Deloitte.

Exponential change
2016 planning priorities for internal audit in financial services

An Internal Audit viewpoint

Introduction

This is our 2016 publication on Internal Audit planning priorities.

Financial Services organisations continue to operate in an environment of exponential change due to continued advances in technology, adoption of new regulations as well as competition from new entrants to the sector. It will be another year of change and Internal Audit departments will need to keep abreast of technology developments, adjust to new regulatory requirements while managing emerging risks and meeting ever expanding stakeholder expectations.

Internal Audit plans for 2016 should be developed keeping in mind the exponential changes that will impact the financial services industry. Internal Audit departments have to adjust and adapt to the regulatory requirements, emerging risks and competition impacting the industry. This change presents a unique opportunity for Internal Audit to lead as a catalyst for change in their organisation for the longer term.

Indeed the challenge is multi-faceted. All of the 2015 planning priorities remain relevant, however, there is a greater spotlight on the way organisations behave with recognition that this is only as good as the weakest link. Expectations from regulators and customers are more demanding than before. Threats such as cyber are being exploited with greater frequency and to greater effect while customers expect greater digital capabilities. New entrants without the burden of legacy platforms or working practices are increasingly successful in meeting these customer needs.

This document covers "*What Internal Audit should do to address the exponential changes*" within the financial services industry and assesses the impact on audit approaches, methodologies and resource models. There is a common theme relating to adequacy of skills and experience in Internal Audit to provide opinions on this range of topics.

This document provides you with our thinking and we hope it proves useful as you prioritise and plan for 2016.

Key areas explored in this publication

Business leadership

- Corporate & risk culture
- Communication
- Annual audit opinions

Risk management

- Risk appetite framework
- Insurance coverage
- Operational risk
- Model risk

Regulatory matters

- New regulators
- Retail conduct
- Financial crime
- Client assets

Capital and liquidity

- Solvency II
- Data quality
- CRD IV

Trading

- Product & valuation controls
- Unauthorised trading
- High frequency and automated trading

IT

- Cyber crime
- IT Disaster recovery and resilience
- Digital forces
- Continuous risk assessment

Accounting and tax

- Tax risk management
- COSO 2013 framework

Business leadership

Corporate & risk culture

A strong **corporate culture** drives positive outcomes and a competitive edge for organisations. In the past year, organisations have worked hard to demonstrate tangible progress on corporate culture through their actions to embed the desired culture, including the "tone from the top" along with their middle management's "tune in the middle" messages.

To sustain the corporate culture across an organisation, leadership teams must be able to measure the progress on their culture transformation programmes so that they know where further enhancement is required. In response to this, many Audit Committees and key stakeholders are demanding that Internal Audit include culture reviews as part of Internal Audit's work. It is a powerful message to regulators, rating agencies and the organisation that the leadership is serious about getting its corporate culture right by requesting Internal Audit to independently carry out culture audits and then management addressing the report with corrective actions.

Many Internal Audit professionals agree **risk culture** assessment is not a fad, risk culture measurement, monitoring and management have been 'hot topics' on regulatory agendas since the financial crisis in 2008. Financial services organisations have continued to develop their risk culture assessment programmes as most organisations now recognise that risk management processes, systems and internal controls are only as good as the behaviour of the people operating or overseeing them. The debate within Internal Audit has moved from should risk and control culture be included in the risk based audit plan to what granularity of risk culture should be covered in its audit plan.

The role of remuneration and incentive arrangements remains important and is becoming more complex. These need to be aligned to the culture and risk appetite of the organisation to ensure the right behaviour is recognised. Many organisations are revising their balanced and risk-adjusted scorecards as well as deferral and clawback arrangements.

As a result, there has been a shift in the work performed by Internal Audit Departments from generic risk and control culture audits to specific audits on a more granular sub risk culture, for areas like conduct risk, operational risk and market risk. Risk culture assessment is becoming an established measure for assessing the quality and embedding of an organisation's strategic plan, risk appetite, governance structure, risk management and remuneration framework. It is becoming increasingly common for Internal Audit to include aspects of assessing organisation's risk and control culture in their annual planning process.

What can Internal Audit do to address this?

Internal Audit should include within its scope review of corporate culture and evaluate the hard and soft controls around corporate culture.

In organisations where leadership have defined the corporate culture, Internal Audit work can be designed around hard controls like codes of ethics/conduct, policies and procedures, organisation structure and roles, responsibilities and authorisation levels. In addition, Internal Audit work should address soft controls like competence, strong leadership, values, ethical standards and equality.

In organisations where the target corporate culture is not defined, Internal Audit can develop a cultural assessment framework by considering a proxy corporate culture baseline considering factors such as management's philosophy and operating style, organisation size and structure and human resources practices.

Three approaches that Internal Audit should take for risk culture audits are:

- **Risk culture specific audits**. Internal Audit should assess the evidence for each of the risk culture indicators in its Risk Culture Assessment Framework to determine an aggregate view of the overall risk culture in the area, function of business unit in scope for the audit.
- **Risk culture consideration in all audits**. A risk culture element is included as a "bolt on" to other audits by carrying out a root cause analysis to identify if any behavioural drivers were primary or secondary causes for the audit findings.
- **Continuous monitoring**. Internal Audit should report on the positioning of the organisation's risk culture against a selection of key risk culture indicators from the organisation's Risk Culture Assessment Framework. There is wide recognition by internal auditors that scorecard approaches alone do not work for assessing risk cultures. A quantitative score card approach, such as a percentage or Red, Amber, Green ratings, will not fully capture an assessors' or Internal Audit's view of an organisation's culture. The behavioural nature of culture means the results of a culture assessment can only be fully set out with qualitative descriptions as well as quantitative scores.

Communication

Communication is the process of transmitting messages or information by an organisation internally (with staff) or externally (customers, regulators or other stakeholders). Organisation's communications are fundamental to helping customers make informed decisions. Regulators expect that organisations embed an organisation-wide culture where the importance of effective communication with customers is recognised and prioritised.

Customers are increasingly using social media to engage with an organisation and if managed appropriately this can be a very effective way in which organisations can engage with their customers. However, when things go wrong, social media is an additional and more real time channel through which an organisation can incur reputational damage given 24/7 coverage by news channels on 'viral' events (including corporate events). It is therefore critical that organisations effectively manage their communication channels and that they consistently convey the proper tone in their communications in a timely manner, regardless of the medium used.

What can Internal Audit do to address this?

Incorporate the review of corporate communication to evaluate the current framework and governance of communication strategy (both internal and external communication), day to day operations of communication management (how past communications were handled), review of effectiveness of communications, benchmark across peers or the industry.

In organisations where there is a defined communication strategy, Internal Audit has a baseline to design the audit work. Where the organisation has not defined a communication strategy, Internal Audit should supplement its team with individuals with appropriate experience to be able to define a reasonable expectation for the strategy.

Annual audit opinion

Providing an opinion on the design and operating effectiveness of the organisation's internal controls continues to be challenging for Internal Audit Departments. Expectations from a number of stakeholders including Audit Committees, senior executives and regulators continue to evolve, to supplement the emerging view of the internal audit profession.

The issuance of an annual audit opinion acts as an acid test as to whether audit coverage has been appropriate – can it be distilled into an opinion on the design and effectiveness of internal controls and the organisation's risk and control culture?

Reporting the annual audit opinion provides additional comfort to the Board of Directors regarding the organisation's system of internal controls. The work required to support annual audit opinion reporting should be considered as part of the annual audit needs assessment in order to ensure there is sufficient coverage and that it is prioritised appropriately.

What can Internal Audit do to address this?

- Determine whether Internal Audit will obtain the required level of support for its opinion through the audits contained in the annual audit plan.
- Challenge its annual audit plan throughout the year to ensure that it aligned to changes in the risk profile of the business.
- Consider where and how its view of risk and control culture has been captured.

Risk management

Risk appetite framework

Financial services organisations have continued to invest time and resources, particularly at the senior management level, in developing **risk appetite frameworks** during 2015, with many organisations requesting their Internal Audit Departments to conduct an audit of the risk appetite framework. Many Internal Audit Departments have based these audits on the Principles for an Effective Risk Appetite Framework, published by the Financial Stability Board in November 2013. However, these organisations have found that it requires a degree of interpretation and therefore many Internal Audit Departments have required technical support to scope and execute such an audit. Typical findings from audits conducted during 2015 include failure to adequately demonstrate a linkage between the Board level risk appetite statements and standards applied by the business, along with a lack of evidence relating to roles and responsibilities for risk appetite across the three lines of defence.

What can Internal Audit do to address this?

During 2016, Internal Audit should consider assessing the effectiveness of the risk appetite framework by considering two views:

- The horizontal view – the insights gained from the stress testing and reverse stress testing conducted as part of the Internal Capital Adequacy Assessment Process (ICAAP). Do the statements, measures and calibration of the limits in the risk appetite framework appear reasonable and in line with the regulatory requirement? How are the roles and responsibilities for the risk appetite framework being defined and how are they being incorporated?
- The vertical view – is there a clear view of how the detailed policy limits and standards aggregate to the Board of Directors' approved risk appetite statements and measures?

Insurance coverage

Directors and officers **insurance coverage** has a high profile at Board level. With increasing focus from the regulators and other external bodies on the growing accountability of the Directors, Boards of Directors are seeking increased comfort that their insurance policies are going to operate effectively in the event the Directors or officers of the organisations need to make a claim. It is important that Internal Audit are able to challenge the processes in place to review the insurance-buying decisions made by the organisation's in-house insurance function, and understand how the policies tie back to the organisation's risk appetite.

What can Internal Audit do to address this?

Auditing of internal insurance functions by Internal Audit, where the responsibility for purchasing and evaluating the insurance needs of an organisation lies, will:

- Require specialist technical expertise to appropriately challenge the processes and resources in place.
- Review the suitability of insurance cover to identify errors, gaps and inadequacies in an organisation's current coverage, as well as unnecessary insurance cover.
- Test for a transparent and robust premium allocation model.
- Ensure compliance with tax rules and regulations, as well as consider international licensing requirements.
- Insurance broker selection reviews, whereby the option to change the organisation's broker of record through a formal tender and review process, has the potential to bring significant cost savings and attain a better advisory and insurance buying service.

Operational risk

As organisations continue to develop and fine-tune their **operational risk** assessment methodologies and taxonomies, thus building a richer picture of the potential risks, effective prioritisation of risk mitigation comes into focus and will become more crucial. Internal Audit should incorporate an assessment of the quality of decision making and extent of the risk mitigation activity by senior management.

Elements of the operational risk framework have often been developed and introduced as separate frameworks and methodologies (e.g. risk appetite, risk assessment, scenario analysis, issues management, loss data capture, etc.). Many organisations now face the challenge of integrating these elements into one coherent and dynamic framework. Without an integrated framework, the processes may not offer a practical solution to day-to-day risk management, and may not facilitate control environment improvement as expected by the regulators. Internal Audit should assess the quality of linkages between the identification, assessment, mitigation and monitoring/reporting stages of the risk management cycle.

What can Internal Audit do to address this?

- Review the risk management framework and provide assurance on the risk management process.
- Evaluate the reporting and management of key operational risks of the organisation.
- Make sure reviews cover key factors such as appropriateness of governance, staff seniority and management information and these should be assessed on a factual basis. Where judgment is used, Internal Audit should ensure it has the appropriate skills and should provide clear rationale for its conclusions.
- Incorporate the concept of probability of operational risk events crystallising and the magnitude of the potential impact of such events when assessing the mitigating activity.

Model risk

With the increasing use of complex quantitative models throughout the financial services industry, model risk has become a major concern for the Boards of Directors, Regulators and external parties like insurers, banks and investment managers. Model risk is largely the potential for inaccuracy and/or inappropriate use of models, which can lead to substantial financial losses and reputational damage.

The Boards and regulators are particularly concerned about the materiality and magnitude of model error and its wider impact on the financial services industry. As a result, the regulators expect Internal Audit Departments to have a strong focus on specialist regulation and technical concepts, particularly where models are used for regulatory purposes (e.g. capital adequacy). Internal Audit should provide an independent evaluation of the effectiveness of model risk governance and controls, model risk appetite and model risk identification in organisations. In order for Internal Audit to provide an independent assessment of the model risk framework, Internal Audit staff should ensure it has relevant subject matter expertise.

What can Internal Audit do to address this?

- Develop a top-down approach to address model risk which transparently demonstrates how compliance with regulatory expectations will be delivered over a 12 month (and longer) horizon.
- Provide an assessment to the Board of Directors on the management of model risk (identification, measurement, monitoring and control) with reference to the entity's clear statement of model risk appetite. This requires an annual plan of aligned model risk audit activities which cover all relevant regulations, all model types and all stages of the model lifecycle (design, development, validation, and application).
- Develop audit programmes that include a combination of deep dives on a sample of material models (selected consistently with model risk quantification), supplemented with high level reviews of a broader range of models and supported by continuous monitoring of model risk metrics.
- Test regularly the ongoing independence between model development, validation and application teams. Internal Audit should also test whether the distinct modelling cultures enable a balanced management of model risk, which allows the full range of technical, operational and commercial concerns to be addressed.

Regulatory matters

New regulators

The European Union's supervisory architecture has undergone major transformation, as two new banking regulators have assumed their powers – the Single Supervisory Mechanism (SSM), with the European Central Bank in charge, and the Single Resolution Mechanism (SRM) which is led by the newly established Single Resolution Board. Amongst its priority areas, the SSM is working on the validation of internal capital models, the calculation of risk-weighted assets, reduction of discrepancies in prudential requirements across countries, and business model viability. The SRM expects to be fully operational from 2016.

This expansion of supervisors and responsibilities will raise regulatory activity and the interaction of regulators with organisations, it will also broaden the scope of activities that are under active scrutiny within a financial organisation, leading to a greater demand on staff at organisations and likely expectations of higher standards at least in some areas. Supervisory relationships will become more complex and more challenging to manage. At the same time, there will be an increased benefit for organisations to getting things right first time, as well as monitoring for future priorities and areas of focus.

What can Internal Audit do to address this?

Include an assessment of regulatory changes that have impacted the organisation. Internal Audit should play a key role in understanding the changes that are being implemented throughout the organisation.

Objectively monitor and assess regulatory changes and their implementation. Report progress of the organisation to its key stakeholders i.e., audit committee, executive management, and the regulators.

Use its knowledge to evaluate the risk assessment process to incorporate regulatory reforms in its risk based audit plans.

Retail conduct

In recent years, the FCA and the financial services industry has focused on embedding greater awareness and integration of retail conduct risk within an organisation's risk framework and appetite. The organisations should demonstrate that conduct-focused behaviour and customer outcomes are truly embedded and play an integral part in all strategic and operational decisions. A significant amount of time and effort has already been spent by front line business and risk functions enhancing their organisation's conduct risk management capabilities. However, concerns remain around how truly embedded is the customer centric culture within organisations and whether behaviours support the overall framework to deliver good outcomes for customers.

Client assets continues to be a challenging and ever increasing hot topic. It will remain an area of key focus for the regulators.

What can Internal Audit do to address this?

Focus of Internal Audit in retail conduct has shifted from undertaking standalone review to integrating conduct risk into existing audit activities. While standalone retail conduct audit reviews provide comfort to the Board on the mechanisms in place to effectively manage conduct risk and achieve fair client outcomes, integrated audits add depth to the audit in relation to conduct.

Internal audit should carry out organisation wide reviews to provide broad assurance on the internal control environment that supports the delivery of fair customer outcomes. This benefits Internal Audit in three ways:

1. Allows Internal Audit to be flexible in their approach to the assessment of conduct risk.
2. Helps demonstrate early on (to the regulators and other interested parties) that the entity does not a have rigid and inflexible framework, and proper retail conduct is truly embedded in all activities.
3. Adds additional value to an organisation by showing that the embedding of conduct risk is not limited to the first and second lines of defence.

This approach provides consistency in coverage throughout Internal Audit's annual audit plan, and provides better insight into how well conduct is considered, embedded and managed within the organisation.

Internal Audit should focus on client money reconciliations, client money segregation as well as looking at an organisation's responses to the rule changes and how they have been implemented, both in terms of process changes and system enhancements.

Financial crime

Financial crime remains a key concern for the regulators, as indicated by their continued supervision and enforcement activity. This long term and continuing trend is evidence that organisations are still struggling with the basic requirement to establish appropriate systems and controls to identify and manage financial crime risk.

Organisations across the industry are at different stages of maturity with their financial crime arrangements and those potentially most at risk can often be the least prepared. Therefore, from the regulators' perspecive, they will further ensure that the accountability for an organisation effectively in managing its financial crime risk, sits squarely with its senior executives. It is only set to increase with the adoption of the fourth EU Money Laundering Directive and with the introduction of additional supervisory techniques.

Financial sanctions continues to be a high priority for Governments and financial organisations so should be considered alongside other areas of crime prevention to ensure a holistic view of financial crime risk. Achieving this for some organisations remains a considerable challenge. Organisations may need to consider the adaptability of their financial crime arrangements (especially systems), given the frequent changes and amendments that are made to sanctions at an international, supranational and domestic level.

What can Internal Audit do to address this?

Internal Audit has a growing challenge in determining specific areas of their organisation's financial crime arrangements warrant their attention. Given the extent to which these arrangements change in terms of systems, people and processes, Internal Audit also needs to consider the experience and knowledge of their teams before undertaking these complicated audit activities. Internal Audit are applying more qualitative techniques (including risk analytics and management information reporting) to provide better coverage against an organisation's increasingly complex arrangements. This includes a focus on the overall financial crime culture, reliability of management information and capabilities across the organisation. Internal Audit should also contribute towards a comprehensive and sustainable financial crime compliance programme going forward along with existing operational risk functions in the future.

Capital and liquidity

Solvency II

Starting on 1 January 2016, European Directive 2009/138/EC, which is known more commonly as **Solvency II**, sets out a step change in capital management, risk and governance frameworks and regulatory reporting for all European insurers in its scope. Solvency II's main aim is to protect policyholders' interests by making insurers more resilient and less likely to fail, thereby reducing market disruption. Insurers have a choice to use a Standard Formula to calculate their capital requirements under Solvency II, or to produce an Internal Model which must be validated. These models are accompanied by the new Own Risk and Solvency Assessment (**ORSA**). There will also be public (Solvency and Financial Condition Report (**SFCR**)) and private (Regulatory Supervisory Report (**RSR**)) reporting of the Solvency II results for organisations.

What can Internal Audit do to address this?

For Solvency II, Internal audit should consider:

- Engagement with business on the development of capital models and reporting infrastructure for Solvency II.
- Liaising with governance committees on key responsibilities for Solvency II.
- Evaluating the adequacy and effectiveness of the internal control system of governance.
- Ensuring flexibility in annual audit plans to accommodate work supporting the development of Solvency II.
- Considering whether Internal Audit possesses the necessary expertise to review the programmes and models.
- Oversee projects supporting the implementation of Solvency II.

Internal Audit should also ensure its approach is aligned with that of its organisation by:

- Understanding and reassessing changes in the business operating model and governance structures.
- Appreciating changes in the Board of Directors' attitude to risk including risk appetite and tolerances.
- Understanding the challenges facing the organisation and its business under Solvency II.

Data quality

Data quality that is fit for purpose for capital and liquidity reporting allows financial organisations to maximise their value from data, whereas poor data inhibits the achievement of strategic goals and potentially exposes the organisation to significant regulatory risks, operational challenges, loss of market competitiveness and wasted costs. This can include incorrect CRD IV regulatory capital reporting (such as risk weighted assets and capital ratios) and incorrect Value at Risk (**VaR**) results for management oversight of the organisation's capital. Furthermore for global systemically important banks, under the Basel Committee on Banking Supervision (**BCBS**) 239, the requirement for effective data aggregation and risk reporting becomes effective in early 2016. BCBS 239 has specific principles focused on data quality and data governance, and as part of the governance principles, it sets out a requirement for ongoing independent validation of Risk Data Aggregation processes – i.e. Internal Audit should audit data quality.

Internal Audit should play a pivotal role in enhancing the control environment and reducing the risk of poor data quality by conducting reviews of data quality processes. In addition, focused reviews of associated governance practices of data rich processes should be reviewed. Use of analytics in Internal Audit is an effective way to identify data quality issues in thematic reviews to ensure the data is of sufficient quality to get value from analytics.

What can Internal Audit do to address this?

Internal Audit should develop data governance skills and knowledge to review the appropriateness of governance, whilst also having deep understanding of data quality techniques and practices.

Internal Audit should also review data quality practices & processes and consider the use of analytics to re-perform the controls in place. The broader data governance will be another key area for review, including clearly defined roles and responsibilities, policies, standards, reporting and escalation across the business.

Finally Internal Audit should undertake BCBS 239 (Basel Committee on Banking Supervision) preparedness audits of the organisation to determine the level of compliance with the BCBS 239 Principles.

Basel 3/CRDIV

Capital Requirements Directive (CRD) IV implements Basel 3 in the European Union and prescribes rules covering capital, leverage, liquidity, corporate governance and regulatory reporting. The new rules were applicable from 1 January 2014, subject to a number of transition points. Implementations for some of the capital and liquidity requirements are on a phased basis through 2019 and beyond.

CRD IV has led to increased expectations on Internal Audit. Increasing regulatory expectations around capital, liquidity, stress testing and models result in higher demands on Internal Audit, both from regulators and from management.

What can Internal Audit do to address this?

For institutions with internal models to calculate regulatory capital, CRD IV imposes a requirement on Internal Audit to assess compliance with all applicable regulations (typically annually) in the following areas:

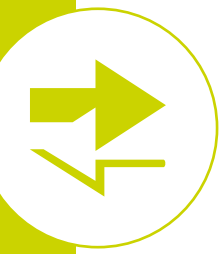
- Internal Ratings Based Approach for Credit Risk;
- Internal Model Method to calculate exposure on derivatives (Counterparty Credit Risk); and
- Value at Risk-based models for Market Risk in the Trading Book.

In addition, CRD IV requires Internal Audit to review valuation processes and controls for fair value positions and trading book policies and procedures, irrespective of whether the bank has model permission. More generally, Internal Audit is expected to provide assurance over the management of the significant risks that CRDIV seeks to address.

In performing these reviews, Internal Audit should consider:

- Management's self-assessment of compliance with CRDIV and remediation of areas of non-compliance.
- The extent to which tactical solutions implemented to meet the tight timelines associated with CRDIV implementation are being replaced with strategic solutions.
- Data quality and accuracy of internal reporting
- Stress testing process and controls.
- Proposed changes to Basel 3 (Fundamental Review of the trading book, revised standardised approach across credit risk, securitisations, counterparty credit risk, market risk an operational risk, for example).
- Management's ability to manage significant "risk change" portfolios.

Internal Audit should also ensure it has sufficient expertise to provide challenge to management across this wide range of technical disciplines.



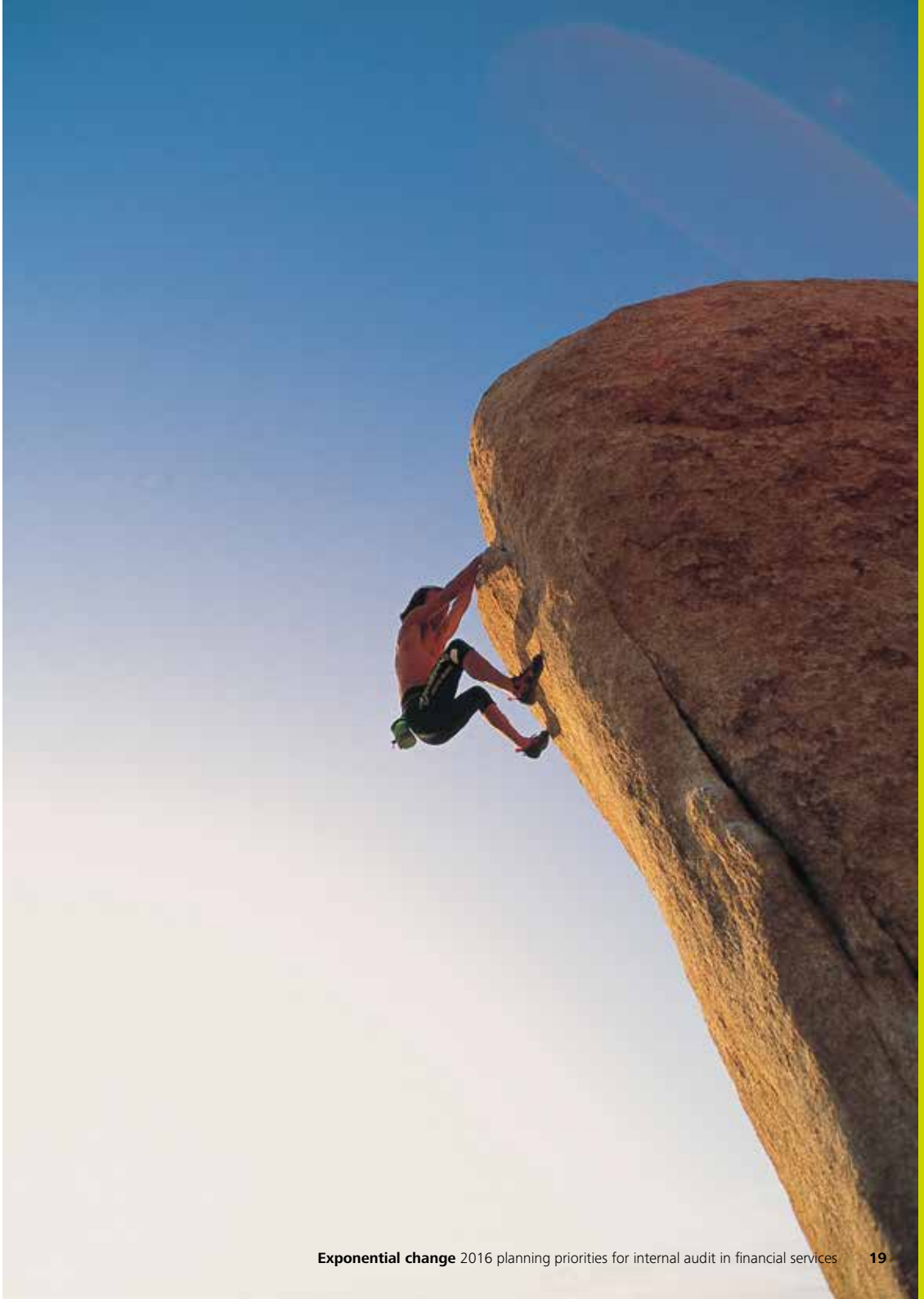
Trading

Product and valuation controls

The regulators remain of the view that product & valuation controls at many financial services organisations are not yet at the desired standard. This is often due to system infrastructure weaknesses which remain the root cause of many control problems. The forthcoming prudent valuation regime, which is expected to be finally approved by the European Commission later this year, will place further expectations on these organisations to produce and manage comprehensive data on the valuation risk of the organisation, which can only be done effectively on top of a well-designed control environment. Identifying and challenging an organisation's product & valuation controls should remain a key priority for Internal Audit over the next year. In addition, Internal Audit should also consider the broader control activities of the organisation which contribute to the valuation controls, rather than just defining them narrowly as the Independent Price Verification (IPV) process.

What can Internal Audit do to address this?

To effectively audit this area, it is important that Internal Audit Departments should include individuals with the appropriate technical and product knowledge to challenge the organisation and raise insightful observations. A strong background in an Internal Audit Department of a significant trading business will no doubt provide individuals with the grounding required, but it may be necessary and appropriate to complement this with other individuals who have backgrounds in trading or risk management, quantitative modelling and finance roles to ensure that satisfactory challenge can be provided in all of the technical areas.



Unauthorised trading

Significant unauthorised trading events remain a key risk area for many trading businesses due to the material financial and reputational impact that an event could have. The supervisory control frameworks at many financial services organisations have moved on significantly in recent years and now well established, albeit continuing to evolve. Testing and confirming the ongoing effectiveness of these frameworks should remain a focus for Internal Audit.

What can Internal Audit do to address this?

Many investment banks now have strong supervisory frameworks covering the front office that establish clear chains of supervision and also provide individuals with the appropriate information to exercise their supervisory responsibilities and evidence this in a system. Internal Audit should confirm that this process remains effectively embedded in the organisation by conducting detailed review of supervisory framework audit of front office functions.

High frequency and automated trading

The increasing use of high frequency and automated trading practices at many organisations increases their susceptibility to losses due to programming or other IT issues. For example, the volatile movement in the Swiss Franc exchange rates following its decoupling from the Euro in January 2015 caused challenges for many organisations which rely on automated hedging controls.

Finally, we note the compliance requirements of the Volcker Rule is likely to increase for organisations caught in the scope of the rules. It is expected that Volcker Rule compliance will start to require an increasingly large allocation of the annual Internal Audit budget for those organisations with capital markets divisions.

What can Internal Audit do to address this topic?

Internal Audit should use trading and IT specialists to confirm that computer based algorithmic trading and hedging methodologies and programming have been appropriately developed, tested, documented and implemented in the trading system.

Internal Audit should independently assess the adequacy of ongoing system review and back testing to confirm that the second line of defence is working effectively. Internal Audit should also review the effectiveness of the implementation of trading and hedging strategies, and in particular, the mechanisms in place to handle unusual market moves.

IT

Cyber crime

An increasingly regular feature in the media over the past 18 months has been **Cyber**, with multiple significant attacks and data breaches impacting all industry sectors, although financial services firms continue to bear the brunt. These upward trends demonstrate a fundamental shift in the nature of attacks, both in terms of complexity and persistence, driving a need for transformational change across the enterprise. High profile incidents, customers concern and media coverage are increasingly a compliance issue as well as business one, with greater regulatory scrutiny, direction and intervention than previously observed.

For many Internal Audit departments, a cyber-security incident is not so much a question of if, but when. Attacks and breaches can result in a range of costs, from technology and resources required in remediation to post-breach legal and regulatory implications. More than ever, the ability to effectively detect and rapidly respond to an attack is both essential and highly valuable. More mature organisations are proactively planning and preparing for incidents and their response, recognising the value that skills and resources can provide in such situations, and testing response effectiveness across a range of scenarios. This is not simply about fixing the vulnerability that was exploited, but wider crisis management skills, including public, media and customer relations.

With the rise in breach size, impact and complexity in 2015, incident response has seen a shift from point-based 'fix-it' type approach towards a more holistic and sustainable one. Boards of Directors and management are slowly coming to the realisation that they are not fully aware of the potential impacts of such breaches. This has necessitated more robust internal controls around incident response being more embedded and integrated into the operational risk framework of a firm as a whole to remain agile to these increasing impacts on businesses. It has also driven a need for businesses to systematically understand cyber risk at the Board level. It is an opportunity for Internal Audit functions to demonstrate that they can understand and provide assurance over all the above. In addition, they should help promote increased organisational collaboration in cyber audits, both internally (between 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 remain agile to the changing nature of cyber threats.

What can Internal Audit do to address this?

Internal Audit should:

- Adopt a people, process and technology framework so tackling cyber security issues remains strong and effective where the critical success factors are identified. This requires Internal Audit to adapt to the changing needs of their organisations, increase its awareness of the cyber security threats faced and the changing demands of regulators resulting in concerted efforts to truly comprehend the wide reaching impacts of cyber-attacks.
- Effectively deal with the challenge of the recruitment and retention of sufficiently technically skilled personnel to execute audits and investigations. The ever increasing technological component to organisational change programmes, particularly in support of many organisations' digital agenda, increases the demand for the right people within Internal Audit.
- Look at organisational collaboration in cyber-crime audits, both internally (between functions such as human resources, IT, security and legal) and externally (with external auditors and third party providers and partners), 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 as well as allowing Internal Audit to remain agile to the changing nature of cyber threats.

IT disaster recovery and resilience

IT disaster recovery and resilience remains a key area of focus for financial sector organisations. IT system failures are increasingly front page news, leading to public coverage and reputational damage for a number of financial institutions after a payments system crash. These 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. 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 their external suppliers) and the controls to mitigate them. These risks arise across technology, people and processes. With this is mind, it is imperative that Internal Audit in the coming year broaden their focus to determine the adequacy of processes in place to avoid, respond and recover from planned and unplanned outages.

What can Internal Audit do to address this?

Internal Audit should consider the adequacy of broader organisational processes in place to avoid, prevent, respond and recover from planned and unplanned outages, rather than simply focusing, for example, on whether there is a disaster recovery and resilience plan for IT in place for loss of a data centre.

Digital

Digital risks like 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. 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. Indeed, identifying, mapping and truly understanding the organisation's digital footprint will help Internal Audit 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 effectively auditing digital and unearthing the associated residual risks

What can Internal Audit do to address this?

In auditing digital, Internal Audit should:

- Include digital forces as part of Internal Audit's annual audit plan in order to provide genuine input, oversight and challenge to the digital parts of the business.
- Have the appropriate expertise and experience to independently verify the effectiveness of all elements of the organisation's digital strategy including the risk management framework.
- Identify and map the current state of the organisation's digital footprint with all associated components.

Continuous risk assessment

The recent explosion of data and management information can complicate and contradict the risk assessment as part of Internal Audit planning processes, if not managed effectively. This makes prioritising and focusing audit planning and resources an ever greater challenge. Continuous risk assessment is a method of proactively identifying areas of potential risks through regular monitoring and measuring emerging trends in the risk profile of the organisation. Use of analytics by Internal Audit functions can greatly enhance this process by identifying, measuring and readily reporting such technology risks. Automation can provide measurement of these risks on a much more frequent basis. Visualisation and dashboards can be developed for stakeholders to ensure they remain engaged and that results are clear and undisputable.

Furthermore, continuous risk assessment enables a rapid response to emerging risks, ensures the annual audit plan is continually aligned to risks, and allows for a more efficient use of resources by more precisely focusing on what matters. As well as audit planning, continuous risk assessment also supports tracking of audit actions. Simple and effective metrics can be used to demonstrate that control failures have been remediated, reducing the need for a full follow-up audit.

What can Internal Audit do to address this topic?

The key challenge for establishing and operationalising a continuous risk assessment approach is to determine what to measure, understanding its significance, and reporting in a way which is clear and compelling. Getting this right for Internal Audit requires deep knowledge of the business, the industry, risk management, as well as technical capability with data and analytics.

More practically speaking, for Internal Audit this can mean:

- Gaining the support and buy-in of stakeholders across the organisation;
- Communicating with management to address concerns over the implications of conducting continuous risk assessment;
- Engaging and collaborating with the 1st and 2nd lines of defence so there are clear roles and responsibilities, information is shared and Internal Audit maintains its independence; and
- Obtaining support from the IT function to implement or redesign technology if necessary.

In a corporate culture which fully embraces continuous risk assessment, new metrics are continually added and existing thresholds are reviewed. Implementing and embedding continuous risk assessment within wider audit methodologies along with assigning ownership and accountability for metrics are also significant challenges.

Accounting and tax

Committee of Sponsoring Organisations (COSO) 2013 framework

Many financial services organisations applied the new COSO 2013 framework to their Sarbanes Oxley (SOX) controls for the first time in 2014. In 2016, the focus is building on the lessons learned by remediating the gaps identified and using the revision in framework as an opportunity to challenge and refine the universe of SOX controls over financial reporting.

What can Internal Audit do to address this?

Internal Audit should provide independent challenge on how the COSO 2013 framework has evolved to:

- Meet the raised bar set by the COSO 2013 framework.
- Respond to challenge from the SEC
- Align itself to changing organisational structures through reform and transformation undertaken by many financial services organisations.

Internal Audit should challenge the risk assessment and scoping process for the identified end-to-end financial reporting processes against the COSO 2013 framework, recent trends in regulatory insights and best practices.

A value add to the business would be for Internal Audit to then take these learnings and apply to other control frameworks across the financial services organisations including those that cover operational risk and conduct risk.

Tax risk management

Given ongoing fiscal challenges by Governments, there continues to be significant political and media scrutiny over any aggressive tax avoidance and illegal tax evasion by those benefiting from and assisting with such activities. Consequently, tax risk management continues to be a focus for financial services organisations wanting to ensure tax strategy remains fit for purpose and aligned with their broader commercial strategy and risk management approach.

In particular, banks with private banking businesses should have appropriately designed and effectively operating controls to prevent the bank from knowingly being involved in aggressive avoidance and tax evasion on behalf of their clients. Similarly, financial services organisations should have effective governance and supporting controls for their own tax exposure. Where the potential tax risk is material for the organisation or its clients, Internal Audit should consider audits of tax governance and related controls to challenge their effectiveness.

What can Internal Audit do to address this?

Internal Audit should have access to tax experts with knowledge in recent tax legislation and tax risks to effectively challenge how the organisation:

- Manages tax risk (including transfer tax) to avoid taxation penalties and reputation damage.
- Complies with tax legislation by jurisdiction.
- Acts appropriately transparent and accurate in financial reporting disclosures and reporting.

Contacts

United Kingdom

Financial Services Internal Audit

Paul Day
Lead Partner, FS Internal Audit
020 7007 5064
pauday@deloitte.co.uk

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

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

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

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

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

Luxembourg

Governance, Risk & Compliance

Laurent Berliner
Partner - Governance, Risk & Compliance Leader
EMEA Enterprise Risk Services Leader
+352 451 452 328
lberliner@deloitte.lu

Roland Bastin
Partner - Information & Technology Risk
+352 451 452 213
rbastin@deloitte.lu

Stéphane Hurtaud
Partner - Information & Technology Risk
+352 451 454 434
shurtaud@deloitte.lu

Michael JJ Martin
Partner - Advisory & Consulting
+352 451 452 449
michamartin@deloitte.lu

Martin Flaunet
Partner - Assurance Banking Leader
+352 451 452 334
mflaunet@deloitte.lu

Eric Collard
Partner – Forensic, AML & Restructuring
+352 451 454 985
ecollard@deloitte.lu

Thierry Flamand
Partner - Insurance & Acturial Services Insurance Leader
+352 451 454 920
tflamand@deloitte.lu

Jean-Philippe Peters
Partner - Risk & Capital Management
+352 451 452 276
jppeters@deloitte.lu

Simon Ramos
Partner - Regulatory Strategy
+352 451 452 702
sramos@deloitte.lu

Johnny Yip
Partner - Assurance Investment Management Leader
+ 352 451 452 489
jyiplanyan@deloitte.lu

Michael Blaise
Director - Business Risk
+352 451 452 562
mblaise@deloitte.lu

Jérôme Sosnowski
Director - Business Risk
+352 451 454 353
jsosnowski@deloitte.lu

Bertrand Parfait
Director - Business Risk
+352 451 452 940
bparfait@deloitte.lu

Laurent de la Vaissière
Director - Information & Technology Risk
+352 451 452 010
ldelavaissiere@deloitte.lu

Designed and produced by The Creative Studio at Deloitte, London. J2279
Edited by MarCom at Deloitte Luxembourg