Deloitte.

Assurance for growth
2015 planning priorities for internal audit in financial services

An Internal Audit viewpoint

Introduction

Internal audit departments in the financial services sector continue to operate against a backdrop of heightened regulatory scrutiny, emerging best practices and increasing stakeholder expectations. We do not expect these challenges to ease in 2015.

In the wake of last year's Chartered Institute of Internal Auditors guidance ('the CIIA guidance'), we published *Looking ahead: 2014 Hot Topics for internal audit in financial services.* This highlighted a number of emerging topics including governance, culture, risk appetite and conduct risk.

As functions develop their plans for the coming year, many of the headline priority areas will be familiar. However, beneath these headlines there are a number of new areas of focus. Many of these are driven by the development of new strategies and business models in response to increased economic confidence, shifting regulatory priorities, and the need for audit functions to build on 2014's 'first-cut' approaches to topics such as governance and culture.

In planning for 2015, internal audit functions continue to face a number of broader challenges to ensure that their approach to these areas is effective and insightful. These include:

Subject Matter Expertise: Specialist resources are needed to offer rigorous challenge in technical areas, in particular where policy and control design has been the preserve of experts, for example across some areas of risk and technology. More judgemental areas such as risk appetite, governance, strategic decision making and culture also require subject matter expertise. The recruitment market for internal auditors with relevant skills and experience remains an extremely competitive one.

Methodology: Continued improvement of internal audit approaches and toolkits to take account of emerging practices, for example in data analytics, governance, risk culture, and outcomes testing.

Stakeholder Management: Engagement with a broader stakeholder group and handling of increasing expectations, in particular those of audit committees, executives and regulators. Functions should also ensure that stakeholders understand Internal Audit's remit in, and approach to, sensitive areas such as strategic decision making.

It continues to be an exciting and interesting time to be involved in financial services internal audit, and functions have the opportunity to add insight and value to their organisations. We hope this document proves to be useful as you plan for 2015.

Key areas explored in this publication

Business leadership
- Governance
- Changing corporate strategy
- Individual accountability
- Subsidiary governance
- Corporate culture

Risk management
- Risk appetite frameworks
- Risk culture
- Operational risk
- Reputational risk
- Model risk lifecycle

Regulatory matters
- Conduct risk
- Product governance
- Financial crime

Capital and liquidity
- Regulatory change agenda
- Data quality
- EMIR
- Solvency II

Trading
- Valuation controls and processes
- Wholesale conduct
- Unauthorised trading programmes

IT
- Cyber security
- Disaster recovery and resilience
- Large-scale change

Accounting and tax
- IFRS 9
- FRS 102
- COSO 2013 Framework
- Tax risk management

Delivery challenges

Subject Matter Expertise

Audit teams will need to be of appropriate experience and standing to challenge senior stakeholders in judgemental and sensitive areas such as culture, governance and strategy.

Methodology

Audit teams need to define their role, approach and tools in providing assurance over firms' attestations to regulators. Internal Audit should develop the format of Audit Committee reporting in support of thematic observations on culture and governance.

Stakeholder Management

There is increased stakeholder reliance on Internal Audit in support of personal attestations and individual accountability. Resourcing plans will need to be sufficiently flexible to enable functions to provide assurance at short notice over, for example, mergers and acquisitions.

Business leadership

The intense scrutiny over the **governance** of financial institutions will inevitably continue following the issues and failures observed in the global financial crisis. Internal audit functions have largely embraced the CIIA guidance, performing more extensive work in this area with many developing multi-year plans to cover their governance universe. These will need to be revisited in 2015 to ensure that a number of new priorities are addressed, such as those noted below.

It is expected that 2015 will bring a marked increase in mergers and acquisitions, divestments and restructurings across the sector. Internal Audit should ensure that it has appropriate coverage of the information used to support strategic decision making, as well as the emerging risks that come with a **changing corporate strategy** and structure.

From a regulatory perspective, **individual accountability** has emerged as a theme given the recent consultation paper on the introduction of new Senior Managers and Certification Regimes in the banking sector. Senior executives and board members are increasingly being asked to provide personal attestations to regulators on a range of topics, including the effectiveness of the governance, risk management and control environments. Senior stakeholders will look to Internal Audit to provide assurance over control self-certification processes, as well as the detail behind individual returns.

Another important area is the robustness of **subsidiary governance**. Internal audit functions should have an appropriate focus on this issue, including consideration of the composition of subsidiary boards, reporting lines from subsidiary or business unit executives and control functions to Group functions, and the quality of management information (MI) for the legal entity. Internal audit plans need to demonstrate appropriate coverage of all entities for which the regulator holds the function responsible, including work performed in other jurisdictions.

Corporate culture continues to be an area of regulatory interest, with boards and executives facing challenge on whether desired behaviours have been effectively articulated and embedded, and whether the board has defined its approach to measuring that the right outcomes have been achieved. 'Tone from the top' has long been an area of importance in assessing culture, but the 'tune from the middle' is receiving increasing recognition as organisations look to middle management to help embed behavioural change. Consequently, internal audit functions should look to gauge culture at a number of levels in their organisations.

Risk management

In recent years organisations have invested significantly in the development of **risk appetite frameworks** and the governance and training needed to embed them. Internal Audit has tended to focus its work to date on the design, implementation and project management of risk appetite frameworks and audit plans should include follow-up work on any identified weaknesses.

In 2015, plans should include work on the operating effectiveness of the risk appetite framework, and the way in which it is used to manage risk and bring broader value to the organisation (i.e. the extent to which the framework is embedded into day-to-day business operations). For example, as many firms develop their plans for growth, audit priorities should include how risk MI is used to inform decisions on business strategy at all levels, from the Board downwards. Internal Audit should also provide challenge over how risk appetite measures and limits are used to drive day-to-day operations and whether the intended levels of improved risk management are being achieved.

Last year many internal audit departments developed their 'first-cut' approach to auditing **risk culture**. With good internal audit practice continuing to emerge, functions will need to regularly review and refine their approach and tools in this area. Organisations continue to develop their approach to defining, embedding and measuring risk culture, and therefore the list of auditable activities and controls also continues to develop.

Operational risk continues to be an area of focus, with organisations making improvements in a number of areas over the past 18 months. These include the linking of operational risk to strategic objectives, and embedding operational risk scenario analysis in the business and using it to validate non-financial assumptions in recovery and resolution plans. Internal audit should include thematic reviews of the extent to which the business has progressed and embedded these enhancements in plans for 2015, as well as testing the design and effectiveness of the operational risk framework.

In some organisations **reputational risk** has emerged as a separate risk class, distinct from operational risk, with its own risk committee and approval process. Internal audit functions need to keep up to date with changing practices in risk categorisation, and the impact of resulting framework redesigns, in this and other areas where risk management practices are evolving quickly such as conduct risk.

The effectiveness of internal audit coverage across the **model risk lifecycle** (design, development, validation, implementation and application) is an area of regulatory concern, and should be reflected in plans for 2015. Functions are expected to review and challenge model risk within a structured model risk audit programme (for example, as described in CRR Article 191 for Basel II Credit Risk Internal Ratings Based approach). Internal Audit's coverage of model risk should be structured to ensure that a firm's model governance policy framework and current status is appropriate to manage risk appetite, meet regulatory requirements (particularly where models are used for capital purposes) and deliver the control environment expected by external auditors (where models are used to inform values in the financial statements). Internal Audit cannot place sole reliance on the work undertaken by Model Validation functions (where they are in place) and, on a targeted basis, should review and potentially re-perform the work to ensure the level of challenge, analysis and assessment meets the requirements of a second line control function.

Delivery challenges

Subject Matter Expertise

Resourcing models will need to support the increasing need for specialist audit leads and teams to challenge the business in areas such as risk framework design, implementation and effectiveness, and model risk.

Methodology

Audit plans need to have appropriate breadth and depth of work on model risk management frameworks and controls. Risk-based metrics should be used to direct and focus audit challenge. Audit methodologies and outputs will need to evolve to reflect changing practices in risk categorisation and better align operations and reporting across the three lines of defence.

Stakeholder Management

Internal Audit will need to clearly explain its role in providing assurance over the risk management framework to avoid stakeholder perceptions of duplication with the other lines of defence.

Regulatory matters

The FCA is increasingly interested in firms' strategies and the adequacy of their controls to manage **conduct risk** whilst seeking growth and increased profitability. Firms need to ensure that customers remain central to their business strategies, and that growth and profitability do not deliver poor customer outcomes resulting in regulatory sanction and the need for customer remediation. The ability of firms to define and monitor conduct risk, and embed a 'customer-centric' culture throughout their organisations is essential. Internal Audit should assess the frameworks, policies and procedures in place to safeguard customers and adhere to regulatory requirements, as well as independently challenging customer outcomes for appropriateness.

In its 2014 Conduct Risk Outlook, the FCA highlighted the issues that can arise due to information asymmetries between firms and their customers. For firms designing and distributing products, **product governance** is a key area of focus and should be high on the Internal Audit agenda in 2015. Products should have a clearly defined target market and organisations must demonstrate that appropriate target customers buy the product. The fairness of contract terms, pricing and product information (including financial promotions) are all key areas that should form integral parts of product design and review processes. The focus of firms and, by extension, internal audit functions should not be confined to current products; legacy product governance is also an important area.

Internal Audit should provide challenge over the appropriateness of changes in policies, procedures and controls in response to specific pieces of regulation and thematic reviews. Examples include the recent Mortgage Market Review, the post-Retail Distribution Review thematic findings on compliance with adviser charging and 'independence' requirements, Policy Statement 14/9 Review of the client assets regime for investment business, and regulatory commentary relating to remuneration codes and staff incentives.

Financial crime remains an area of concern. With its 'intensive and intrusive' approach, the FCA wishes to ensure that firms maintain and enhance systems and controls to address financial crime and that senior management has clear responsibility for managing financial crime risks. Recent anti-money laundering fines continue to highlight failings in relation to identifying and managing higher risk customers. With the impending introduction of the fourth EU Money Laundering Directive, Internal Audit is expected to be able to assess firms' existing financial crime capabilities and highlight areas of potential weakness. Financial sanctions imposed by the UK, US, EU and UN remain an area of priority and should continue to be firmly on the Internal Audit agenda, (particularly given recent developments with Russia and the Ukraine), to ensure firms can adapt systems and controls in a timely manner. The increasing trend in the use of attestations by the FCA should also be an area of focus, to ensure that work carried out to support management attestations is robust and would stand up to regulatory scrutiny.

Delivery challenges

Subject Matter Expertise

Audit teams will need to have appropriate expertise in assessing customer outcomes, as well as being able to consider whether policies and procedural controls have been adhered to. Assessing customer outcomes is a judgemental and skilled area, and internal auditors will need to clearly document the rationale for their conclusions. Teams will also need to challenge whether firms' conduct risk appetites and supporting MI are appropriate.

Methodology

Audit methodologies need to be designed to enable customer outcomes to be explicitly considered in audits covering a wide range of functions and activities. This provides an opportunity for increased use of data analytics. This creates its own challenge as the use of analytics remains relatively immature for many internal audit functions and embedding this into the audit methodology requires expertise and a focus on long-term benefits.

Stakeholder Management

Heads of Internal Audit can expect supervisory challenge over the breadth and depth of internal audit oversight of the factors influencing customer outcomes.

Capital and liquidity

The prudential **regulatory change agenda** continues apace, driven by a combination of Basel III, Solvency II and the final elements of the wider G20 response to the financial crisis. Following the introduction of the new CRD IV regime for capital in 2014, minimum mandatory requirements for Liquidity Coverage Ratio (LCR) will be introduced in 2015, with the Net Stable Funding Ratio (NSFR) and Leverage Ratio to follow. The breadth and complexity of change, together with the evolving and uncertain nature of the final calibration of key regulatory ratios (for example LCR, NSFR and leverage ratio), brings numerous challenges from a practical and operational standpoint, not least ensuring that governance, internal controls and qualitative standards are updated and are operationally effective to maintain compliance.

The robustness of internal control frameworks around capital (including the calculation of Risk Weighted Assets), liquidity and leverage metrics, and the completeness and accuracy of related Common Reporting Framework (COREP) regulatory reporting and external Pillar 3 regulatory disclosures, should be a priority area of focus for Audit Committees and Boards in 2015 due to:

- The increasing reliance placed on regulatory capital ratios by investors, shareholders and regulators, in particular as a trigger point for bail-in under the new UK Recovery and Resolution Directive;
- A step change in the volume, complexity and granularity of data submitted to regulators under COREP and Financial Reporting (FINREP), and for regulatory stress testing; and
- The PRA and Bank of England focus on **data quality**, and more broadly on personal accountability under the new Senior Managers' Regime.

As a result, there is an increasingly important role for Internal Audit in providing assurance on a variety of Basel III (CRD IV) areas. The focus for independent review and challenge is expected to be on the significant areas of new regulation, for example additional capital deductions, additional capital charges for Credit Valuation Adjustment, the leverage ratio, the LCR and NSFR, and the new regulatory reporting templates in COREP and FINREP.

The **European Market Infrastructure Regulation** (EMIR) requires standardised OTC derivatives to be cleared through central counterparties (CCPs); derivatives which cannot be cleared to be subject to bilateral margining arrangements; and OTC and exchange traded derivatives to be reported to a trade repository. One of the most significant implications of EMIR is the pledging of collateral to the CCPs. Organisations have had to develop processes and controls that enable them to validate their exposure to a CCP and to deliver or recall collateral on a timely basis to mitigate the exposures. Stakeholders will look to Internal Audit to provide an opinion on the robustness of the control framework for EMIR compliance together with assurance that the regulatory obligations from EMIR are being met.

For insurers, **Solvency II** (which goes live on 1 January 2016) is split into three pillars covering technical provisions and capital requirements, system of governance and regulatory reporting. The key challenges for Internal Audit will be to ensure the Solvency II implementation plan is flexible in responding to the large-scale changes within the business, particularly around the increased quantum and granularity of regulatory reporting. Audit plans should include project assurance around Solvency II readiness, independent validation of the models or reviewing preparatory phase reporting.

Delivery challenges

Subject Matter Expertise

Audit teams will need to include appropriate technical expertise around areas such as EMIR, Basel III (CRD IV) and Solvency II to ensure effective scoping and rigour of work.

Stakeholder Management

Internal audit teams will need to ensure that their roles and responsibilities for assuring regulatory change programmes are clearly defined against, and aligned with, the other lines of defence.

Trading

Continued regulatory focus on **valuation controls and processes** has led many internal audit functions to increase their level of resource with quantitative expertise, sometimes hiring former front office staff or risk managers who have detailed product knowledge. This has enabled functions to challenge in complex areas such as the model approval and independent price verification processes in a more detailed and analytical way. We expect regulators to look to place increasing reliance on the work of Internal Audit in this regard.

Given the number of regulatory issues and fines levied on banks relating to **wholesale conduct** matters, providing assurance on conduct related matters is a significant area of focus for many audit functions. The number of mandatory audits in this area continues to increase as new regulation (such as the FCA's MAR 8.2 and the EURIBOR Code of Conduct) mandate periodic audits of the relevant benchmark submission process. Many institutions have sought to extend their work in this area beyond the mandatory requirements to cover other similar benchmarks, indices and related price setting processes such as foreign exchange market fixes.

Significant unauthorised trading events remain a key risk area for many trading businesses due to the material financial and reputational impact an event could have.

Operational risk, and increasingly the front office, take a lead in managing unauthorised trading risk, through designing and implementing control frameworks which effectively capture all risks across institutions, which can prove challenging. Reviewing and challenging the effectiveness and completeness of **unauthorised trading programmes** is a focus area for many internal audit functions.

Delivery challenges

Subject Matter Expertise

Audit teams will need appropriate expertise in wholesale conduct and associated regulation. Specialist audit leads are required to challenge the business effectively in the areas of unauthorised trading, model approval and independent price verification. These skills command a premium in the marketplace and candidates often do not have associated internal audit experience.

Methodology

Audit tools and approaches will need to be refined to support the effective delivery of mandatory regulatory audits.

IT

Internal audit functions continue to face challenges in keeping up with the pace of technology change and retaining the right skills to provide assurance over the complex technical landscapes which prevail across the financial services sector. In our view, audit plans for 2015 should continue to prioritise some of the more traditional areas of technology risk which support the sustainability of firms.

Cyber security remains high on the agenda for many organisations, in part due to increasing regulatory scrutiny and government-backed exercises to assess the readiness of firms to respond to cyber threats. In particular, an industry-wide ethical security test (CBEST), which aims to test the stability of the UK financial system, has received board-level attention in many organisations leading internal audit functions to continue their focus on assessing the various layers of cyber defence, including intelligence and monitoring capabilities alongside processes to detect, prevent and importantly manage the impact of cyber attacks.

Recent high-profile system outages for high street banks and other firms across financial services have increased corporate and regulatory focus on **disaster recovery** processes and systems **resilience**. Despite "Dear Chairman" letters having been issued to significant financial services firms, outages impacting ATM and branch networks, payment systems and ultimately customer access to services continue to cause regulators and organisations to focus great attention on the stability of their systems. Internal Audit has an important role in the provision of assurance over the adequacy of resilience controls and processes, the effectiveness of change controls and the maintenance programmes which firms have in place to keep their systems running.

Internal audit functions are devoting more time and resource than ever before to providing assurance over the **large-scale change** in which their organisations are investing to meet regulatory demand and drive growth. Given the high technological content of change programmes in areas such as Solvency II, Basel III, COREP and IFRS 9, IT specialists have a significant contribution to make to multi-disciplinary internal audit teams in delivering appropriate and robust challenge.

Delivery challenges

Subject Matter Expertise

Internal audit functions face a challenge in having the skill sets necessary to audit the 'in-depth' approaches which organisations are taking to address cyber risk. Functions have also found it difficult to retain the technology skills necessary to assess resilience across their complex technology estates.

Greater reliance is being placed on Internal Audit to help assess data governance and data quality in support of broader business audit reviews.

Methodology

Internal Audit is increasingly expected to assess whether required outcomes are being achieved by large-scale change programmes, as well as whether programme governance controls are operating effectively. Many functions will need to develop their approaches and range of reporting tools to deliver flexible, timely assurance in these areas.

Stakeholder Management

Whilst technology is at the heart of the cyber and disaster recovery topics, the impact of these reviews is significantly enhanced by engaging business stakeholders, in areas such as communications, public relations and crisis management.

Delivery challenges

Subject Matter Expertise

Audit teams will require specialist experts with knowledge of the relevant accounting standards, tax rules and regulations across different jurisdictions. Effective assurance over IFRS 9 readiness programmes will require a combination of project management, technical accounting and impairment modelling skills, as well as knowledge of the broader operational implications of the standard.

Accounting and tax

IFRS 9 *Financial Instruments (*effective 2018) remains the highest profile accounting standard on the horizon. It will have a direct, quantifiable impact on loan loss provisions and financial instrument valuations and therefore on both the balance sheet and income statement. It is also expected to impact indirectly on a wide range of factors contributing to enterprise value. The most significant change within the standard is the expected loss provision model which replaces the incurred loss model used under IAS 39. Delivery of this forward-looking methodology represents the key challenge of IFRS 9 for financial institutions. The resulting model will rely heavily on the completeness and accuracy of data from multiple sources (including risk, finance, operations and treasury) which will have been subject to varying degrees of control, oversight and independent scrutiny in the past. The controls over these inputs will therefore be a critical area of focus.

Many organisations have started multi-year implementation programmes which capture the design, build and test phases of their IFRS 9 projects to ensure delivery of a robust solution by 2018. Internal Audit should include these programmes, as well as their project management and governance arrangements, within its plans from 2015 to ensure that key design principles and associated risks are challenged from an early stage.

Other accounting developments which should be monitored by Internal Audit include changes to the standards on leasing, insurance ('IFRS 4, Phase II'), and, for current UK GAAP reporters, the introduction of **FRS 102** *The Financial Reporting Standard applicable in the United Kingdom.*

Internal audit functions should challenge the implementation and embedding of the **COSO 2013 Framework** (effective 2014) by their organisations in connection with Sarbanes Oxley 404 (SOX) compliance and an increased focus on internal control over financial reporting. While the 2013 Framework's internal control components (control environment, risk assessment, control activities, information and communication, and monitoring activities) are the same as those in the 1992 Framework, companies are now required to assess whether 17 principles underpinning these components are 'present and functioning' in determining whether their system of internal control is effective. Many organisations are also taking a fresh look at the identification and monitoring of key SOX controls and their wider control environment. Areas where Internal Audit might increase its focus in 2015 include control activities affected by non-routine transactions or events, the effectiveness of management review controls, and performing periodic tests of general IT controls, source information and data transfers.

Financial services organisations continue their focus on ensuring that their **tax risk management** is fit for purpose and aligned with their broader commercial strategy and risk management approach. In recent years HMRC has introduced the Senior Accounting Officer rules, and consulted on strengthening the Code of Practice on Taxation for Banks. Internal Audit should provide appropriate coverage of related initiatives and controls in 2015.

Contacts

Financial Services Internal Audit

Mark Fitzpatrick
Vice Chairman and Partner
020 7303 5167
mfitzpatrick@deloitte.co.uk

Paul Day
Partner, Banking and Capital Markets
020 7007 5064
pauday@deloitte.co.uk

Russell Davis
Partner, Banking and Capital Markets
020 7007 6755
rdavis@deloitte.co.uk

Matthew Cox
Director, Insurance
020 7303 2239
macox@deloitte.co.uk

Terri Fielding
Partner, Investment Management and Private Equity
020 7303 8403
tfielding@deloitte.co.uk

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

Kevin Doherty
Partner, Technology
0141 304 5711
kedoherty@deloitte.co.uk

Jamie Young
Partner, Regions
0113 292 1256
jayoung@deloitte.co.uk

Owen Jackson
Director, Regions
029 2026 4297
ojackson@deloitte.co.uk

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. 39143A