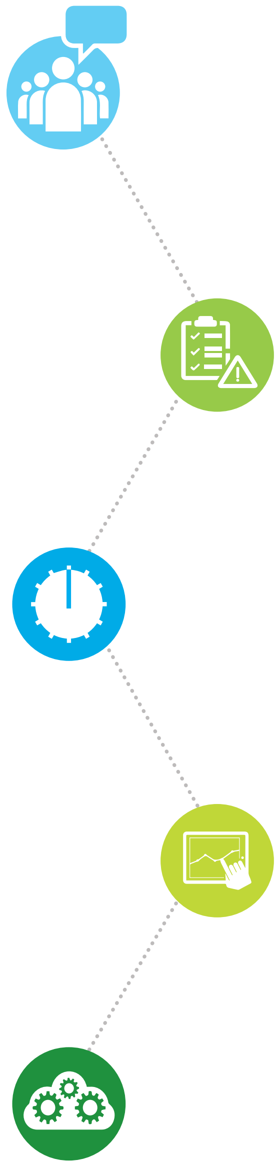
Deloitte.

Exponential change
2016 planning priorities for internal audit in financial services



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 and emerging risks. For Internal Audit, this change presents a unique opportunity to lead as a catalyst for change in their organisation for the longer term.

Indeed this challenge is multi-faceted. For 2016 there will be a greater spotlight on the manner in which organisations behave. Expectations of regulators and customers are more demanding than ever. 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 at meeting these customer expectations.

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

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

Key areas explored in this publication

Business leadership

- Corporate culture
- Communications
- Board effectiveness

Risk management

- Risk appetite framework
- Operational risk
- Model risk
- Outsourcing

Regulatory matters

- New requlators
- Retail conduct
- Client assets
- Sustainability

Capital and liquidity

- Solvelcy II
- Data quality
- Basel 3/CRD IV

IT

- Cyber crime
- Cloud migration
- IT Disaster recovery and resilience
- Digital forces
- Continuous risk asessment

Business leadership

Corporate culture

A strong corporate culture drives positive outcomes and brings competitive edge. In the past year, organisations have worked hard to demonstrate tangible progress 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 followed by management undertaking 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 Departments 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.

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, 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 can take for risk culture audits are risk culture specific audits, risk culture consideration in all audits and continuous monitoring:

- 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 or 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 to the Board of Directors and Board committees. 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 assessor's 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. It is important 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 organisations and, managed appropriately, this can be a very effective way by 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?

Internal audit plans should incorporate reviews 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, and 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 this is not the case Internal Audit should supplement its team with individuals with appropriate experience to be able to define a reasonable expectation for the strategy.

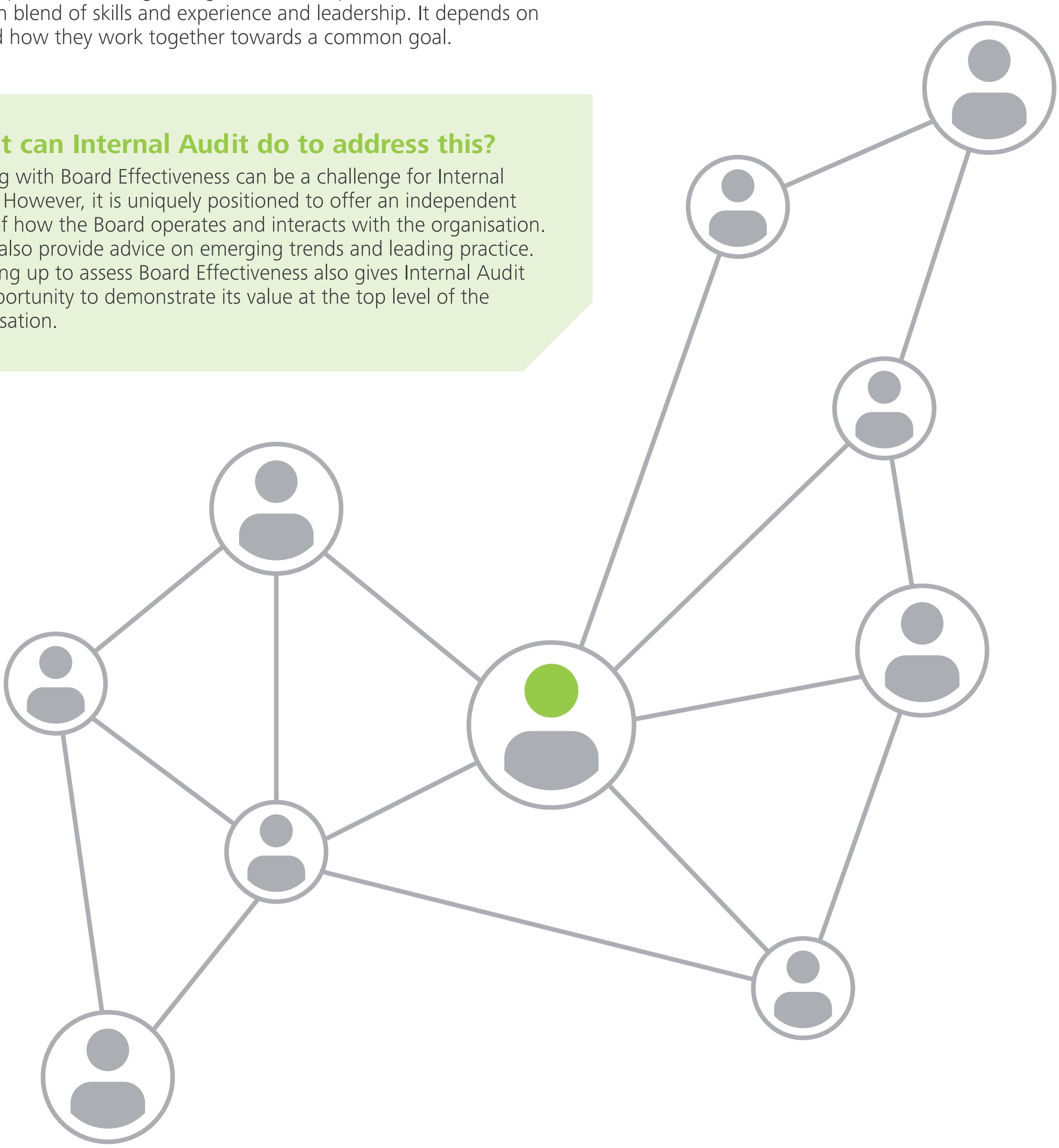
Board effectiveness

Complexity of regulation, organisational structures, technology and business relationships make being an effective Board increasingly challenging. The Companies Act places responsibility on the Board for confirming material compliance with relevant obligations. Codes of corporate governance require the Board to have the right skills and experience to lead their organisations, and to do so ethically and with integrity. Directors need to be able to demonstrate this to regulators, shareholders and other stakeholders.

There is no one right answer to the question of what makes an effective Board. It depends on having the right structures, processes, access to information blend of skills and experience and leadership. It depends on people and how they work together towards a common goal.

What can Internal Audit do to address this?

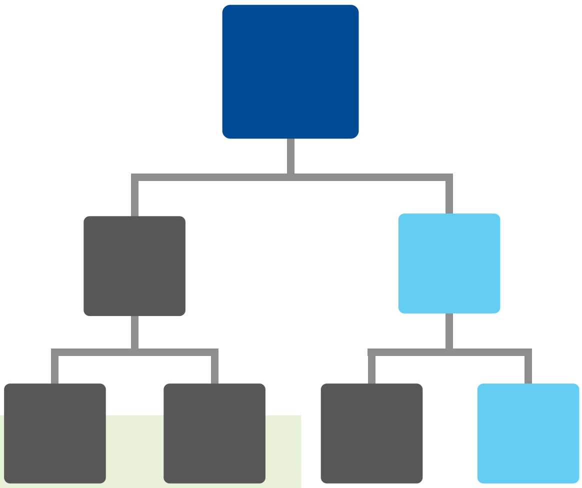
Dealing with Board Effectiveness can be a challenge for Internal Audit. However, it is uniquely positioned to offer an independent view of how the Board operates and interacts with the organisation. It can also provide advice on emerging trends and leading practice. Stepping up to assess Board Effectiveness also gives Internal Audit an opportunity to demonstrate its value at the top level of the organisation.



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 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) and Individual Liquidity Adequacy Assessment Process (ILAAP). Do the statements, measures and calibration of the limits in the risk appetite framework appear reasonable and in line with regulatory requirements? How are the roles and responsibilities for the risk appetite framework being defined and executed?
- 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?

Operational Risk

Organisations continue to develop and fine-tune their operational risk assessment methodologies and taxonomies, building a richer picture of the potential risks. This means that effective prioritisation of risk mitigation comes into focus. Internal Audit should incorporate an assessment of the quality of decision making and extent of risk mitigation activities by senior management as part of the 2016 plan.

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.

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.
- Ensure that 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.
- Assess the quality of linkages between the identification, assessment, mitigation and monitoring / reporting stages of the risk management cycle.
- 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.

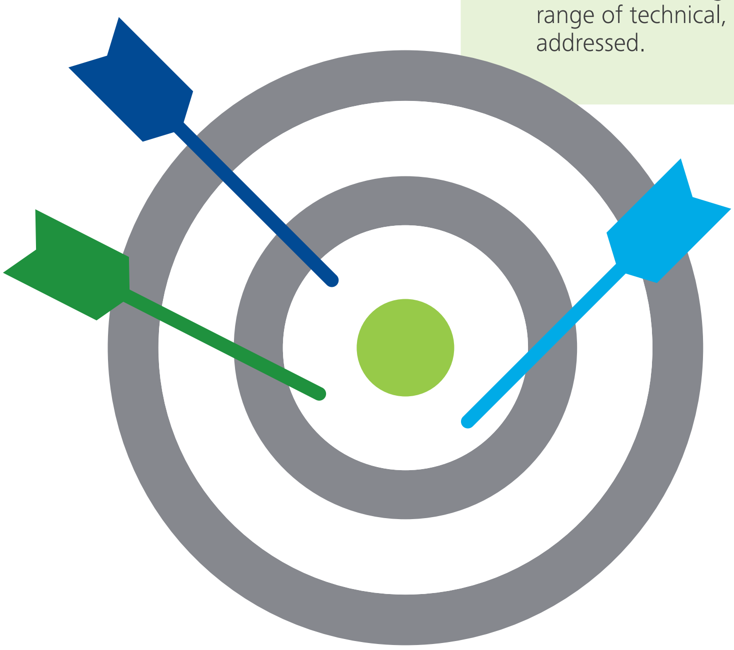
Model Risk

With the increasing use of complex quantitative models throughout the financial services industry, model risk has become a major concern for Boards of Directors, Regulators and external parties such as insurers, banks and investment managers. Model risk refers to 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 topic?

- 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 broad 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.

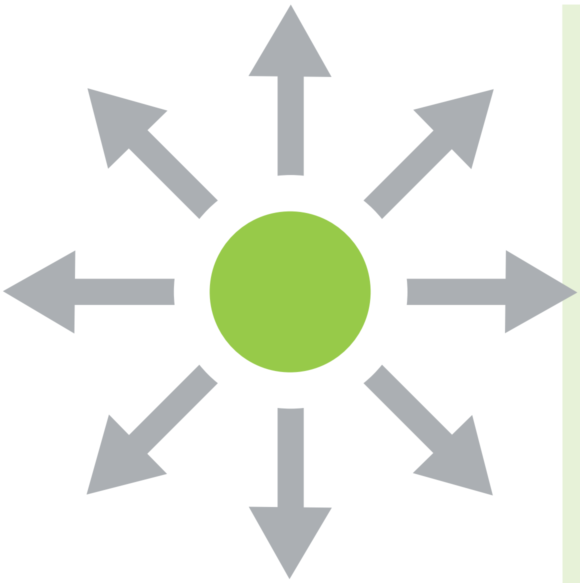


Outsourcing

Continued pressure on budgets and recruitment embargoes has meant that financial services organisations have increasingly relied on third party service organisations. In addition to cost control, organisations outsource so as to gain access to scarce skills and knowledge, and enhance business agility. Getting outsourcing right can bring significant benefits. The risks are significant as well. These include business failure leading to loss of service, accountability for illegal third party actions, or reputational damage as a result of unethical activity on the part of the service provider. The contracting organisation remains accountable for effective delivery of the overall service. While elements of service provision can be outsourced, the risks cannot.

As organisations continue to become more reliant on third parties for delivery of services, the approach of internal audit needs to evolve, reflecting that third party suppliers occupy strategic positions in organisations' business models. Reviews of day-to-day contract management and monitoring remain important, but internal audit can add value in other ways.

Outsourcing continues to be a key theme of Central Bank of Ireland (CBI) focus. The regulator has consistently re-iterated the importance of ensuring that outsourcing arrangements are adequately and appropriately documented in Service Level Agreements and that the Board of the outsourcing regulated entity ensures on a continuous basis that the outsourced services are the subject of ongoing review. The CBI expects full compliance with all applicable regulatory requirements, including the Consumer Protection Code, and appropriate oversight and supervision by firms of any such outsourced activity.



What can Internal Audit do to address this?

Consider how the decision to outsource was reached, and to whom. Look at how risks are managed within the context of the relationship, and assess whether the parties have a shared understanding of risks to the service. Assess the materiality assessment methodology to ensure that it is appropriate. If contracts include right to audit clauses, internal audit can take a closer look at the internal controls, practices, governance and culture of suppliers. Internal audit can add value by identifying characteristics of good service providers and communicating these to the business so that they are built into contracts from the start of the relationship.

Use of third party service providers and ever more complex supply chains present internal audit with a number of challenges. They also present an opportunity for it to demonstrate its value to the organisation by bringing innovative approaches based on a more profound understanding of the risks raised by outsourcing.

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 make greater demands on organisations' resources. 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. Likely areas of focus for the SSM include governance and leadership, risk appetite, reporting sustainable profitability, capital plans, models and cyber risk.

What can Internal Audit do to address this topic?

Internal Audit should plan to undertake reviews of the implementation of regulatory changes that have impacted the organisation. To provide forward-looking assurance Internal Audit should also consider the approach that the organisation is taking to planning for emerging new and amended regulation.

Throughout the audit planning and execution phases, Internal Audit must use its knowledge of regulatory change to evaluate the risk identification and assessment processes within the organisations.

Retail Conduct

Increasingly, the Central Bank of Ireland (CBI) and the financial services industry is focussing on embedding greater awareness and integration of retail conduct risk within organisations' risk framework and appetite. The CBI expects organisations to be able to 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 is being spent by front line business and risk functions enhancing their organisation's conduct risk management capabilities. Focus must also be placed on how truly embedded the customer centric culture is within organisations and whether behaviours support the overall framework to deliver good outcomes for customers.

What can Internal Audit do to address this topic?

The focus of Internal Audit in retail conduct has shifted from undertaking standalone reviews 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 regulator and other interested parties) that the entity does not have a 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.

Sustainability

Sustainability is the ability of organisations to survive and thrive over the long term. Understandably, shareholders, regulators and other stakeholders want to know that organisations are economically resilient. They want to know that their investment, be it in terms of shares bought, stability of the system, tax revenues or source of employment, is secure. At no time in the past has sustainability come into the spotlight than the present times.

Regulation forces organisations to take sustainability seriously. Financial regulators want to see that institutions have undertaken stress testing to ensure that they have adequate capital or liquidity in the event of market shocks. Investors want to know that corporate governance and internal control are in place, promoting a culture of risk management at the same time as entrepreneurial risk taking.

Sustainability is not just about long term profitability. It is also about organisations placing themselves within the communities and environment in which they operate. Consumers, concerned with the effects of commerce on people and the environment, want to know that what they buy is not the end result of unethical or illegal practices.

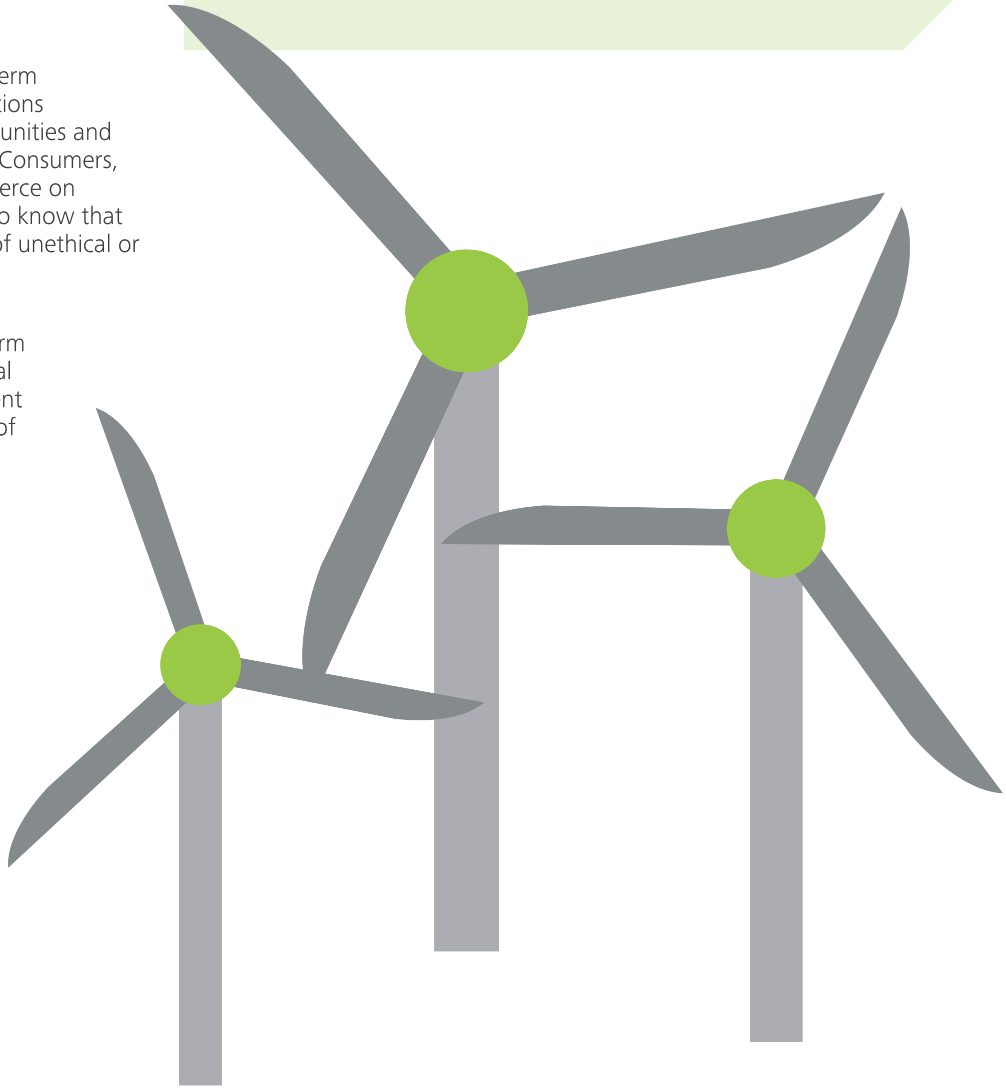
Sustainability is about seeing long term profitability, good governance, ethical practices, concern for the environment and treating people fairly as all part of the same thing.

What can Internal Audit do to address this?

Internal audit must consider sustainability when undertaking reviews of strategy, linking objectives to environmental and macro-economic factors. Using subject matter expertise, it can review models and the processes around stress testing. In human resources reviews it can consider how remuneration and bonus policies are aligned to organisational objectives and how they reinforce "good" behaviours.

Internal audit can review sustainability reporting, considering public statements made in relation to the organisation's corporate social responsibility programme. It can review or provide advice in relation to ethics programmes and ethical aspects of sustainability can be built into reviews of procurement.

Internal audit needs to ask questions about sustainability in all its activities. In addition to addressing concerns around the industry, environment and social responsibility it will help align internal audit thinking with the long term objectives of the organisation.



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 required.

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.
- Involvement in 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.

Basel 3/CRD IV

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. Implementation 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:

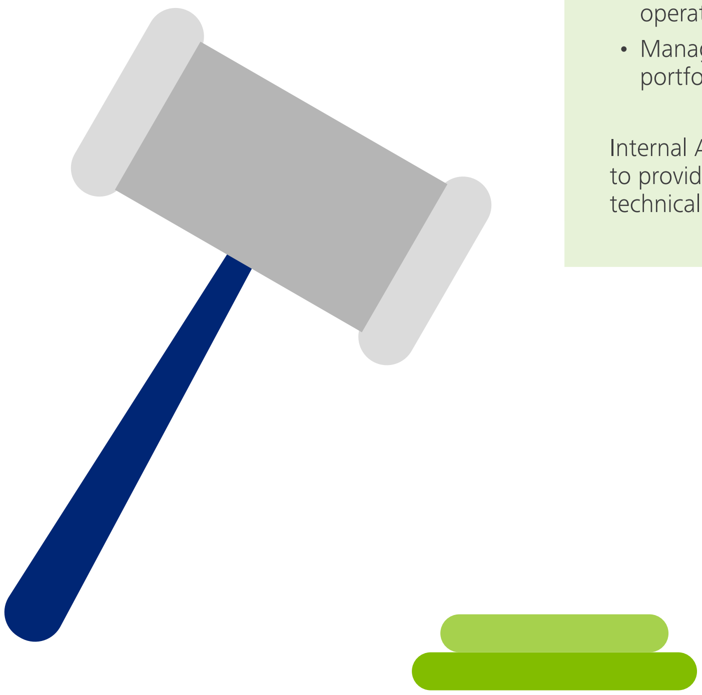
- Internal Ratings Based Approach for Credit Risk;
- Internal Model Method to calculate exposure on derivatives (Counterparty Credit Risk); and
- Value at Risk-based models for Market Risk in the Trading Book.

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 CRD IV seeks to address.

In performing these reviews, Internal Audit should consider:

- Management's self-assessment of compliance with CRD IV and remediation of areas of non-compliance;
- The extent to which tactical solutions implemented to meet the tight timelines associated with CRD IV implementation are being replaced with strategic solutions;
- Data quality and accuracy of internal reporting;
- Stress testing processes 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 and operational risk, for example);
- Management's ability to manage significant "risk change" portfolios.

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



Data quality

Data quality that is fit for purpose for capital and liquidity reporting allows financial organisations to maximise their value from data.

What can Internal Audit do to address this?

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, reviews focussing on the governance practices of data rich processes should be undertaken. 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.

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

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

Cyber crime

An increasingly regular feature in the media over the past 18 months has been cyber crime, 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 industry. High profile incidents, customer concern and media coverage are increasingly compliance as well as business issues, with greater regulatory scrutiny, direction and intervention than previously observed.

For all organisations 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. Recent high profile incidents demonstrate that cyber attacks damage organisational reputation and customer confidence. Boards of Directors and management are slowly coming to the realisation that they are not fully aware of the potential impacts of such breaches.

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.

The rise in breach size, impact and complexity in 2015 has driven a shift in incident response from point-based 'fix-it' type approaches towards those that are more holistic and sustainable. This has necessitated more robust internal controls and incident response being more embedded and integrated into the operational risk framework of a firm as a whole. 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 in this emerging risk area. 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 the coming year. This should enable a more coherent view of emerging risks and threats, and in turn drive more effective risk management practices whilst allowing Internal Audit to remain agile to the changing nature of cyber threats.

What can Internal Audit do to address this?

Internal Audit should:

- As the third line of defense in risk management, internal audit should verify that the steps taken by the first line (business) and second line (risk management) are equal to existing and anticipated cyber risks. If one hasn't already been done, Internal Audit should conduct a cyber risk assessment based on a robust framework that considers security, vigilance and resilience to develop a risk-based audit plan. Internal audit should consider the threat profile (who might attack, why they might attack and what they might go after) when developing the plan. Depending on the organization, high-risk areas might include data protection, vendor management, cyber incident management, and resiliency, among others. This is an iterative, multi-year endeavour calling for a programmatic, prioritized approach. Cyber security audits demand ongoing improvement of internal audit talent and skills and close engagement with IT and security staff, business units, and risk management.
- Encourage organisations to 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; and
- 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

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. 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 broadens its focus to determine the adequacy of processes in place to avoid, respond to 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 to 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. Impacts of a crisis—natural or manmade, physical or virtual, and local or remote—may compromise operations, employees, supply chains, plant and equipment, and IT and data. Audit plans should ensure that management has developed integrated plans based on sound assessment of all impacts. Each audit cycle can then focus on two or three areas and assess the depth, responsiveness, and integration of plans.

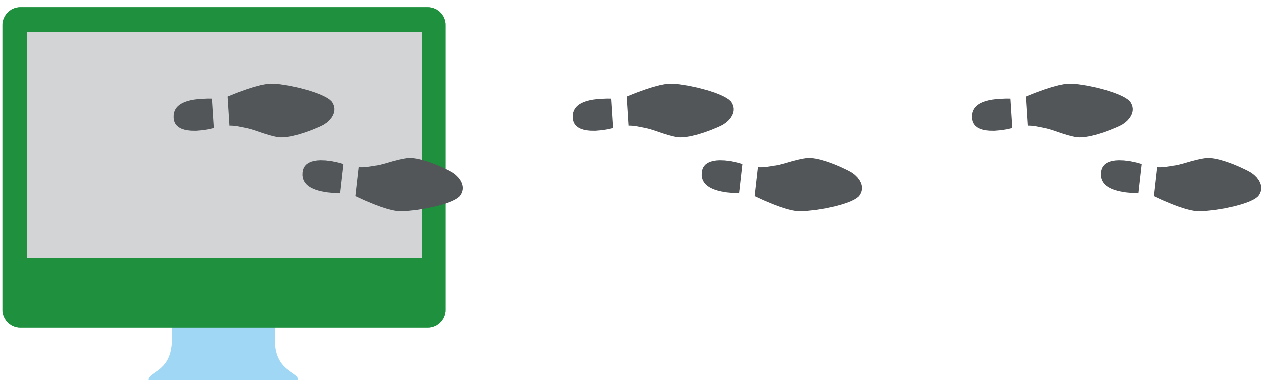
Digital

Digital capabilities 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 organisations' existing governance, oversight and internal controls frameworks. 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 risks, Internal Audit should:

- Include digital as part of Internal Audit's annual audit plan in order to provide genuine input, oversight and challenge to the digital-led 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; and
- 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 Internal Audit risk assessment processes if not managed effectively. The continually changing data landscape can make it difficult for Internal Audit to prepare a plan that will be relevant over the course of a year. 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?

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.

Contacts

For more details please contact a member of our team:

Colm McDonnell
Partner, Risk Advisory
01 417 2348
cmcdonnell@deloitte.ie

David Kinsella
Partner, Risk Advisory
01 417 2529
davkinsella@deloitte.ie

Sean Smith
Partner, Risk Advisory
01 417 2306
seansmith1@deloitte.ie

Eileen Healy
Partner, Risk Advisory
21 490 7074
ehealy@deloitte.ie

Jacky Fox
Director, Cyber
01 417 2208
jacfox@deloitte.ie

Sinead Carey
Senior Manager, Risk Advisory
01 417 5700
sicarey@deloitte.ie

Anlo Taylor
Senior Manager, Risk Advisory
01 417 2826
anltaylor@deloitte.ie

Dublin
Deloitte
Deloitte & Touche House
Earlsfort Terrace
Dublin 2
T: +353 1 417 2200
F: +353 1 417 2300

Cork
Deloitte
No.6 Lapp's Quay
Cork
T: +353 21 490 7000
F: +353 21 490 7001

Limerick
Deloitte
Deloitte & Touche House
Charlotte Quay
Limerick
T: +353 61 435500
F: +353 61 418310

Galway
Deloitte
Galway Financial Services Centre
Moneenageisha Road
Galway
T: +353 91 706000
F: +353 91 706099

deloitte.com/ie/