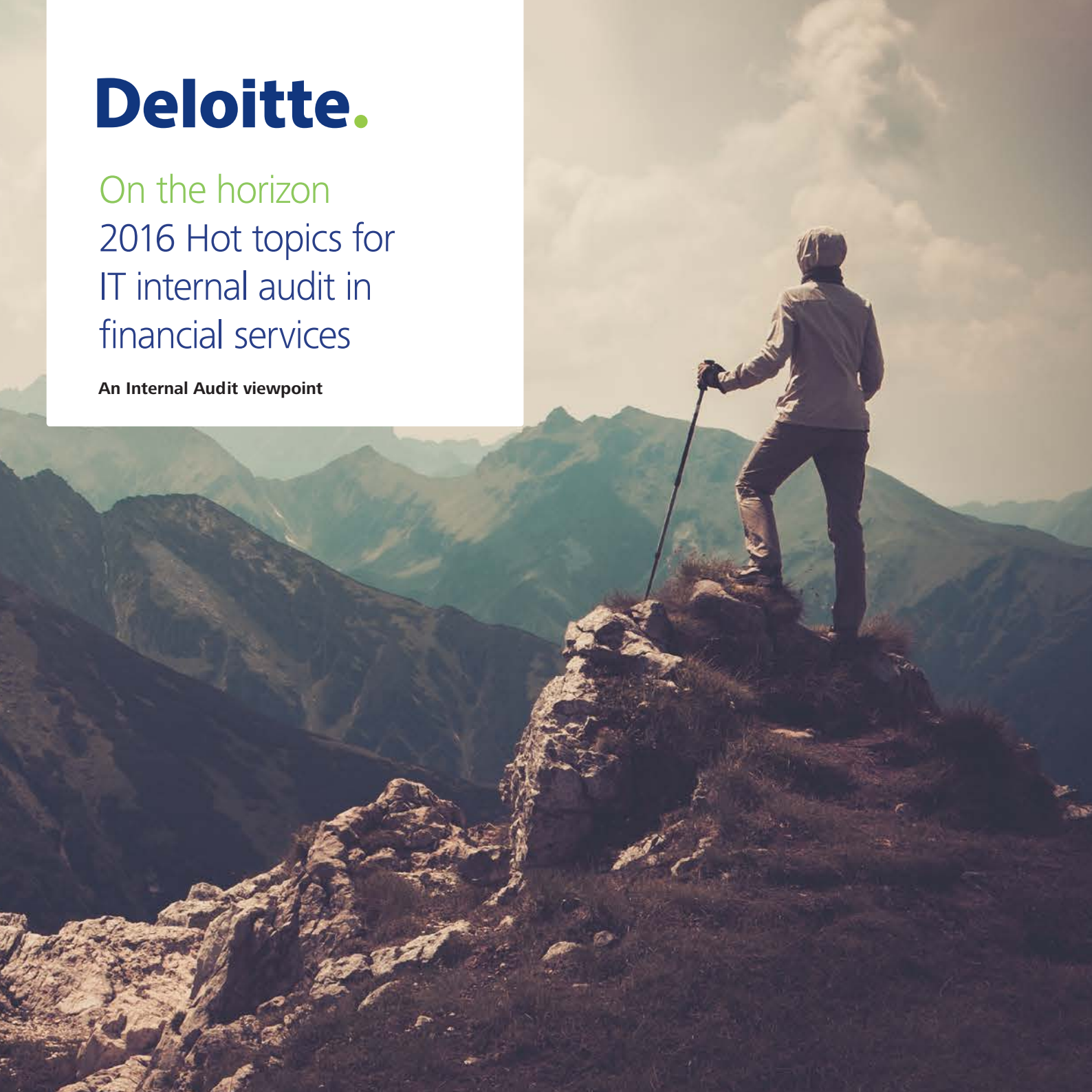
Deloitte.

On the horizon
2016 Hot topics for IT internal audit in financial services

An Internal Audit viewpoint



Introduction

Welcome to our fifth annual review of the information technology hot topics for internal audit in financial services.

Executive management and Internal Audit departments in financial services continue to operate within an evolving environment of new regulatory requirements (e.g. MiFID II; payments), emerging risks (e.g. new technologies; mobile and digital) and expanding stakeholder expectations (drive for innovation). This environment is further challenged by the arrival of new entrants into the world of financial services that are likely to disrupt and transform the industry, such as 'challenger' banks, the UK peer-to-peer foreign exchange start-ups or peer-to-peer insurance.

There are a number of core control areas which feature in the 2016 hot topics, such as traditional high-profile items, which form the backbone of IT internal audit plans. For example, cyber security unsurprisingly features as the highest priority topic for a second year running. What is interesting to note is that even organisations with a relatively mature control environment continue to see this as a key area of audit focus as they try to align their approach with the growing regulatory expectations on how to assure such a mutating global threat. Strategic or large-scale change was another key theme which reflects the regulatory focus and growing expectations by Boards on managing strategic initiatives and providing appropriate oversight over the associated execution risk across the organisation.

We had 22 organisations from across financial services participate in this survey; in comparing and contrasting the key areas of focus of IT Internal Audit departments in each of the sub-sectors, it is not surprising to see that the core areas of cyber, strategic change and third-party risk management feature consistently in the top 5 of organisations in all sub-sectors (table 2).

Survey participants from the Retail Banking, Insurance and Investment Management sectors underlined the challenges in auditing legacy infrastructure and systems, with Retail Banking particularly highlighting the recent changes in payment models. The latter is a new topic for the year, and reflects the anticipated impact from the second Payment Services Directive (PSD2) as well as recent developments on the traditional payment models from both a regulatory and technology perspective. The Retail Banking sub-sector is facing challenges and emerging competition from new providers who are heavily investing in payments systems, while at the same time it grapples with high profile payment outages which threaten the availability of existing payments services.

Capital Markets respondents, on the other hand, highlight a focus on electronic trading, referencing the concern over high-frequency and automated trading practices, which increase their susceptibility to losses due to technology issues. The more mature Internal Audit departments have started using a combination of trading, audit analytics and technology specialists to understand the risks comprehensively and review those areas, including the way trading methodologies have been developed, tested and implemented in the trading platforms.

This publication has been well received, both in the financial services sector and beyond, by Heads of IT Internal Audit and Heads of Audit as well as by IT Directors and IT Risk functions. We have obtained useful feedback over the years, and we will continue to both produce and enhance the publication. I truly hope that for another year this proves to be a useful resource, which can help you benchmark your own IT Audit plans for 2016.

Mike Sobers
Partner

IT Internal Audit Hot Topics: 2012–2016

The table compares the top 10 IT Internal Audit hot topics over the past five years as identified through our annual survey of Internal Audit departments in the financial services industry. It highlights some interesting trends over time. The table also reflects the core, high-profile items that have appeared consistently in the top-10 (which are marked in bold).

Rank	2016	2015	2014	2013	2012
1	**Cyber Security**	**Cyber Security**	Large Scale Change	**Third-Party Management**	**Cyber Threat**
2	Strategic Change	Disaster Recovery and Resilience	IT Governance and IT Risk Management	Identity and Access Management	Complex Financial Modelling
3	**Third-Party Management**	Large Scale Change	Identity & Access Management and Data Security	**Data Governance and Quality**	Data Leakage
4	IT Disaster Recovery and Resilience	Enterprise Technology Architecture	**Data Governance and Quality**	Large Scale Change	**Data Governance and Data Quality**
5	**Data Management and Data Governance**	**Third-Party Management**	**Third-Party Management**	**Cyber Security**	Rogue Trader and Access Segregation
6	Information Security	Information Security	**Cyber Security**	**Resilience**	Regulatory Programmes
7	Digital Risk	Digital and Mobile Risk	Digital Risk	Cloud Computing	Financial Crime
8	IT Governance and IT Risk Management	**Data Management and Governance**	Service Management	Mobile Devices	**Third-Party Management**
9	Enterprise Technology Architecture	IT Governance and IT Risk Management	**Disaster Recovery and Resilience**	Complex Financial Modelling	Social Media
10	Payment Systems	Service Management	Cloud Computing	Social Media	Mobile Devices

Topics which appear in more than two years have been colour-coded to help illustrate their movement in the top 10 over time.

2016 IT Internal Audit Hot Topics: An analysis by sub-sector

Top 10	Financial services	Retail Banking	Capital Markets	Insurance/Investment Management
1	Cyber Security	Cyber Security	Cyber Security	Cyber Security
2	Strategic Change	Strategic Change	Strategic Change	Third-Party Management
3	Third-Party Management	Third-Party Management	IT Governance and IT Risk Management	Strategic Change
4	IT Disaster Recovery and Resilience	IT Disaster Recovery and Resilience	Electronic Trading	Mergers/Integration of systems
5	Data Management and Data Governance	Payment Systems	Data Management and Data Governance	Information Security
6	Information Security	Digital Risk	New Technologies	Data Management and Data Governance
7	Digital Risk	Enterprise Technology Architecture	IT Disaster Recovery and Resilience	IT Governance and IT Risk Management
8	IT Governance and IT Risk Management	Information Security	Third-Party Management	Obsolescence of Infrastructure
9	Enterprise Technology Architecture	Data Leakage	Digital Risk	IT Disaster Recovery and Resilience
10	Payment Systems	Legacy Infrastructure/ Obsolescence	Complex Financial Models	Enterprise Technology Architecture

2016 IT Internal Audit Hot Topics

1. Cyber Security (=1)

It is no surprise that cyber appears as the top concern for IT internal audit professionals in the industry for another year. Indeed it has been an increasingly regular feature in the media over the past 18 months, with multiple significant attacks and data breaches impacting all industry sectors, including some high-profile incidents for financial services firms. Cyber security is not simply about fixing the vulnerability that was exploited, but wider crisis management skills, including public, media and customer relations (refer also to topics 4, 6 and 10). With the increase in breach impact and complexity in 2015, incident response has seen a shift from point-based 'fix-it' type approach towards more robust internal controls around incident response and has also driven a need for businesses to understand cyber risk at Board level.

Internal Audit departments have an opportunity to demonstrate that they can understand and provide assurance over all the above. They can help to promote more organisational collaboration in cyber audits, both internally (across functions) and externally, as this will be a key area of focus for the sector over coming months. This should enable a more transparent view of emerging risks and threats, and in turn drive more effective risk management practices whilst allowing Internal Audit to remain agile to the changing nature of cyber threats. For the organisations with a less mature cyber control environment, Heads of IT Audit understandably see cyber as a topic of focus and concern in light of their organisation's legacy control weaknesses; however, even the more mature organisations are still concerned about keeping up with growing regulatory expectations on "what good looks like" and how to provide commensurate levels of assurance over cyber.

2. Strategic Change (▲ 3)

As with the previous three years, there is a significant amount of change in support of organisational strategy across the organisations we surveyed. Whether this has been investment in new channels such as mobile, new products or business lines, acquisition or divestment or to reduce operational risks and "keep the lights on", technology is often at the heart of enabling these strategic changes. Internal Audit departments are continuing to immerse themselves in the change portfolios and increase the resources allocated to assuring the strategic change programmes which the organisation is trying to deliver. It is becoming more typical for Internal Audit departments to include dedicated change audit teams and resources, with experience of technology development, change and testing as well as business change and project and programme delivery, in some cases focusing up to 40% of the total audit plan effort on change programme assurance.

Note. The number in brackets indicates the ranking of the topics in our 2015 survey and the relative movement this year

The challenge is how to deploy these resources effectively across the organisations' change portfolio and ensure that audit interventions are timely and provide a high impact on the control environment, but without hindering the programme resources trying to deliver. In our experience, Internal Audit departments are continuing to attend regulatory programme boards for Solvency II, IFRS 9, MIFID II and the enormous change driven by Structural Reform in the Banking sector, providing assurance that these programmes are on track and are delivering their intended outcomes.

3. Third-Party Management (▲ 5)

For the fourth year running, respondents to our survey highlighted that management of third-parties remains a key priority. Global third-party ecosystems of organisations, also known as the 'extended enterprise', are becoming stronger sources of strategic advantage and the scale on which this is now taking place in financial services has increased. Businesses are also facing new risks, such as the threat of high profile business failure, accountability for illegal third-party action or regulatory enforcement action with punitive fines, all leading to reputational damage and erosion of shareholder wealth. The financial services sector has dominated industry-specific regulation impacting the use of third-parties; and this is expected to get even more severe. Deloitte estimates that the failure by large multinational businesses to identify and manage third-parties appropriately, aside from the significant reputational damage, can lead to fines, direct compensation costs or other revenue losses in the range of US$ 2-50 million, while action under global legislation can be far higher, touching US$ 0.5-1 billion[1].

Internal Audit's focus on third-party risk has traditionally been reactive and this decentralised approach to risk has led to micro-focus on risk areas aligned to certain parts of a business or functional areas for example, operational performance from an extended enterprise perspective or information security from a corporate security perspective. Internal Audit functions should start to consider operational risk factors (e.g. performance, quality standards, delivery times, KPI/SLA measurement) with reputational and financial risk factors (e.g. an understanding of financial health, appropriate charging mechanisms and adherence to these) and legal and regulatory risks (e.g. compliance with anti-bribery regulations and awareness of global industry standards as they apply to third-parties).

1 *Third-Party Governance and Risk Management: Turning risk into opportunity;* Deloitte Touche Tohmatsu Limited, 2015

4. IT Disaster Recovery and Resilience (▼ 2)

IT system failures are front page news, leading to public coverage and reputational damage for a number of financial institutions. In 2015 instances of failures continued to emerge despite "Dear Chairman" letters and remediation programmes. Outages impacting ATM networks, digital services (refer to topic 7), payments systems (refer to topic 10) – including the recent 2014 Bank of England outage – and ultimately customer access to services continue to drive the attention of regulators and organisations to the stability of their systems. As a result, IT disaster recovery and resilience remains a key area of focus for Heads of IT Internal Audit.

Many progressive institutions are moving their focus from a traditional IT disaster recovery and resilience plan to understanding better the risks to services inherent in their IT environments, both in-house and outsourced services, and the controls to mitigate them. IT failures rarely result in a full invocation of the disaster recovery and resilience plan for IT as they are more often a result of a management process issue or human error rather than a "big ticket" data centre outage. With this is mind, it is imperative that Internal Audit departments broaden their focus to determine the adequacy of processes in place to avoid, respond and recover from planned and unplanned outages. Whilst technology is at the heart of the disaster recovery, resilience, in line with regulatory expectations, should be broader, encompassing areas such as operations, information and corporate security, communications, public relations and crisis management.

5. Data Management and Data Governance (▲ 8)

The volume of enterprise data is increasing exponentially, with more than 90% of the world's data estimated to have been created in the last two years alone[2]. Data governance brings benefits such as greater efficiency, visibility and cost savings, whilst in many cases helping to drive improvements in areas like data quality, or give greater confidence over data security. There has been a growing regulatory pressure to improve data governance, particularly in support of initiatives such as MiFID II, Solvency II, Basel III. In our experience, the most advanced organisations have addressed data governance at a senior level, with defined structures, policies and standards implemented across the entire organisation. This usually also involves the appointment of a Chief Data Officer (CDO).

2 SINTEF. "Big Data, for better or worse: 90% of world's data generated over last two years." ScienceDaily

Unfortunately, data governance implementations can be prone to becoming a leviathan of 'red tape' and onerous controls that do little to add value. Internal Audit departments will naturally have assessed aspects of data control in previous audit plans, however as businesses increase their focus on the customer, digital channels and explicit requirements in regulations, the need to audit data governance practices more thematically is pressing. They will need to determine the scope of the governance activities to audit, and the depth of that assessment. Plans may need to extend over a timeline of several years, with a prioritised approach to address more business critical areas first. For a large number of functions, auditing data governance requires expertise and toolsets which may not have traditionally been contained within the function and therefore a level of upskilling may be required. Leading Internal Audit departments in financial services, however, far from continuing a perennial deferral of their data governance review, have taken the initiative to leverage analytics capabilities which allow the use of sophisticated data quality and profiling tools to assess data quality comprehensively, helping to make sense of their data and unlock its value.

6. Information Security (= 6)

For some organisations, the topic of cyber is considered to include aspects of business continuity, crisis management, financial crime and fraud as well as traditional information security. For others, information security remains a topic of importance in its own right, which warrants its own place in the Internal Audit plan. Either way, the emergence of cyber in the past few years has shone a spotlight on the need to 'fix the basics' in order to minimise exposure to cyber threats. In many cases in financial services, fixing the basics is about assuring the appropriateness of access to information and focusing on identity and access management initiatives.

High-profile data loss incidents continue to make headlines, irk regulators and generate considerable workload across the three lines of defence to ensure that access is managed effectively. Given the scale of many financial services organisations, along with the size of their IT estates, this is a vast and continual challenge. We note in particular several banks with extensive 'Privileged Access Management' programmes aiming to minimise the volume of accounts with privileged access to systems along with similar programmes to sever direct access to systems by third-party organisations. Internal Audit departments are providing assurance over the effectiveness of these programmes, conducting re-performance or verification exercises to confirm that access is appropriate once the remediation programmes have concluded.

7. Digital Risk (= 7)

Digital channels such as mobile, cloud and social media are interacting and converging. While this convergence holds the promise of new opportunities for organisations, digital also introduces new risks that may not be effectively managed by the organisations' existing governance, oversight and internal controls frameworks. A number of these risks were noted in the Financial Conduct Authority's (FCA) thematic review on mobile banking[3], where financial institutions are using mobile banking as a catalyst for enhancing existing frameworks and future proofing their digital risk landscape by having a better understanding of their digital footprint. Mobile banking is also growing in popularity. As the British Bankers' Association (BBA) confirmed, "a revolution" in mobile banking use "is under way in the UK", with app use for customers at the five major UK high street banking groups almost doubling over the past year. Customers now make 5.7 million transactions a day using smartphones and other mobile devices. It is predicted that the take up of mobile banking will continue to rise.

Identifying, mapping and truly understanding the organisation's digital footprint will help Internal Audit departments to have a more targeted and risk focused view of the firm's digital landscape, which in turn can lead to a structured and robust plan for effective auditing of 'digital' and unearthing the associated residual risk. The role of Internal Audit in this era of fast-moving digital innovation and transformation cannot be underestimated in providing genuine input, oversight and challenge to the digital parts of the business.

8. IT Governance and IT Risk Management (▲ 9)

We have seen a significant uptake of IT governance and risk audits in the past 18 months and an increased emphasis on providing a view on whether the "information technology governance of the organisation supports the organisation's strategies and objectives" in line with the Institute of Internal Auditors (IIA) code. Many IT governance assessments are structured in line with COBIT 5 and the recently revised ISO/IEC 38500:2015 framework. Internal Audit departments are being challenged by their Boards and regulators to form an opinion regarding the transparency of decision making and effectiveness of governance practices in their technology teams, including the alignment of technology with business strategy, the appropriateness of risk reporting to executive management and the Board, as well as the efficiency of mechanisms to measure performance.

3 FCA Thematic Review: TR14/15 Mobile Banking and Payments (September 2014)

A key component of this landscape is IT risk management, which covers technology functions' compliance with enterprise wide risk management requirements but also their approach towards identifying and managing technology risk proactively. It is becoming increasingly common for Internal Audit departments to include such aspects in their IT governance and risk assessments. We have also noted a shift to auditing risk culture on a more granular level, through audits of technology risk culture for instance. Such assessments are becoming an established measure for assessing the quality and embedding of an organisation's strategic plan, risk appetite, governance structure and its risk management frameworks. To meet the above challenges, Internal Audit departments should continue to ensure that they upskill their teams with subject matter expertise and experience in order to meet the expectation of their Boards and regulators.

9. Enterprise Technology Architecture (▼ 4)

This year, we have seen a divergence in trend between the sub-sectors with respect to focus on the Technology Architecture. In Retail Banking, where there typically remains a heavy reliance on legacy estates and there are often large architectural transformation programmes to address the legacy issue, Internal Audit departments are continuing to devote time to reviewing these programmes as well as the capability, functionality, resilience and security of the legacy systems, themselves. Respondents in the Insurance sub-sector were devoting less time to the issue, reflecting the Insurance market's comparative underinvestment in upgrading existing systems or FinTech which is not necessarily revenue generating. By contrast, in the Capital Markets sub-sector, which is characterised by organisations with a drive towards high-frequency, low latency transactions, where speed is a competitive advantage, the Enterprise Technology Architecture topic did not feature at all. This reflects the fact that for many respondents from the sub-sector, Internal Audit effort is being directed elsewhere.

Irrespective of sector, the challenge for Internal Audit departments at the one end of the spectrum will be to retain the skills needed to test legacy platform controls, whilst at the other to challenge the newer FinTech developments which are emerging and in some cases are replacing the legacy estate.

10. Payment Systems (NEW)

Recent developments from both a regulatory and technology perspective are causing a significant shift in traditional payment models, resulting in major changes in the market. This is providing a difficult set of challenges across the financial services sector as banks face disruption from FinTech providers who are heavily investing in payments. Cash is becoming increasingly replaced by contactless and mobile transactions as Apple Pay and other offerings start to take a significant foothold in the market. Requirements for opening up access to the payments market to competition from non-bank players is coming in the form of the second Payment Services Directive (PSD2). This will, amongst other areas, allow direct access to banks' customer account information by licensed third-parties and enforce key payment security standards. High-profile payment outages are still all too common as institutions grapple with these future challenges whilst trying to ensure the 24/7 availability of existing payments services, often supported by legacy applications and infrastructure (refer also to topic 3 and 9).

Internal Audit departments need to upskill quickly and become more involved as organisations value their independent assurance on whether they are reacting appropriately to the risks related to the major regulatory and technological advances and that existing systems are scalable with expected market changes. This includes regulatory risk assessments, security assessments, review of key payment projects and assessment of existing payment services to ensure appropriate current and future operability.

Key contacts

Cüneyt Kırlar
Enterprise Risk Services Leader
Partner
ckirlar@deloitte.com

Barış Bağcı
Partner
bbagci@deloitte.com

Metin Aslantaş
Director
maslantas@deloitte.com

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. J2277