Deloitte.



Leading lights

2018 Hot topics for IT Internal Audit in Financial Services

An Internal Audit viewpoint

Contents



Introduction

01



IT Internal Audit Hot Topics through the years: 2012-2018

02



Analysis by sub-sector

04



Challenges for IT Internal Audit Functions

07



Internal Audit viewpoints by topic

09



Contacts

20



Welcome to our annual review of the Information Technology Hot Topics for Internal Audit functions in Financial Services, which is being run for its seventh year.

Technology and the impact of disruption on the Financial Services sector is fast becoming a top priority for organisations alongside regulatory compliance. Financial institutions are feeling the burden of the ever-increasing threat of cyberattacks, the imperative to innovate to keep pace with maturing FinTech combined with increased focus from regulators on the management of IT, data and the operational resilience of the financial system. As a result, there is pressure on IT Internal Audit functions to ensure that there is adequate and appropriate assurance coverage of this evolving IT risk landscape and to adapt in order to make an impact both from an assurance perspective and value-add input to management as a business partner.

We surveyed over 20 organisations across the Financial Services sector in the UK to obtain views from Heads of IT Internal Audit or the Chief Internal Auditors on the 'hot topics' or areas of focus in their IT audit plans for 2018. It will come as no surprise that topics such as Cyber Security, Strategic Change and Data management / Governance featured consistently across all sub-sectors surveyed. The imminence of the EU General Data Protection Regulation has ensured that Data Management / Governance is one the top priorities as organisations prepare for the May 25th 2018 implementation date. Linked to this is the rise of Information Security/Identity and Access Management in the rankings.

The "Analysis by Sub-Sector" section provides further insight on topics which were more pertinent for each sub-sector analysed, while the detailed "Viewpoints by Topic" reflects the opinion of respondents on the significance of each area, coupled with our analysis on how Internal Audit should address these topics. As we did last year we have included a short commentary on the challenges facing IT Internal Audit functions across the sector, also based on responses to our survey.

Leading lights | 2018 Hot Topics for IT Internal Audit in Financial Services

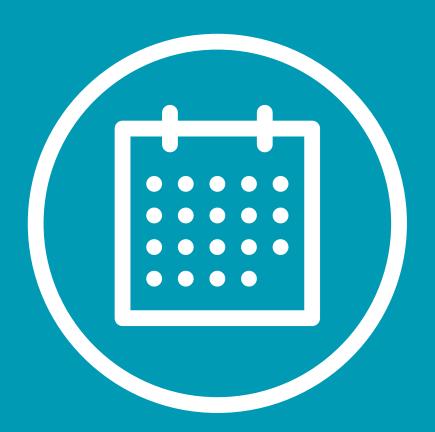
As always, we welcome your feedback on improving the way we conduct the survey, as well as the quality of the publication itself year on year. I genuinely hope that our issue for 2018 continues to provide useful insight, generates constructive debate amongst your teams and your IT stakeholders, and helps you shape your IT Internal Audit plans.



Medder

Mike Sobers

IT Internal Audit Hot Topics through the years: 2012-2018





IT Internal Audit Hot Topics 2012-2018

Below is a comparison of the top 10 IT Internal Audit hot topics over the past seven years as identified through our annual survey of Heads of IT Internal Audit in the Financial Services sector.

It highlights some interesting trends over time, including the continued presence of Cyber Security and Strategic Change at the top of our list, the added importance given to Data Management and Data Governance in the times when there

has been increased regulatory focus (now, for instance, with the EU General Data Protection Regulation (GDPR), and previously in the insurance sector for Solvency II), and the fluctuating importance of Disaster Recovery and Business Continuity which aligns with the frequency of high profile incidents being reported in the media driving greater focus of the subject. Topics which appear in more than two years have been colourcoded to help illustrate their movement in the top 10 over time.

Rank	2018	2017	2016	2015	2014	2013	2012
1	Cyber Security	Cyber Security	Cyber Security	Cyber Security	Large scale change	Third-party management	Cyber threat
2	Strategic change	Strategic change	Strategic change	Disaster Recovery & Resilience	IT Governance and IT Risk Management	Identity & Access Management	Complex Financial Models
3	Data management and Data Governance	Data management and Data Governance	Third-party management	Large scale change	Identity & Access Management and Data Security	Data Governance & Quality	Data Leakage
4	IT Disaster Recovery & Resilience	Third-party management	IT Disaster Recovery & Resilience	Enterprise Technology Architecture	Data Governance & Quality	Large scale change	Data Governance & Quality
5	Information Security/Identity & Access Man.	IT Disaster Recovery & Resilience	Data management and Data Governance	Third-party management	Third-party management	Cyber Security	Rogue Trader and Access Segregation
6	Third-party management	IT Governance and IT Risk Management	Information Security	Information Security	Cyber Security	Resilience	Regulatory Programmes
7	IT Governance and IT Risk Management	Information Security/ Identity & Access Man.	Digital and Mobile Risk	Digital and Mobile Risk	Digital and Mobile Risk	Cloud Computing	Financial Crime
8	Cloud Computing	Enterprise Technology Architecture	IT Governance and IT Risk Management	Data management and Governance	Service Management	Mobile Devices	Third-party management
9	Digital and Mobile Risk	Cloud Computing	Enterprise Technology Architecture	IT Governance and IT Risk Management	Disaster Recovery & Resilience	Complex Financial Modelling	Social Media
10	Enterprise Technology Architecture	Digital and Mobile Risk	Payment Systems	Service Management	Cloud Computing	Social Media	Mobile Devices

Figure 1. IT Internal Audit Hot Topics through the years: 2012-2018

Analysis by sub-sector





Retail Banking

Survey respondents across Retail Banking highlighted a continued focus on IT Disaster Recovery and Resilience, placing it third in their list of hot topics, while other sub-sectors did not place this in the top 5. Supervisory expectations are looking for more detailed planning from Retail Banks in their responses to scenarios; including cyber breaches and technological failures that require robust resilience plans, due to the impact these events can have on customers and the wider financial system. Uniquely, Retail Banking participants called out IT Availability and Performance and Regulatory Compliance as key concerns. Retail Banks are walking a fine line between offering high availability services to customers, and complying with increasingly complex regulatory requirements. Many Retail Banks are also burdened with maintaining a complex legacy estate with the associated challenge of systems with multiple upstream and downstream dependencies.

Capital Markets

The challenge of ongoing regulatory change continues to be a significant priority in the Capital Markets sector, and in this context it is unsurprising that Data Management & Governance and Strategic Change rank in second and third place for respondents from the sector. Recent experience has again demonstrated that in grappling with major regulatory implementations such as MiFID II, both data quality and the ability of an organisation to execute extensive technological change are key. Meanwhile, the prioritisation of Enterprise Technology Architecture and Incident Response in this sector reflect the ongoing challenge of responding to incidents effectively in a high availability environment with a complex legacy estate.

Insurance

Insurance firms share the concerns of Capital Markets respondents around compliance with upcoming regulation, also ranking Data Management and Governance as 2nd in their list of hot topics. Interestingly, this topic did not make the top 10 for Insurance firms last year, which may reflect an expectation from Heads of IT Internal Audit that firms do not have as firm a grip on addressing the challenge of compliance with the GDPR as they had expected. Insurance firms also showed an increased focus on emerging technologies such as Robotic Process Automation and Blockchain enabled technologies pushing this topic into the top 10, which is likely a reflection of the industry-wide focus through initiatives such as the Blockchain Insurance Industry Initiative B3i and a recognition that there are significant opportunities to enhance the efficiency of manual processes that are prevalent in the sector through Robotic Process Automation.

Investment Management

The selection of Cyber Security, Information Security and Data Management and Governance by investment managers is indicative of significant concerns from Heads of IT Internal Audit around organisations' ability to protect and manage their data. At the same time, as Investment Managers continue to invest in digital services too, it is clear that being first to market with new digital services or having the capability to adapt rapidly to either changes in consumer demands or market conditions is increasingly important. This is evidenced by the appearance of Agile / DevOps as a hot topic for Investment Managers, indicative of the fact that their IT functions are adapting to meet rapidly evolving demands.

Rank	Financial Services	Retail Banking	Capital Markets	Insurance	Investment Management
1	Cyber Security	Cyber Security	Cyber Security	Cyber Security	Cyber Security
2	Strategic Change	Strategic Change	Data Management and Governance	Data Management and Governance	Information Security
3	Data Management and Data Governance	IT Disaster Recovery and Resilience	Strategic Change	Strategic Change	Data Management and Governance
4	IT Disaster Recovery and Resilience	Data Management and Governance	Enterprise Technology Architecture	Third-Party Management	Large Scale / Strategic Change
5	Information Security	Information Security	Information Security	Cloud Computing	Agile / DevOps
6	Third-Party Management	IT Governance and IT Risk Management	Third-Party Management	IT Disaster Recovery and Resilience	Disaster Recovery and Resilience
7	IT Governance and IT Risk Management	Third-Party Management	Disaster Recovery and Resilience	IT Governance and IT Risk Management	Incident Response
8	Cloud Computing	IT Availability and Performance	Incident Response	Enterprise Technology Architecture	Enterprise Technology Architecture
9	Digital and Mobile Risk	Regulatory Compliance	Digital and Mobile Risk	Digital and Mobile Risk	Third-Party Management
10	Enterprise Technology Architecture	Cloud Computing	IT Governance and IT Risk Management	Emerging technologies (Robotics, Blockchain)	Digital and Mobile Risk

Table 1. Analysis by sub-sector. Items in the table above highlighted in red appeared as unique results for this sub-sector

Challenges for IT Internal Audit Functions



Challenges for IT Internal **Audit Functions**

The word cloud in Figure 2 shows the words / phrases that our respondents used most frequently when asked about challenges for IT Internal Audit functions. As in previous years Heads of IT Internal Audit listed 'getting the right resources at the right time' as their main challenge. Recruitment, management and retention of specialist resources in particular continues to present a challenge, particularly as we have observed that salaries for "scarce" skills are on the rise while Internal Audit functions are under increasing pressure to "do more with less".

robotics audit analytics cyber skillset gdpr readiness budget information security expertise cyber attacktiming of audits real time reduce costs. good practice technology environment internal audit getting the right resources use of data analytics emerging risks areas adapting to new processes cyber security capabilities expanding IT skillsets forward looking advice data protection brexit implications blockchain predictive analysis

Figure 2. Challenges for IT Internal Audit Functions

Data analytics has been on the agenda for Internal Audit functions for several years, however few functions have effectively embedded the use of data analytics in their audit practices. Typically this is linked to the availability of reliable data sources from the business and, as the quality of these sources improves, Internal Audit functions should ensure that they have built a capability to use these data sources particularly in areas that would enable the use of automated auditing techniques with the intention of freeing up resources from routine audits in order to focus on emerging risk areas. Internal Audit has the opportunity to demonstrate the use of automated auditing and/or monitoring approaches to 1st and 2nd line oversight functions as further means of adding value to the organisation.

Respondents also mentioned the increased difficulty of staying abreast of multiple emerging risk areas while adapting to new business processes. IT Internal Audit functions must ensure there is an appropriate investment in talent development to ensure that they are able to retain an appropriately skilled team to focus on key emerging risks with the ability to call on specialist resources for non-key emerging risks. There is also a requirement, while adapting to new business processes and ways of working, to ensure that the IT Internal Audit approach remains relevant. Particularly when considering large scale Strategic Change, IT Internal Audit functions are increasingly moving away from the traditional "point in time" audits at the conclusion of events, but are performing more real-time reviews in a guest to remain both relevant and to provide added value to the organisation they serve.

IT Internal Audit Hot topics through the years 2012-18

Internal Audit viewpoints by topic





1. Cyber Security (=1)

What has changed?

Cyber Security takes the top spot in our survey for a fourth year in a row. This will come as no surprise given the constantly evolving cyber threat environment and publicity that cyber incidents receive. However, our respondents indicated a shift in focus in their organisations from Cyber Defence to Cyber Resilience i.e. the ability to respond effectively following a cyber incident. This is a signal that Financial Services organisations have accepted that it is now a question of "when" rather than "if" a cyber incident occurs and consequently that it is no longer acceptable to focus solely on preventative measures; the ability to identify and recover from a cyber incident is perhaps more important.

High-profile breaches such as the \$81 million theft from the Central Bank of Bangladesh using the SWIFT network and the increasing prevalence of ransomware attacks means that this topic is never far from headlines, the attention of regulators, and Board agendas. As a result of the increased awareness of cyber threats there is an elevated focus on cyber risk reporting at Board level. In 2016, 87% of FTSE100 annual reports highlighted cyber risk as a principal risk, however only 5% had identified a board member with cyber expertise. We expect that Boards will increasingly be under scrutiny over their practical IT and cyber expertise, and their ability to demonstrate that they can oversee and challenge management's Cyber strategy appropriately.

What is the impact?

Detailed requirements are anticipated from national supervisors, while Banks and Financial Market Infrastructure firms (FMIs) in particular should expect increased scrutiny. An example is the new requirement around Cyber Security from the New York Department of Financial Services (23 NYCRR 500) which took effect in March 2017. The rules contain strict requirements for financial institutions to establish enhanced cybersecurity programmes, adopt written cybersecurity policies and procedures, and report cyber-events.

What is Internal Audit's response?

Internal Audit has a critical role in helping organisations in the ongoing battle to manage cyber threats, both by providing an independent assessment of existing and required controls, and helping the Board Audit and Risk Committees understand and address the diverse risks of the digital world.

Internal Audit functions must ensure they have access to appropriately skilled and experienced cyber resources to engage with stakeholders and fully understand the cyber risk challenges the organisation is facing. Internal Audit should enhance their understanding and readiness to assure cyber risks across new technologies that will form the architecture of the future, such as cloud-based and blockchain enabled systems.

The Internal Audit plan for providing assurance over Cyber risks should not be set in stone; adjustments can and should be made based on the emergence of new risks, changes in the relative intensity and importance of existing threats, and other key organisational developments.

Note: The number in brackets indicate the ranking of the topics in our 2017 survey and the relative movement this year.



What has changed?

The pace of business and technological change shows no sign of slowing and is likely to be hastened by maturing FinTech services supported by disruptive technologies. Organisations must continue to meet the demands of increasingly techsavvy and digital native customers, or face the prospect of being left behind. More than ever the success or failure of Strategic Change initiatives have the potential to make or break organisations, and failure to follow through on ambitious changes can have a negative impact on value perception and staff engagement. Equally, changes must be relevant and following the market into the wrong solutions may pose a greater risk than doing nothing.

What is the impact?

In light of a rapidly evolving market, political and technology landscape, many organisations are facing up to the need for wholesale reorganisation of business operations. With demand for new customer engagement models, upgrades to legacy IT environments after years of tactical fixes and making-do, and the onward push to cut operating costs, the time is right for a strategic portfolio of change that will deliver a balance of transformation and stability. Transformation on this scale intrinsically presents greater risks to the business strategy, and the importance of effective controls being embedded as part of any change initiative should not be underestimated.

What is Internal Audit's response?

Internal Audit functions are increasingly being challenged by Audit Committees and Management to provide a view of risks before they are realised in the portfolio, rather than after the fact reporting. More broadly, there is an increased focus on providing a view on the capacity and capability of management to execute the change agenda, leveraging the three lines of defence to oversee this execution risk challenge.

In the context of Strategic Change, this may require audit to adopt Agile methods, real-time analysis and a continuous approach to assurance; including having a seat at the table for key strategic initiatives and providing regular, relevant challenge to management with a direct route to reporting issues to decision makers.





3. Data Management and Data Governance (=3)

What has changed?

Data Management and Data Governance takes third spot in our survey for the second year in a row. The continued relevance of this topic is not a surprise, with organisations now more than ever "waking up" to the challenges of achieving compliance with the GDPR by 25th May 2018. Not only does the new regulation bring greater consumer rights, including the right to erasure, but it brings the need for organisations to prove a "defensible position" i.e. to be able to evidence compliance with the new regulation to the relevant supervisory authority (in the case of the UK, the Information Commissioner's Office - ICO). As such, the old adage of "nobody will be ready come May 2018" no longer washes; if an organisation cannot demonstrate a "defensible position" they may well be getting a visit from the ICO.

What is the impact?

While many viewed the GDPR as an extension of the UK Data Protection Act (DPA) regulation, organisations are recognising that they perhaps were not compliant with the DPA, and as a result they have more work to do to achieve compliance than was initially thought.

A starting point for being able to demonstrate compliance is for organisations to ensure they have a data inventory of all personal data. However, this provides challenges; namely, what is "personal data"? Per the regulation, personal data is "any information relating to an identified or identifiable natural person"; the challenge being often the term "identifiable".

Even if a person cannot be identified solely from a single piece of data (i.e. a staff personnel number), if it can be used in conjunction with other data to identify a person then it can be classed as personal data. With this, organisations are realising the scale of the task ahead of them.

Finding time to do all of the above is proving a challenge; the majority of organisations have realised that this cannot be run as a side of desk activity but will require significant time and resource. Further, this is not a change that can be made in isolation, it requires time and effort across the organisation; nobody knows the data they use better than individual business units. However, this is often time organisations simply haven't budgeted for.

What is Internal Audit's response?

Internal Audit are typically engaged in two ways relating to GDPR; reviewing the scope and progress of an organisation's readiness programme for the new regulation, or assessing the capability of the organisation to present a defensible position. Additionally, IT Internal Audit functions in our survey are being asked to provide assurance over organisations' broader Data Governance strategies and framework. This may also include reviewing the organisation's approach to data collection and use of 'Big Data' as a tool for targeting customers with relevant products, offers or services e.g. location and demographic based targeting.



4. IT Disaster Recovery and Resilience (▲5)

What has changed?

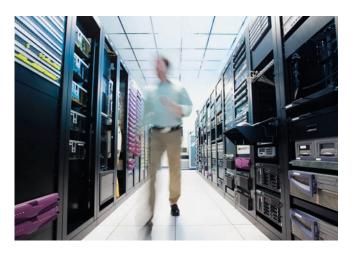
IT Disaster Recovery and Resilience climbs one place in this year's survey, reflecting organisations' continuing focus on the need to ensure their business remains resilient in an ever more technology enabled environment. There continues to be ever increasing focus from regulators on this topic, and as such it remains high on the agenda across the Financial Services sector.

What is the impact?

New and innovative technology is being used to bring a competitive edge to many organisations. It can provide greater insight from data mining for an insurance quotation, enabling Insurance companies to offer competitive premiums, or high-performance and high-availability systems in Capital Markets organisations allowing them to maintain an edge over competitors and liquidity in markets where quick response times and access to data underpins profitability. In these and many more examples, technology is more than ever shaping the way organisations seek a competitive advantage. This competitive advantage can only be maintained while the technology is working and this, coupled with the ever increasing focus on organisations ability to recover from a cyber incident, means the need to be resilient remains high on organisations' agendas.

What is Internal Audit's response?

While Internal Audit functions may still be required to perform one-off reviews over individual disaster recovery plans, the focus has switched to assessing the end to end operational resilience of the organisation. This can be considering the readiness of an organisation to cope when disaster recovery plans are invoked, but also the overall resilience of systems so that a full disaster recovery scenario can be avoided in the first place. This presents a challenge for IT Internal Audit functions around developing the right skillsets to assess the technical aspects of operational resilience planning.





What has changed?

As in prior years there is a continuation in the trend for organisations to separate the topics of Information Security and Cyber Security. While some use the terms interchangeably the distinction between the topics is often seen to be that Information Security is linked to controls implemented to support the effective management of business processes such as identity and access management and application security, whereas Cyber Security focuses on an organisation's ability to detect, respond to and recover from external and/or internal attempts to disrupt or damage the organisation or its customers.

What is the impact?

Many organisations will be forced to revisit the effectiveness of elements of their Information Security programmes in the light of the requirements of incoming regulation, with a particular focus on identity and access management. There is continued concern that the emergence and current prominence of Cyber Security may be causing management to focus too much attention on the latest cyber initiatives at the expense of remediating the basics of Information Security (an area many organisations continue to struggle with) such as user access management that may underpin the effectiveness of such initiatives.

Additionally, the emergence of Robotic Process Automation (RPA) will mean that organisations will have to consider whether access for robots can or should be managed in the same way as their human counterparts; for instance, is the concept of segregation of duties relevant for a robot operator?

What is Internal Audit's response?

Internal Audit should ensure that in addition to providing assurance over emerging risks, management does not lose sight of the importance of traditional Information Security controls and ensure that these are incorporated into the audit plan either as a specific review or as part of a programme of integrated audits. Internal Audit should continue to challenge management to maintain focus on fixing the basics while responding to the ever-changing cyber threat landscape.





6. Third-Party Management (▼4)

What has changed?

Third-Party Management has fallen two places in our survey this year, but this is largely due to organisational focus on compliance with upcoming regulations such as the GDPR as opposed to a decrease in the perception of the importance of the effective management of Third-Party risk.

What is the impact?

In today's business environment, organisations continue to face pressure to find ways to create a competitive advantage and operational efficiencies. Third-party 'ecosystems', also known as the 'extended enterprise', are becoming more prominent sources of strategic advantage for organisations, with the recent Deloitte Third-Party Risk Management report noting that leveraging an 'ecosystem' of third-parties can help organisations innovate and generate flexibility, agility, and cost savings¹. However, inconsistency in approach and weak controls around third-party risk management can result in significant financial, reputational or regulatory damage. Where Third-Parties act as processors of personal data, the GDPR will require organisations to make it clear to data subjects which third-parties are processing their personal data. It will also be the responsibility of the organisation to notify the relevant supervisory authority of any data breach without undue delay, even if that data breach is the responsibility of the Third-Party data processor.

What is Internal Audit's response

Organisations may place a level of reliance on third-party assurance reports, such as SOC1 or ISAE3402, but this often only gives an organisation a narrow level of assurance. Instead, Internal Audit departments are considering ways in which they can play a greater role in providing assurance over third parties, be it performing audits of third-parties on behalf of organisations, or focusing more traditionally on internal organisational controls, such reviewing the overall approach to Third-Party risk management against good practice and regulatory requirements. IT Internal Audit functions also have a role to play in educating the business around the ownership of controls wholly or partly operated by a Third-Party and requirements for demonstrating an effective control environment regardless of the control owner.





7. IT Governance and IT Risk Management (▼6)

What has changed?

IT Governance and IT Risk Management has fallen one place in our ranking since last year. However, given the pace of technological change and increased regulatory focus on IT Governance and IT Risk Management, Boards continue to challenge management to demonstrate that effective IT Governance structures are in place to ensure that IT performance is managed effectively and delivers value for money. All this must be delivered while also ensuring that IT Risk Management processes are effective in ensuring that IT risk exposure is proactively managed in line with the organisation's broader risk appetite.

Leading lights | 2018 Hot Topics for IT Internal Audit in Financial Services



What is the impact?

While organisations recognise the need to evolve their IT strategy this need often does not extend to IT Governance and IT Risk Management processes. Inadequate IT Governance or Risk Management processes can leave management with a lack of visibility to the performance and value delivered by IT as well as emerging risks within the IT environment. This could consequently lead to strategic decisions being made without a full understanding of the impact on the organisation's risk profile and alignment with risk appetite.

What is Internal Audit's response?

Internal Audit should incorporate assessments of IT Governance and IT Risk Management within their thematic IT reviews and provide independent challenge on the capability of 1st and 2nd line functions in identifying and reporting IT risk through appropriate forums to decision makers. IT Internal Audit functions also have an important role to play as an advocate for day-to-day engagement and alignment between technology, IT risk and operational risk functions as an enabler for risk intelligent decision making considering the full spectrum of relevant risks.



What has changed?

Organisations began their adoption of Cloud Computing by moving their non-core systems and / or non-production environments to the cloud. Increasingly organisations are looking into migrating core processing and production environments to the cloud, with many adopting a 'cloud first' IT strategy shifting the question from 'can this be in the cloud?' to 'why can't this be in the cloud?' Whether this a private, public or hybrid cloud, organisations are looking to realise the benefits of rapid scalability and predictable cost models that cloud solutions promise. Another advantage of moving to a cloud solution is the potential to rapidly decrease the proportion of outdated systems often found in organisations with a complex legacy estate and transferring the burden of ongoing infrastructure maintenance and refresh to the cloud provider.

What is the impact?

Management should ensure that they have the capability to manage the risks associated with the adoption of cloud technologies. For example they will need to ensure that their vendor selection processes are sufficiently rigorous to incorporate additional considerations presented by the type of arrangements being entered into and that there is capability within the organisation to effectively monitor the performance of cloud providers both operationally and from a risk management perspective.

What is Internal Audit's response?

As with other Strategic Change initiatives, IT Internal Audit functions should ensure that the organisation is set up to realise the benefits outlined in the original business case and that the organisation has considered the risks related to the move to the cloud. The FCA has issued 'FG16/5: Guidance for firms outsourcing to the 'cloud' and other third party IT services' which provides IT Internal Audit functions with a reference point for the expectations of the regulator around risk management and reiterates the FCA's position that while processing can be outsourced, risk management cannot be. IT Internal Audit functions can play a role either during the transition of services to the cloud by acting as an advisor during the course of cloud adoption projects or through post-implementation reviews of the benefits delivered and the operation of key controls implemented to monitor the service provider and manage the associated risks.





9. Digital and Mobile Risk (▲10)

What has changed?

Reversing last year's trend Digital and Mobile Risk has climbed a place in our top 10. This is due to the ubiquitous nature of Digital and Mobile platforms, the maturing of mobile only offerings, and customer expectations around access to services driving the strategic imperative for organisations to engage with customers through these channels. Our recent Global Mobile Consumer survey found that 85% of 16-75 yearolds now own or have access to a smartphone. Smartphone adoption is not limited to younger generations, in fact 55-75 year olds are the fastest growing adopters over the last five years with two thirds of this age group now having access to a smartphone².

What is the impact?

With the increased focus on accessibility of services and user experience there is a drive to accelerate the route to market for new applications and/or enhancements to existing products. To respond to this many IT functions are adopting an Agile software development methodology to iteratively improve end user experience rather than focusing on larger, slower release cycles. There is a pre-conception that moving to an Agile software development methodology results in weaker controls; this is not the case when Agile principles are applied as intended, however the implementation of the controls may appear very different to those applied when using a traditional waterfall software development methodology.

What is Internal Audit's response?

IT Internal Audit functions should be prepared to adapt their style to accommodate new ways of working without losing focus on the control objectives they are looking to provide assurance over. In an Agile environment this requires being able to understand the language and definitions used by agile teams and having the ability to identify the applicable control points in the new ways of working. Typically this may lead to the usage of automated tools and analytics to review the operation of these controls both historically and real-time.

Internal Audit should remain vigilant for situations where Agile principles are inconsistently applied throughout the software development lifecycle. In general, it is acceptable to use a mixture of agile and traditional waterfall processes (hybrid approach). This should however not be used as an excuse to operate an environment with partial control adherence and documentation.





10. Enterprise Technology Architecture (▼8)

What has changed?

While Enterprise Technology Architecture has dropped two places, it remains in our top 10 as Financial Services organisations struggle with complex and often prohibitively expensive technology estates often as a result of extended periods of growth through mergers and integrations.

What is the impact?

Organisations faced with the threat of increasingly agile competitors continue to look for opportunities to simplify their estate as part of the drive to increase their ability to keep pace with rapidly evolving market demands. While simplifying the technology footprint is a logical goal to reduce operational overheads, any attempt at simplification places an additional burden on stretched IT functions tasked with ensuring legacy systems remain operational. The cost of additional resource to ease this pressure must be weighed against the cost of failing to adapt and needs to be managed appropriately. Equally, the approach to change should reflect the organisation's risk appetite; incremental changes will present less risk to BAU processes and spread the cost over a longer period, but may not deliver benefits quickly enough to be viable; conversely, large scale change projects present a higher risk of disruption to BAU and a higher short term cost, but may allow benefits to be realised more rapidly.

What is Internal Audit's response

While IT Internal Audit functions are expected to provide assurance over the security and resilience of the legacy estate it is important to balance this and ensure that IT Internal Audit functions are perceived as adding value and not simply repeating known issues. To address this, many IT Internal Audit functions are focusing attention on change programmes that aim to address the challenges of the legacy estate, by reviewing the governance around strategic decisions as well as providing ongoing assurance during the course of large scale change programmes. IT Internal Audit functions are also reviewing the effectiveness of IT Risk Management in ensuring that decision makers are provided with appropriate risk information to inform strategic decisions.







Mike Sobers Partner 020 7007 0483 msobers@deloitte.co.uk



Yannis Petras Director 020 7303 8848 ypetras@deloitte.co.uk



James Bugden **Senior Manager** 020 7303 7043 jambugden@deloitte.co.uk



Jonathan Roffey Senior Manager 020 7007 8755 jroffey@deloitte.co.uk

Technology and the impact of disruption on the Financial Services sector is fast becoming a top priority for organisations alongside regulatory compliance. Financial institutions are feeling the burden of the ever-increasing threat of cyber-attacks, the imperative to innovate to keep pace with maturing FinTech combined with increased focus from regulators on the management of IT, data and the operational resilience of the financial system.

Notes

Deloitte.

This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

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.

Deloitte LLP is the United Kingdom affiliate of Deloitte NWE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NWE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

© 2017 Deloitte LLP. All rights reserved.

Designed and produced by The Creative Studio at Deloitte, London. J13847