Deloitte.

Exponential change
2016 priorities for Internal Audit in financial services

#DeloitteRA

Introduction

Internal Audit plans for 2016 should be developed keeping in mind the exponential changes that will impact the financial services industry.

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 and adoption of new regulations. It will be another year of change and Internal Audit 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 has 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.

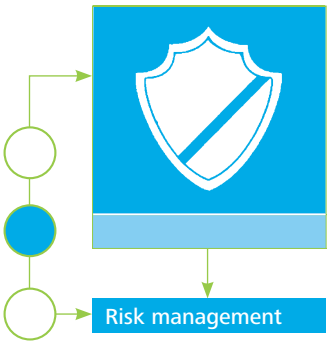
Indeed the challenge is multi-faceted. All of the 2015 planning priorities remain relevant, however, there is a greater spotlight on the way organisations behave with recognition that this is only as good as the weakest link. Expectations from regulators and customers are more demanding than before. Threats such as cyber and financial crime 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 will be 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 your next audit cycle.

Key areas explored in this publication

Risk management



Board Notice 158

The Financial Services Board released Board Notice 158 (BN158) of 2014, applicable to all insurance licensed entities, which effectively makes the Internal Audit function a requirement under Solvency Assessment and Management (SAM). The Internal Audit function has been a statutory requirement under the Banks Act and Regulations, for all banking licensed entities, for a number of years. The Banks Act and Regulations prescribes the role and responsibilities of the independent Internal Audit function as it pertains to risk management and internal controls. BN158 gives effect to the interim measures (risk management, governance and internal controls) under the new SAM framework to be implemented on 1 January 2017. It is the requirements under BN158 where most of the challenges will arise for Internal Audit because of the requirement to:

- Establish, implement and maintain a risk-based audit plan.
- Evaluate the effectiveness of the governance framework.
- Evaluate the adequacy and effectiveness of the insurer's risk management, compliance and actuarial functions.

These requirements will necessitate Internal Audit to focus on areas which are not typically reviewed by Internal Audit and which may require upskilling and training.

Internal Audit may also have responsibilities towards reviewing the Own Risk and Solvency Assessment (ORSA), including:

- The calculating of economic capital should be subject to independent review. The independent review can either be internal, where Internal Audit has the appropriate independent skills and expertise in-house, or external (to help execute Internal Audit's responsibilities). Elements of the model (such as completeness and accuracy of data, appropriateness of assumptions etc.) should be included within these regular reviews. Where modelling and analysis techniques remain consistent from one year to the next, these elements need to be reviewed less frequently.
- The ORSA document should be subject to an independent assessment either internally, by Internal Audit or externally (to help execute Internal Audit's responsibilities).
- Internal Audit is expected to provide challenge, benchmarking and independent review around the process governance structures and the ORSA report.
- Internal Audit should also provide quality assurance around the process governance structures around the ORSA.

Again, these technical requirements may necessitate upskilling and investment on behalf of Internal Audit to be able to perform these reviews in house, or may require outside skills to be sought.

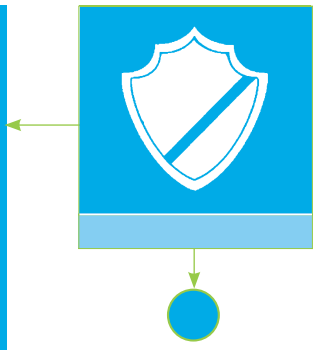
Risk appetite framework

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 Internal Audit to conduct an audit of the risk appetite framework. Internal Audit have based these audits on the Principles for an Effective Risk Appetite Framework, published by the Financial Services Board in November 2013. However, these organisations have found that the principles require a degree of interpretation and therefore many Internal Audit teams 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 2015 Mock ORSAs, produced by insurers, as well as the Internal Capital Adequacy Assessment Process (ICAAP) conducted by banks. 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.
- 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?



Directors' 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. 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, issue management, loss data capture, etc.). Many organisations now face the challenge of integrating these elements into one coherent and dynamic framework. Without an integrated Enterprise Risk Management (ERM) 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. In addition, the ERM framework should be audited for alignement against business goals.

What can Internal Audit do to address this?

- Review the ERM framework and provide assurance on contained risk management processes.
- Evaluate the reporting, management and treatment 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.

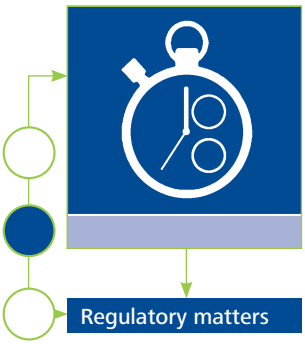
Of particular concern is the materiality and magnitude of model error and its wider impact on the financial services industry. As a result, Internal Audit should have a strong focus on specialist regulation and technical concepts, particularly where models are used for regulatory purposes (e.g. capital 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.

Model risk is largely the potential for inaccuracy and/or inappropriate use of models, which can lead to substantial financial losses and reputational damage.

What can Internal Audit do to address this?

- 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 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.

Regulatory matters



Retail conduct and RDR

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

Firms need to ensure that customers remain central to their business strategies, and that growth and profitability do not deliver poor customer outcomes resulting in regulatory sanction and the need for customer remediation.

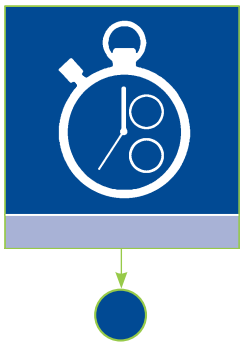
For firms designing and distributing products, product governance is a key area of focus and should be high on the Internal Audit agenda in 2015. Products should have a clearly defined target market and organisations must demonstrate that appropriate target customers buy the product. The fairness of contract terms, pricing and product information (including financial promotions) are all key areas that should form integral parts of product design and review processes. The focus of firms and, by extension, Internal Audit functions should not be confined to current products; legacy product governance is also an important area.

With the focus of regulation firmly on the conduct of firms selling bundled insurance products alongside credit and banking products, Internal Audit will be expected to provide proactive guidance on risk exposure and methods to address issues identified.

With the onset of the Retail Distribution Review (RDR), firms will be embarking on many changes to the way that products are designed and sold and how firms interact with intermediaries. The many detailed proposals under the RDR will form part of business practices over time and Internal Audit will be expected to include these within the scope of their Internal Audits. Assurance over RDR programmes, from both a scope and delivery perspective, will also be key for Internal Audit to assist Audit Committee's in understanding their risk exposure. The focus that the RDR places on eliminating conflicts of interest within the financial services value chain will be key for firms going forward. Many distribution models and channels have inherent conflicts of interest imbedded in them and although these may not be identified within the RDR, firms could benefit from identifying these proactively and taking steps to eliminate these risks proactively. Internal Audit can play an active role in the identification of such conflicts of interest.

Insurance products sold alongside credit products

Recent developments around the selling of credit life products within the South African market has placed heightened awareness of potential customer risks and reputational risks faced by companies should these products be miss-sold. Internal Audit can play an active role in providing independent assurance over the programs put in place to determine the residual risk faced by entities in relation to these products and how they are sold.



What can Internal Audit do to address this?
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 Financial Services Board 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 be focusing specific efforts on reviewing an organisation's responses to both the RDR and the sale of credit life products. This can be achieved by ensuring that staff are adequately equipped to understand the current specific risk profiles associated with both these areas so that they can be embedded within Internal Audit approaches and testing strategies. The effect that emerging regulation has on organisation strategy requires Internal Audit to remain vigilant and up to date with these themes and their impact, both from a risk and strategy perspective.

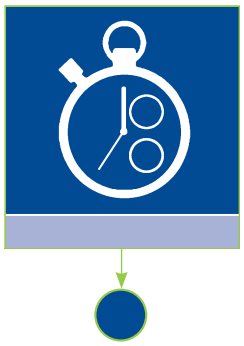
Financial crime

Financial crime (comprising money laundering, the financing of terrorism and sanctions) remains a key concern for governments and regulators globally and has been further brought into the limelight by the recent geo-political tensions and terror threats. In South Africa, the South African Reserve Bank (SARB) has enhanced its supervision in this area over the past 3 years and has issued a multitude of fines to the banking sector. This has partly been in response to pressure from international organisations such as the Financial Action Task Force (FATF), of which South Africa is a member.

The long term and continuing global trend of financial institutions being penalised is evidence that organisations are still struggling with the basic requirement to establish appropriate systems and controls to identify and manage financial crime risk. South African organisations are no exception to this. 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.

Financial sanctions continue to be a high priority for governments and financial organisations so these 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 which 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 is 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.



Privacy not POPI

The Protection of Personal Information Act, No 4 of 2013 (POPI) promotes the protection of personal information by public and private bodies in South Africa.

POPI has been signed into law by the President on 19 November, but the effective date was not set at the time. Parliament held a meeting on 11 November 2015, on the role of the Information Regulator. The outcome of that meeting was that Parliament has asked for another workshop to be set up in 2016. The anticipated POPI commencement date will be in the second half of 2016. So if in the best case scenario the regulator gets appointed towards the end of 2016 and companies have another year to comply ... why should any changes be made in 2016?

In financial services, the driver for privacy compliance may very well be global privacy compliance and competitive edge in respect of customer experience, rather than POPI.

On Tuesday, 15 December 2015, the European institutions agreed on a final text for the new General Data Protection Regulation (GDPR). The GDPR will replace the former EU Data Protection Directive and create a unified data protection law that will apply directly across all 28 EU Member States from 2018.

With the new Regulation, the EU intends to strengthen citizens' control over the use of their personal data, while simplifying the regulatory landscape for business.

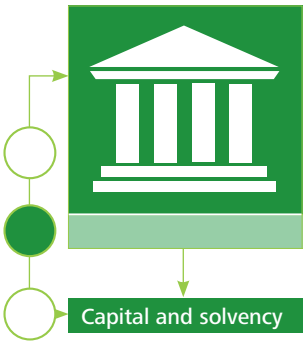
Aside from reaffirming core privacy principles such as consent, purpose limitation, data minimisation, accuracy, storage limitation and integrity and confidentiality; the GDPR shifts the regulators' focus towards accountability.

Privacy and information security policies and procedures, personal data processing records (such as inventories or data flow mapping), documented training and awareness programmes, data protection impact assessments and compliance/audit plans will be considered key elements in order to demonstrate compliance.

What can Internal Audit do to address this?

Privacy compliance across the various jurisdictions in which the business operates would need to become part of the audit risk universe. In this first year 2016, Internal Audit should play a pro-active role to evaluate the adequacy of control in respect of privacy policies, processes to manage the consent collected from data subjects, information security pertaining to privacy, cross-border transfer of personal information, as well as retention and destruction schedules. By 2017/18, the audit plan should include effectiveness testing of controls across all privacy related controls, moving on towards an integrated approach of privacy testing as part of normal business process control testing.

Capital and solvency



Regulatory capital and solvency requirements

Starting on 1 January 2017, Solvency Assessment and Management, which is known more commonly as SAM, sets out a step change in capital management, risk and governance frameworks and regulatory reporting for all South African insurers in its scope. SAM'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 SAM, 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 SAM results for organisations, including quarterly reporting to the Prudential Authority and the Financial Conduct Supervisory Authority along with a new narrative reporting requirement for these reports.

The first draft of the proposed amendments to the Banking Act regulations was released for public comment in September 2015. The proposed changes include amendments to the following aspects of the regulations, in order to align with the Basel III changes proposed in the EU and changes proposed by other global standard setting bodies:

- Liquidity coverage ratio and liquidity risk monitoring tools.
- Monitoring tools for intra-day liquidity management.
- Basel III leverage ratio framework and disclosure requirements.
- Liquidity coverage ratio disclosure standards.
- Liquidity coverage ratio and restricted use committed liquidity facilities.

What can Internal Audit do to address this?

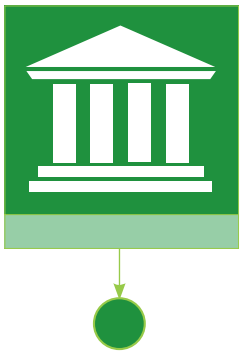
For SAM, Internal Audit should consider:

- Engagement with business on the review or validation of capital models and reporting infrastructure for SAM.
- Liaising with governance committees on key responsibilities for SAM.
- 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 SAM.
- Considering whether Internal Audit possesses the necessary expertise to review the programmes and models.
- Oversee projects supporting the implementation of SAM.

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 SAM.

For Basel III, Internal Audit should stay close to management in order to understand how bank management is preparing for the proposed amendments, and upskill themselves in order to be able to provide assurance over these new complex areas of the regulation, once the new regulation is implemented.



Data quality

Data quality that is fit for purpose for capital and solvency 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.

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.

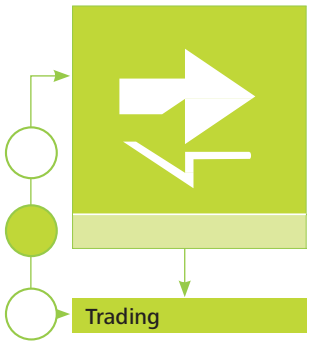
Internal Audit should play a pivotal role in enhancing the control environment and reducing the risk of poor data quality by conducting reviews of data quality processes.

What can Internal Audit do to address this?

Internal Audit should develop data governance skills and knowledge to review the appropriateness of governance, while also having 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. 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.

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.

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 are now well established, albeit evolving. 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 reviews of supervisory framework audit of front office functions.

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.

High frequency and automated trading

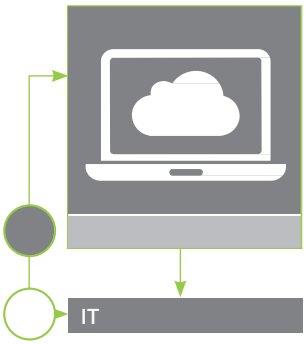
The increasing use of high frequency and automated trading practices at many organisations increases their susceptibility to losses due to programming or other IT issues. This risk is heightened where markets experience high levels of price volatility.

What can Internal Audit do to address this?

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



For many Internal Audit departments, a cyber-security incident is not so much a question of 'if', but rather 'when'.

For many Internal Audit departments, a cyber-security incident is not so much a question of 'if', but rather 'when'. The result of cyber-attacks and related breaches can result in a range of business impacts and costs, from technology and resources required in remediation to post-breach legal and regulatory implications. Moreover, in worst case scenarios the lack of proper cyber resiliency measures, have the potential to render business inoperable and even lead to failure of all business operations.

More than ever, the ability to effectively detect and rapidly respond to an attack is both essential and no longer an optional investment. More mature organisations are proactively planning and preparing for cyber related 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.

More mature organisations are proactively planning and preparing for cyber related incidents.

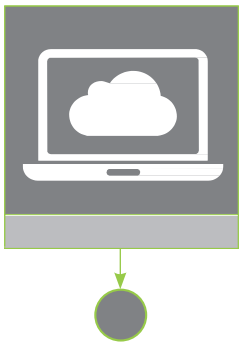
Cyber crime

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

More than ever, the ability to effectively detect and rapidly respond to an attack is both essential and no longer an optional investment.

This is not simply about fixing the vulnerability that was exploited, but wider crisis management skills, including public, media and customer relations. In view of this, cyber resilience should be on the agenda of all Boards of Directors, including the accountability for addressing holistic IT governance and management solutions with a strong focus on cyber resiliency.

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 in terms of lost revenue, orderly market operations and loss of market confidence.



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 related risk at Board level. It is an opportunity for Internal Audit to demonstrate that they can understand and provide assurance across all IT governance and IT management domains, as the third-line of enterprise defense.

In addition, Internal Audit should promote increased organisational collaboration in IT governance audits, both internally (between functions) and externally, as this will be a key area of focus for the sector during coming months. This should enable a more transparent view of emerging risks and threats, and in turn drive more effective risk management practices while allowing Internal Audit to remain agile to the changing nature of cyber threats.

What can Internal Audit do to address this?
Internal Audit should:

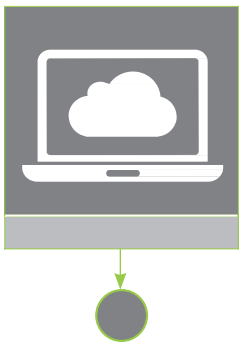
- Engage strong IT governance and IT management audit practices, which will not only support cyber resilience audits but also provide overall assurance around the benefits achieved from IT-Enabled Investments.
- Adopt good practice business and audit frameworks, such as COBIT®5, in support of tackling cyber resiliency issues. This empowers Internal Audit to adapt to the changing needs of their organisations, increase its awareness of the IT governance, IT management (including cyber security threats faced) and the changing demands of regulators resulting in concerted efforts to truly comprehend the wide reaching impacts of cyber threats.
- 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 allow 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, including the Bank of England, after a payments system crash. Increasingly we are seeing Regulators taking a tougher stance where instances impact the general public. 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.

Additionally, learning the lessons from others to 'Stress Test' in-house plans against scenarios impacting other organisations should be adopted e.g. Royal Bank of Scotland/Ulster Bank payments issues. These risks arise across technology, people and processes. With this in mind, it is imperative that Internal Audit broadens their focus in the coming year 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 forces

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 control 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, Internal Audit should:

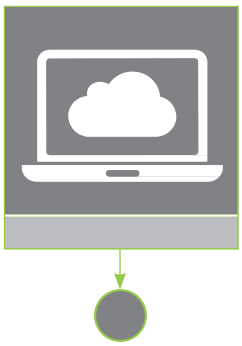
- Include digital forces as part of Internal Audit's annual audit plan in order to provide genuine input, oversight and challenge to the digital parts of the business.
- Have the appropriate expertise and experience to independently verify the effectiveness of all elements of the organisation's digital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

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.

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 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.
- 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.

Recent developments from both a regulatory and technology perspective are causing a significant shift in traditional payment models, resulting in major changes in the market.

Payments

Recent developments from both a regulatory and technology perspective are causing a significant shift in traditional payment models, resulting in major changes in the market. This is providing a difficult set of challenges across the financial services sector as banks face disruption from FinTech providers who are heavily investing in payments. Cash is becoming increasingly replaced by contactless and mobile transactions as MPesa, Zapper, Hello Paisa, Instant Money and other offerings start to take a significant foothold in the market. High-profile payment outages are still all too common as institutions grapple with these future challenges while trying to ensure the 24/7 availability of existing payment services, often supported by legacy applications and infrastructure.

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

Contacts

Navin Sing
Managing Director: Risk Advisory Africa
Mobile: +27 (0) 82 83 304 4225
Email: navising@deloitte.co.za

Akiva Ehrlich
Risk Advisory Africa: Financial Services Industry Leader
Mobile: +27 (0) 82 443 2020
Email: akehrlich@deloitte.co.za

Dean Chivers
Risk Advisory Africa Leader: Governance, Regulatory & Risk
Mobile: +27 (0) 82 415 8253
Email: dechivers@deloitte.co.za

Nina le Riche
Director: Risk Advisory Africa
Mobile: +27 (0) 82 331 4840
Email: nleriche@deloitte.co.za

Mark Victor
Director: Risk Advisory Africa
Mobile: +27 (0) 82 772 3003
Email: mvictor@deloitte.co.za

James Alt
Associate Director: Risk Advisory Africa
Mobile: +27 (0) 72 163 9356
Email: jamalt@deloitte.co.za

Paul Day
Lead Partner, FS Internal Audit
Mobile: +44 (0) 779 965 8055
Email: pauday@deloitte.co.uk

Designed and produced by Creative Services at Deloitte, Johannesburg. (811061/jo)