoidance of unwelcome publicity, regulatory scrutiny and negative impact on customer sentiment has continued to drive the need to maintain robust controls over information security, be it personal data or corporate sensitive data. The scale of the IT estate, the volume of users, vast number of roles, disparate nature of data and the extensive use of third-parties makes managing access, maintaining segregation of duties and protecting data a major management challenge. Many organisations continue on the path to implement access management programmes with varying levels of success. Internal audit functions are continuing to review access provisioning and recertification processes thematically as well as during integrated reviews. We also see use of analytics playing its part as internal audit functions make increased use of available data to assess information security controls.

6. **Third-Party Management (= 6)**

For a third year running our survey demonstrates that management of third parties remains a key priority. Organisations' reliance on third parties to support key business processes has increased, as they seek to reduce costs, make efficiency gains or simply re-focus on core activities. Together with this, it is well understood that ultimate accountability for the services provided and the effectiveness of the control environment cannot be delegated or devolved, a point reinforced by the regulators in financial services. This is complicated when third parties are in turn using their own vendors, resulting in firms losing visibility or control over the entirety of the supply chain. The increased uptake of cloud computing services provided by specialised third-parties has amplified the concerns about key risks such as security and compliance. In most cases, internal audit teams are using multi-disciplinary teams to provide assurance over third-party due diligence practices, or perform ongoing monitoring to ensure both organisational policy and relevant regulatory standards are being complied with. We are also observing a focus on evaluating the vendors' approach to managing emerging risks as well as their responsiveness to control issues impacting their clients. We are starting to see some of the larger functions establishing dedicated third-party audit teams, electing to conduct third-party contract reviews for significant or high-risk vendor relationships.

7. **Digital and Mobile Risk (= 7)**

Customer demand for mobile apps is showing unprecedented levels and far exceeds uptake of traditional web based access to transactional services when originally launched. This demand has precipitated a surge in the number of digital and mobile services in the financial services industry and it is increasingly seen as an essential channel for organisations to engage with customers. Regulatory interest has been awakened into digital and mobile as a platform for customer engagement, influenced to a large extent by the high customer demand as mentioned above. In September 2014, the FCA published the results of its thematic review into Mobile Banking and Payments highlighting concerns over security of customer data and funds and whether technology is robust enough to cope with the change in customer behaviour. Internal audit functions are now including mobile apps in their audit plans, blending of specialisms on such reviews including IT, marketing, conduct and anti-fraud skill sets. We are not seeing, however, any significant internal audit focus on the risks relating to mobile devices as a corporate tool. Smartphones and tablets are internet connected devices with tremendous processing power that enable access to data assets and systems; they normally store confidential data and are in the hands of individuals who may lose them, share them or use them in ways that expose vulnerabilities to attackers (e.g. the use of Cloud services or untrusted third-party applications).

8. **Data Management and Governance (▼ 4)**

The volume of data in the digital universe has increased 9-fold in just 5 years, a significant component of which is generated by enterprises. *IDC's Digital Universe Study* predicts that in the next five years "data will grow by a factor of 8, while the pool of IT staff available to manage them will grow only slightly"[1]. Meanwhile, the cost of storing such vast amounts of data by organisations is continuously reducing. This leads to a substantial increase in organisational data assets while appropriate data oversight and monitoring efforts are not always keeping pace with the growth of data. New digital channels for customers and employees (such as mobile applications and social media) contribute to the data accumulation and fragmentation for both static and transactional data. Data governance remains a focal point for regulators in the financial services industry in particular, who require that firms assess the controls over data underpinning the calculation and reporting of capital, liquidity and risk. As such, we are seeing Audit functions being involved in thematic reviews of data governance, compliance with regulatory requirements as well as reviews of the data quality programmes themselves. Analytics capabilities (in-house or co-sourced) for the more mature of the functions allow the use of sophisticated data quality and profiling tools to assess data quality comprehensively and present results using visualisation techniques.

1 IDC's Digital Universe Study, "Extracting Value from Chaos"

9. IT Governance and IT Risk Management (▼ 2)

IT governance as an audit area remains a high priority for Heads of IT Internal Audit across financial services. Following the CIIA guidance *'Effective Internal Audit in the Financial Services Sector'*, internal audit functions are explicitly expected to voice their views on the transparency of decision making and effectiveness of governance practices. With respect to technology, recent systems failures that impacted retail banking customers brought added attention to IT governance practices in ensuring an optimal IT service delivery model and prioritised IT investments. Boards and Audit Committees are asking IT to answer questions such as:

– Is IT appropriately and efficiently managed to deliver business value whilst enabling the achievement of the corporate objectives?

– Are the associated risks to deliver the IT service, including major change effectively and sustainably managed?

Internal audit functions are being challenged to form an opinion regarding IT compliance and governance, including an assessment of alignment with business strategy, appropriate risk reporting to executive management and the Board, and the mechanisms to measure and track IT performance.

10. Service Management (▼ 8)

In addition to the focus on IT change, there is an equal requirement to ensure the quality of the day-to-day services provided by IT functions, as well as managing the wider relationships with their internal customers and users effectively. Extending the concept of IT delivering business value (as covered in Topic 9) the IT service management discipline focuses on adopting structured planning and robust financial control processes whilst maintaining customer-aligned operations. Budget control is indeed of particular concern to organisations and IT functions are under pressure to keep operational costs low ('keeping the lights on'), allowing the funding of innovative solutions and strategic change. Many internal audit functions are choosing to assess IT service management in their 2015 plans and this is closely linked to the need to provide assurance that service continuity can be maintained throughout incidents, outages or peak periods. Internal audit functions should seek to evaluate whether the service delivery lifecycle is governed by appropriate structure and controls to drive the desired cost efficiency, without compromising in the quality and effectiveness of business-as-usual support offered to the business.

Key contacts

Mike Sobers
Partner
+44 20 7007 0483
msobers@deloitte.co.uk

Dan McDonough
Director
+44 20 7007 9706
dmcdonough@deloitte.co.uk

Yannis Petras
Senior Manager
+44 20 7303 8848
ypetras@deloitte.co.uk

Notes

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 2 New Street Square, London EC4A 3BZ, United Kingdom. Tel: +44 (0) 20 7936 3000 Fax: +44 (0) 20 7583 1198.

Designed and produced by The Creative Studio at Deloitte, London. 39728A