Deloitte.



Storming ahead

2017 Hot Topics for IT Internal Audit in Financial Services

An internal audit viewpoint



Contents

Introduction	02
IT Internal Audit Hot Topics 2012-2017	03
An analysis by sub-sector	04
Challenges for IT Internal Audit functions	06
Internal Audit viewpoints by topic	07
1. Cyber Security	07
2. Strategic Change	08
3. Data Management and Data Governance	09
4. Third-Party Management	10
5. IT Disaster Recovery and Resilience	11
6. IT Governance and IT Risk Management	12
7. Information Security	13
8. Enterprise Technology Architecture	14
9. Cloud Computing	15
10. Digital and Mobile Risk	16
Contacts	18

Introduction

Welcome to our annual review of the information technology hot topics facing Internal Audit functions in financial services, which is now in its sixth year.

Technology remains high on the agenda for financial services organisations. Financial institutions recognise the burden of "unfit for purpose" solutions that are both costly in the long term and more prone to risk exposures. At the same time, organisations seek to invest and innovate to compete effectively in the global marketplace, and to satisfy requirements by their global regulators.

The pace of technological development in financial services is expected to continue to create market opportunities for challenger organisations seeking to improve operational leverage and drive further investment from existing players. In the midst of this, there is definite value from, and expectation of, IT Internal Audit's ongoing efforts to understand the risk landscape and adopt new, innovative ways to provide assurance to help mitigate risk effectively.

We surveyed 23 organisations across financial services in the UK to obtain views from Heads of IT Internal Audit and Chief Internal Auditors on key areas of focus in their IT audit plans for 2017. It will come as no surprise that 'hot topics' such as cyber

security, strategic change and third-party management featured consistently across all sub-sectors surveyed. Ensuring appropriate audit coverage across these areas remains part of financial organisations' internal audit priorities. It was interesting to observe the re-emergence of Cloud Computing as a hot topic in our Top 10, as well as the elevation of Data Governance to claim the third place on the list. These topics reflect an increasing focus on alternative, cost effective use of technology and a regulatory drive to enhance governance over institutions' data in the financial services industry.

The "Analysis by Sub-Sector" section provides further insight on the topics which have made an appearance this year, while the detailed "Viewpoints by Topic" reflects the opinion of the respondents on the significance of each area, coupled with our own analysis on how InternalAudit could best tackle these topics. This year we have also added a short commentary on the challenges facing IT Internal Audit functions, based on responses collated through our survey.

As always, your feedback on the publication, as well as your insights on how to continue improving it going forward, is most welcome. I truly hope that this continues to act as a useful resource that can generate healthy debate amongst your teams and inform discussions with your stakeholders, whilst also helping with your IT internal audit planning for the upcoming year.

Mike SobersPartner, Risk Advisory



IT Internal Audit Hot Topics 2012-2017

The table compares the Top 10 IT internal audit hot topics over the past six years as identified through our annual survey of Internal Audit functions in the Financial Services industry. It highlights some interesting trends over time. The table also confirms that the core, high-profile topics have appeared consistently in the Top 10 for Internal Audit (marked in **bold**).

Rank	2017	2016	2015	2014	2013	2012
1	Cyber Security	Cyber Security	Cyber Security	Large Scale Change	Third-party management	Cyber Threat
2	Strategic Change	Strategic Change	Disaster Recovery and Resilience	IT Governance and IT Risk Management	Identity and Access Management	Complex Financial Models
3	Data Management and Data Governance	Third-Party Management	Large Scale Change	Identity & Access Management and Data Security	Data Governance and Quality	Data Leakage
4	Third-Party Management	IT Disaster Recovery and Resilience	Enterprise Technology Architecture	Data Governance & Quality	Large Scale Change	Data Governance and Quality
5	IT Disaster Recovery and Resilience	Data Management and Data Governance	Third-party management	Third-party management	Cyber Security	Rogue Trader and Access Segregation
6	IT Governance and IT Risk Management	Information Security	Information Security	Cyber Security	Resilience	Regulatory Programmes
7	Information Security	Digital and Mobile Risk	Digital and Mobile Risk	Digital and Mobile Risk	Cloud Computing	Financial Crime
8	Enterprise Technology Architecture	IT Governance and IT Risk Management	Data Management and Governance	Service Management	Mobile Devices	Third-Party management
9	Cloud Computing	Enterprise Technology Architecture	IT Governance and IT Risk Management	Disaster Recovery and Resilience	Complex Financial Modelling	Social Media
10	Digital and Mobile Risk	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 Top10 over time.

An analysis by sub-sector





Retail Banking

Survey participants across retail banking particularly underlined the challenges with Data Management and Data Governance, helping it rise into our top three. A number of international banks within scope of the global principles for effective data aggregation and risk reporting (BCBS 239) face the burden of compliance over the next few years, with IT Internal Audit teams seeking to assure how global technology infrastructure will support such initiatives.



Capital Markets

Major capital markets

organisations are faced with hugely complex IT environments serving legacy business processes that must adapt to become flexible market facing solutions. Updating and simplifying IT estates is key to reducing running costs and successfully managing operational risk. As such, the impact of mergers, acquisitions and restructuring to the enterprise architecture of global banks is another hot topic for these organisations and their Heads of IT Internal Audit, raising it to the top three for Capital Markets. Assurance that these projects are soundly managed and deliver on benefits is key to support business growth and ensuring

that the organisation can withstand competition and meet regulatory requirements.



Investment Management

Retail banks have traditionally been at the forefront of digital services; from our responses it is clear that investment managers are now also recognising this as a hot topic for their business models. These organisations are increasingly using alternative digital servicing models (such as Robo-Advisors, online sales platforms) to offer services to clients. This has now come under the attention of the Financial Conduct Authority (FCA) with the launch of a Robo-Advice unit in 2016 and will become an increasingly prevalent topic in the sector.



Insurance

The Insurance sector is facing similar challenges, focusing on streamlining their complex legacy environments and establishing appropriate governance and risk frameworks to manage the risks arising from the use of new technologies. Interestingly, the topic of Data Management and Governance is not in the Top10 for insurance firms, possibly due to prior years' attention over data through Solvency II initiatives.

Rank	Financial services	Retail Banking	Capital Markets	Insurance/ Investment Management
1	Cyber Security	Cyber Security	Large Scale/Strategic Change	Cyber Security
2	Strategic Change	Large Scale/Strategic Change	Cyber Security	Third-Party Management
3	Data Management and Data Governance	Data Management and Governance	Enterprise Technology Architecture/Mergers Integration/ Obsolescence	IT Governance and IT Risk Management
4	Third-Party Management	IT Governance and IT Risk Management	Third-Party Management	Merger/Integration
5	IT Disaster Recovery and Resilience	Information Security	Data Management and Governance	Large Scale/Strategic Change
6	IT Governance and IT Risk Management	Enterprise Technology Architecture	Information Security/Identity & Access Management	Cloud Computing
7	Information Security	Third-Party Management	Disaster Recovery and Resilience	Digital and Mobile Risk
8	Enterprise Technology Architecture	Disaster Recovery and Resilience	Conduct Risk for Tech	Incident Response
9	Cloud Computing	Conduct Risk for Tech	IT Governance and IT Risk Management	Information Security
10	Digital and Mobile Risk	IT Operations/Batch Processing	Regulatory Compliance	Enterprise Technology Architecture

Challenges for IT Internal Audit functions

Our respondents highlighted identifying, managing and retaining the right skills and audit talent as their continuing priority and concern for many functions.



Given the proliferation of technology solutions and need to keep up with technology developments, recruiting for "scarce" skills and retaining skilled staff is vital to establishing and nurturing a high performing Internal Audit team. We observe that salaries for "scarce" skills have been steadily increasing

Participants also highlighted the challenge of keeping up with the evolving "threat landscape" and new requests by Board Audit Committees, its members and regulators and the drive to continuously meet their needs and expectations. An ongoing challenge is the ability to sufficiently demonstrate that internal audit coverage through the IT audit universe model adopted is sufficient across the everchanging technology landscape; as well as commensurate to the nature and complexity of risks that the organisation is facing today.

Another concern highlighted is how to audit "change" effectively given the potential limitations in the existing resource base. Furthermore, challenges were also highlighted regarding how to optimise the value added through project assurance work, which underlies the growing importance of the strategic change topic as a risk theme for Internal Audit teams.

Finally, an ongoing area of focus is embedding a successful interaction model between the three lines of defence, with clear accountability and engagement. We believe that there is definite value from Internal Audit's continuous involvement to help shape a fit for purpose model that mitigates risk effectively and increases shareholder value.

Internal Audit viewpoints by topic



Cyber security retains the top spot on our hot topics for another year, reflecting the on-going attention of the media, numerous key stakeholders and the resulting focus for Internal Audit on this high profile area. The term 'Cyber Security' continues to evolve, encompassing areas including security, resilience, crisis management, communications and fraud. Regulatory interest in preventing, detecting and appropriately managing cyber risk across financial services also shows no signs of abating. Many organisations will have taken part in the CBEST exercise in the previous year and can expect on-going dialogue and follow-up with regulators on their results. Furthermore, organisations' increasing reliance on third parties to provide business critical processes exposes them to unknown cyber security risks; for example third-party incidents can lead to critical data breaches and service. interruptions, which can have severe reputational and financial impacts.

Cyber crime is associated with malicious internal or external threat 'actors' and this is reflected in the specific reviews and cyber topics we see included in 2017 internal audit plans. In particular threat intelligence and vulnerability management was highlighted as a key area of focus next year for many Internal Audit functions. Crisis management and incident response frameworks were also highlighted, reflecting the sentiment that organisations recognise that it is a question of 'when' and not 'if' in regards to a cyber incident occurring. For larger organisations with more mature frameworks. Internal Audit attention is also now turning towards control assessment and cyber risks associated with their overseas offices, off-shore service centres and thirdparty providers. We are also seeing the more mature and larger Internal Audit teams recruiting specifically for 'Cyber Audit Directors' and expanding their specialised teams in this area. This is

likely linked to our survey results which highlighted the challenges Internal Audit faces in responding to the expectations of stakeholders for how assurance over 'Cyber' is being covered in internal audit plans. An important step for Internal Audit is to clearly understand what 'Cyber' means for their organisation and ensure that this is consistently reflected through their internal audit plans.



Note: The number in brackets indicate the ranking of the topics in our 2016 survey and the relative movement this year



2. Strategic Change (= 2)



Constant change is the new reality for financial services organisations with strategic transformation projects a critical element of maintaining a sustainable business. The success or failure of such initiatives can have a substantial impact on regulatory compliance, business performance and the confidence of stakeholders. Such transformation projects place increasing demands on technology and may necessitate largescale initiatives to upgrade or replace ageing legacy systems. At the same time, large IT programmes are driven by organisations' realisation that the market is more competitive than ever and technology provides an opportunity to innovate, differentiate and succeed against competitors. Technology developments and projects must maintain the stability of the IT environments and optimise running costs, while enabling new, innovative solutions to be delivered to customers.

Internal Audit plays a vital role in assuring strategic project reviews, in particular through continuing to challenge management on how project execution risks are controlled. The focus should not just be on adherence to project management frameworks, but also seek to help provide assurance around whether the project remains viable, will deliver its intended benefits and remains. aligned with organisational strategy. We have seen instances where Internal Audit functions are deploying up to 40% of the internal audit plan effort on transformation assurance, leveraging dedicated change assurance resources complemented by specific subject matter experts. The ongoing challenge by Audit Committees to Internal Audit functions is how to ensure adequate coverage across the change portfolio and timely audit "presence" that can deliver high value, impactful, recommendations whilst minimising disruption to programme resources.



3. Data Management and Data Governance (▲ 5)

Data Governance includes a set of processes, frameworks and systems that ensures that data assets are formally owned and managed across the enterprise, particularly with regard to their availability, usability and security. Recent and upcoming regulatory requirements and the changing data technology landscape mean that this will be a core area of focus for organisations and internal auditors alike, so it comes as no surprise to see Data Governance rising to the top three of the 2017 hot topics.

The costs and complexity of data remediation work may be a prohibiting factor, but firms will need to bite the bullet sooner rather than later. The EU General Data Protection Regulation (GDPR) and Safe Harbour 2.0, create new data privacy and protection compliance demands (e.g. a consumer's 'right to erasure'). Regulators want financial services organisations to provide better quality data, faster, and

at the same time harness the potential of their data for own operational excellence purposes. A number of key risks associated with ineffective data management and governance includes regulatory non-compliance (e.g. regarding BCBS 239 and GDPR which have explicit data management and governance requirements), cost and operational impact associated with poor data quality (e.g. resulting from a high volume of manual adjustments) and inaccurate reporting impacting both business decisions and regulatory submissions.

Internal Audit teams are increasingly providing audit coverage over a number of areas including assessing compliance with regulatory initiatives and evaluating the Data Governance strategy and framework. This can be supplemented with Analytics techniques and the use of sophisticated data modelling, quality and profiling tools to holistically assess the data environment.





4. Third-Party Management (▼ 3)



Third-Party Risk has become a regular Board level agenda item as a result of growing global regulatory attention around the use and control of third parties for key business activities. Third-party 'ecosystems', also known as the 'extended enterprise', are becoming more prominent sources of strategic advantage and the scale on which this is now taking place in financial services has increased significantly¹. Relevant third-party risks are particularly prevalent for technology functions given the overall spend, reliance upon, and materiality of technology service organisations. Inconsistency in approach and weak controls around third-party risk management can result in significant financial, reputational or regulatory damage. Refer also to topic 9, Cloud Computing. The Office of the Comptroller of the Currency (OCC) and the Financial Conduct Authority (FCA) have led the way in terms of guidance on third-party risk management, highlighting the need for increased risk management assurance over all third parties, including external, intra-group and inter-entity third parties. There is also a need for greater Board level

oversight, resulting in a need to enhance internal reporting processes and central visibility, even for internal material suppliers. This is something that Structural Reform programmes have recently brought to the fore.

Although for specific risk areas SOC 1 type reports can provide Internal Audit with a level of coverage, the assurance requirements are much wider. Internal Audit departments should look to expand their remit and consider ways to increase their own assurance coverage. Many organisations, for example, perform diagnostic maturity assessment of the approach to third-party risk management against good practice and regulatory requirements, assess compliance with existing third-party risk management policies and procedures, or seek to evaluate the quality, relevance and reliability of underlying data in relation to third-party portfolios.

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



5. IT Disaster Recovery and Resilience (▼ 4)

By the term 'resilience' respondents did not just refer to their organisation's ability to prepare for, respond to, and recover from adverse risk events but also aptitude to withstand such disruption, maintaining the availability and performance of services across diverse and complex technology landscapes. As a recent Deloitte paper highlighted², there is increased supervisory interest in the area of operational resilience, particularly with regard to the increased dependencies of financial services firms on the resilience of the IT infrastructure, coupled with an increased level of threat from cybercrime and other non-technology events. For example, as some respondents in our survey reported, the current, increasingly fragile geo-political situation and the ongoing uncertainly and impact from "Brexit" are key items in their agenda.

Resilience is critical wherever customers and regulators expect high availability of services. Regulators are asking how firms ensure that they will be able to maintain client services, in particular for controlling access management and managing change. Resilient systems in retail financial institutions improve services to customers and reduce the risk of regulatory intervention. Equally, high-performance, high-availability and resilient systems are critical for Capital Markets organisations in maintaining an edge over competitors and liquidity in markets where fast response times and access to data underpins profitability. Technology is weaved within every product or service of financial services firms; consequently, Internal Audit functions are starting to move away from assessing isolated disaster recovery or resilience testing events and instead looking to assess end-to-end technology architecture and its relative importance, in order to provide an opinion over the operational resilience of the organisation.



Outlook for Financial Markets Regulation in 2016;
 Deloitte Touche Tohmatsu Limited, 2016



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



IT Governance remains a key component of Internal Audit plans. In the wake of recent corporate scandals, not only corporate governance but also IT governance are being singled out as the root cause. Respondents to our survey highlighted that this topic warrants a place in their internal audit plans as the robustness of IT governance practices and transparency of decision making processes underpins performance across a number of other subjects.

The ISO/IEC 38500:2015 standard as well as the Control Objectives for Information and Related Technology (COBIT5) continue to be leveraged by Internal Audit departments in their assessments of organisational compliance against established frameworks. Besides these more traditional approaches however, some Internal Audit departments also elect to assess elements of governance or risk

culture as part of their root cause analysis on every standard IT audit.

The related topic of IT risk management is also a focal point for Internal Audit teams which are required by the Audit Committee to assess the capability of the first and second lines of defence to manage IT risk proactively and also comply with enterprise risk management requirements and regulatory obligations. Given the pace of technological change, the threats and opportunities posed by the rise of emerging technologies and the real challenges that IT Risk teams are now facing, IT Internal Audit clearly has a crucial role to play. Through assurance activities, continuous monitoring, independent challenge and a healthy day-to-day engagement, Internal Audit should help drive a closer alignment with Technology, IT Risk functions and the wider operational risk teams.



7. Information Security (▼ 6)

Many organisations that participated in the survey continued to differentiate between the topics of Information Security and Cyber Security, while others used the terms interchangeably. In most cases this distinction is served by the relative position of the threat; with Cyber typically aligned to malicious threats deriving from external sources in the cyber realm, and Information Security aligned to risks around the security of data, or information (and information systems) more broadly. Consequently, Information Security is often seen to include some of the more traditional concerns such as identity and access management, application security and secure development. Many financial services organisations continue to face significant challenges in these areas, for example with large identity and privileged access management remediation programmes underway.

Interestingly a number of responses highlighted that management attention and investment was becoming too focused on "overly hyped" cyber initiatives, such as threat intelligence monitoring, with a concern that traditional, operational, Information Security controls were being overlooked as a result. Internal Audit has a role to play in ensuring that focus is maintained across the full breadth and depth of Information Security operational controls, commensurate to the nature of the information risk exposures and risk profile of the organisation.





8. Enterprise Technology Architecture (▲ 9)



Enterprise Technology Architecture emerged as a theme in our publication three years ago, and has remained a hot topic in our listing ever since. The complexity of technology estates has resulted in environments which are ever more difficult to manage and maintain. In many instances this is the legacy of underinvestment or lack of timely upgrades of systems, which now remain in production but are unsupported or prohibitively expensive to maintain. In other cases, a lack of effective systems integration during past merger and acquisition activities has resulted in a complex environment of applications and platforms. As well as increasing operational costs and associated risks, this has also impacted the ability to remain competitive against the evolving market landscape featuring new entrants, such as FinTech start-ups and challenger banks.

As IT departments struggle under the burden of managing complex legacy estates, Internal Audit functions also face the challenge of how to cover this risk sufficiently in their internal audit plans in a way which adds value to management, rather than simply re-iterates a known problem. Some survey respondents report significant audit activity to assess the large-scale programmes in place to replace legacy systems or flag the need to pay close attention to consolidation activity with regard to the impact this may have on the stability of the existing environment. As a result such considerations are front and centre of continuity and resilience audit activity for many organisations.

(P)

9. Cloud Computing (NEW)

Although, the term 'cloud' is not especially well defined, it usually means the different types of IT services (infrastructure, operating system and applications) provided over the internet. Advantages of cloud-based services, such as those provided by Amazon Web Services or Microsoft Azure, include speed of deployment (and decommissioning), flexibility, scalability and cost. The Financial Conduct Authority (FCA) has tried to level the playing field for new market entrants, FinTech and RegTech providers and recently released guidance on its expectations for financial services firms using cloudbased services. This has clarified the FCA's appetite for use of cloud and has set out clear control expectations for cloudadopters, treating cloud-based services in line with other outsourced services. The latest guidance brings some important additional requirements, which Internal Audit functions will have to consider when providing assurance over the use of cloudbased services.

Third-party assurance reports (such as SOC1 or 2) may be considered adequate to

assess certain controls which are aligned to well understood international standards or operated on a pervasive basis across all of the cloud providers' services to all customers. However, this will not be sufficient for critical or material services which have been designed uniquely for that firm.

Furthermore, there is a need to ensure that there are no contractual restrictions. on the number of requests the firm, its auditor or the regulator can make to access or receive data; and that data is not stored in any jurisdiction which inhibits the UK regulator's effective access to data. This would have a significant impact on the Internal Audit function's ability to discharge assurance responsibilities. In addition, outsourced services should not be a barrier to the orderly wind-down or resolution of a firm, and the outsourcing provider should agree that resolution procedures or change-in-control should not be regarded as a contract termination. Specifically, firms should be able to exit outsourcing relationships without undue disruption to their services.

Perhaps the most significant impediment to the use of cloud services has been removed however, with the amendment in the FCA's guidance of the explicit need for firms to have access to "the business premises of the service provider", with the FCA clarifying that this does not necessarily mean the data centres in which the firm's data is housed. Regardless, Internal Audit functions will need to take care that their assurance plans are not impaired by a lack of access to key cloud environments, particularly as the extent of use of such service models becomes increasingly prevalent across the organisation.





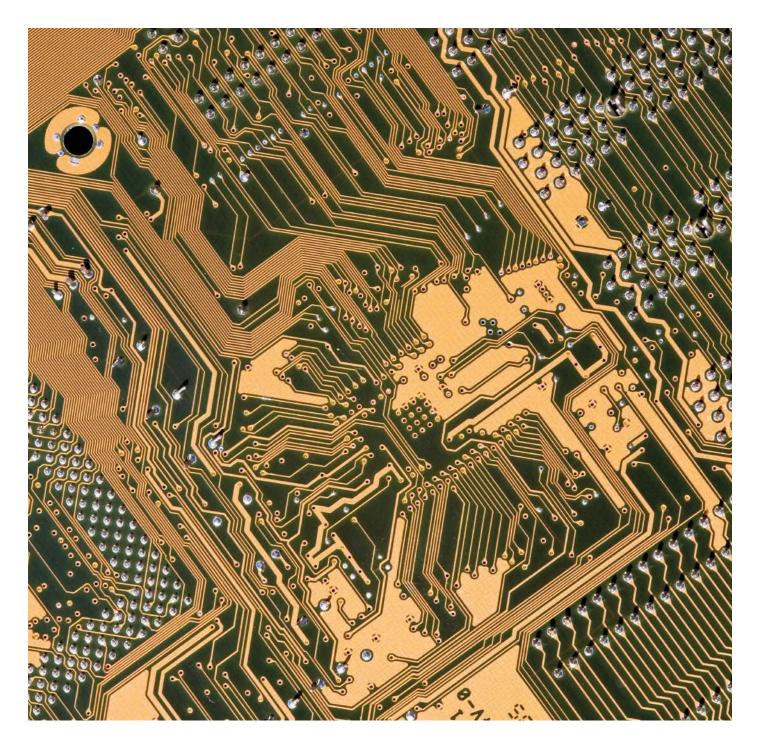
10. Digital and Mobile Risk (▼ 7)



Although as a topic Digital and Mobile Risk has dropped a few places in our top 10, the use of Social Media, Mobile, and other Digital platforms is growing. As a response, many organisations are investing heavily in Digital Transformation programmes to build or improve customer experience. This has led to IT Internal Audit teams being asked to evolve their practices and help promote a balance between digital innovation and management of risk, governance and compliance.

Inherent risks resulting from traditional servicing models are now changing and new risks are surfacing. Mobile devices for instance, (both corporate or employee-owned devices) have introduced a number of new device and network configuration risks that are expected to challenge traditional approaches to risk management. Such risks include legal risks, with the potential implications of storing data on mobile devices, including whether and how litigation and e-discovery requirements might apply.

Internal Audit teams continue to explore relevant risks and consider innovative audit approaches to provide adequate assurance in this area; we are seeing many functions setting up specific teams and designing plans to focus on their organisation's Digital initiatives. Internal Audit need to stay at the forefront of regulatory requirements and guidance on Digital technologies, while continuing to interact with the business to ensure that the governance and oversight mechanisms are in place through strategy, policy, awareness and monitoring.



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

Technology remains high on the agenda for financial services organisations. Financial institutions recognise the burden of "unfit for purpose" solutions that are both costly in the long term and more prone to risk exposures. At the same time, organisations seek to invest and innovate to compete effectively in the global marketplace, and to satisfy requirements by their global regulators.

Notes

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), 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.co.uk/about for a detailed description of the legal structure of DTTL and its member firms.

Deloitte LLP is the United Kingdom member firm of DTTL.

This publication has been written in general terms and therefore cannot be relied on to cover specific situations; application of the principles set out will depend upon the particular circumstances involved and we recommend that you obtain professional advice before acting or refraining from acting on any of the contents of this publication. Deloitte LLP would be pleased to advise readers on how to apply the principles set out in this publication to their specific circumstances. Deloitte LLP accepts no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

© 2016 Deloitte LLP. All rights reserved.

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. J9726