Deloitte.

Building on New Approaches

2019 Planning Priorities for Internal Audit in Financial Services

Contents

Introductory Letter

Welcome to Deloitte's *2019 Planning Priorities for Internal Audit in Financial Services*, now in its 5th year, which highlights a selection of the more interesting developments and challenges being addressed by audit functions in our industry.

Reflecting on the financial services (FS) landscape in 2018 it is, in many ways, little changed from this time last year. Interest rates remain low, corporate strategies remain focused on cost reduction, whilst the uncertainty of Brexit continues to dominate the political agenda.

Despite this, it is clear from the breadth of topics covered in this publication that the role of internal audit (IA) in FS continues to evolve. Recognising the increasingly complex assurance that IA is being challenged to provide, and a continued focus on functional transformation first articulated in our 2018 publication, the theme of this year's publication is ***'building on new approaches'***.

For the first time we have included a dedicated section focusing on some of the new tools and techniques available to IA to deliver against their evolving mandate. Agile auditing, the use of automation and the talent needs of the IA teams of tomorrow are all featured. Whilst readers may be familiar with some of these terms, the inclusion of topics such as risk sensing and behavioural analytics represent the cutting edge of internal auditing and demonstrate how technology is changing the way our professions works. We develop such topics further in a separate publication, *Internal Audit 3.0*, released earlier this year.

There are also a number of new focus areas to consider for inclusion in annual audit plans. We anticipate an increased emphasis on digital risks (including artificial intelligence and 'cloud' computing), a renewed focus on prudential risks (including model error risk) and an acknowledgement that sustained M&A activity is increasingly requiring IA functions to confront the challenge of auditing high-risk Fin and Reg Tech acquisitions.

Our 'Topics by Theme' section provides further detail on each of these interesting topics including, where relevant, additional sector-specific insights. For each of the topics you will find a brief commentary providing some background, along with notes on how the topic can be audited and some of the potential challenges that you may face.

As always, we hope this edition contributes to your annual planning process, providing useful insights and generating meaningful debate with key stakeholders and with your teams. Should you wish to discuss any aspect in further detail, please do not hesitate to contact one of our team.

Russell Davis
Partner
Financial Services Internal Audit Lead

Market Overview

Financial Services Ecosystem

- MiFID II and IDD will overhaul the FS trading landscape.
- New connections will be created through technological innovation and reliance on third party service providers.

Technology Opportunities

- New solutions will allow the introduction of new products, services and ways of working.
- Innovation will allow businesses to do things better, and more efficiently.

Customer Relationships

- Firms are looking to use customer data in novel ways, customers are gaining stronger rights over how this data is used.
- New technologies are enabling new ways of interacting with customers.

High inflation

- In the UK persistently high inflation led to an unexpectedly sharp slowdown in Q1 18.
- US activity continued to strengthen and inflationary pressures rose following further fiscal stimulus.

Protectionism

- Markets were unnerved by rising global trade tensions after the US imposed tariffs on steel and aluminum imports sparking retaliatory measures.
- The price of oil climbed above $80 a barrel for the first time in almost four years fueled by geopolitical tensions in the Middle East and continued OPEC production quotas.

Brexit

- Uncertainty around the timing and nature of the Brexit settlement has added worries about the final destination of the process.
- 75% of CFOs expect Brexit to lead to a deterioration in the long-term business environment.

Weak UK demand

- Only 17% of CFOs anticipate an increase in revenues over the next 12 months.
- Focus on cost control and building up cash.

Recruitment Challenges

- 43-year low unemployment rate and inflows into the UK labour force from overseas slowing.
- 44% of CFOs reported recruitment difficulties or skills shortages in the 2nd quarter of 2018.
- A sustained rise in wages, following a period of muted wage inflation, will add to the challenges the FS sector are facing as they seek to rein in/ reduce costs.

Rate Rises

- The Federal Reserve raised interest rates by 25bps and set out a course for two further increases.
- The Bank of England raised the interest rate for only the second time in a decade.
- Events in Italy sparked unease in financial markets and led to a sharp surge in government bond yields.

Section 1: Planning Priorities for Internal Audit Topics by Theme

Digital Risk

Strategy & Change

Payments

Conduct

Section 1: Planning Priorities for Internal Audit

New Regulation

Prudential Risk

Governance

Taxation

Section 2: New Methodologies for Internal Audit Topics by Theme

Audit 3.0

Enablers

Innovation

Methodology

Key – Industry Icons

Banking and Capital Markets

Insurance

Investment Management and Private Equity

Section 1:
Planning Priorities for Internal Audit

Artificial Intelligence and Robotic Process Automation

Evolving process efficiency

Why is it important?

Artificial Intelligence (AI) makes use of machine learning, visual recognition and natural language processing techniques, with advanced algorithms offering the ability to analyse data in an "intelligent" way. This can in turn drive operational and cost efficiencies as well as strategic transformation programmes, resulting in better and more tailored customer engagement.

Robotic Process Automation (RPA) is an evolving form of business processing that relies on automated technologies such as software robots to perform repeatable processes in an efficient and cost effective manner.

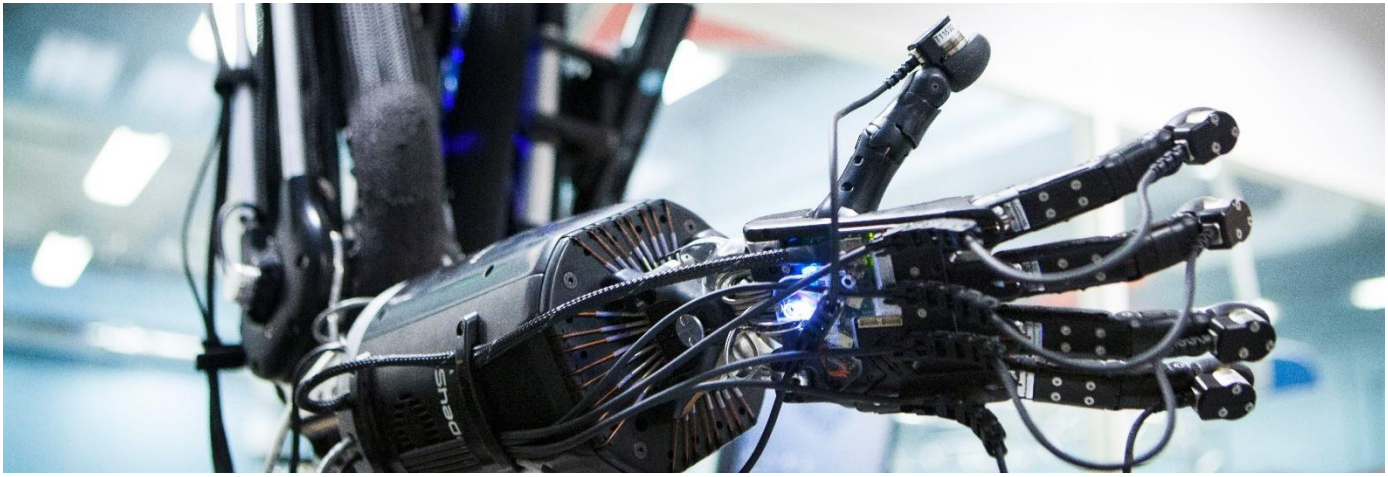
In the FS sector, the use of AI and RPA is increasing, therefore the need for a robust and reliable control environment, and the ability to effectively report on the status of that environment is ever more critical.

EU and international regulators have taken an active interest, and while they recognise the benefits AI and automation can bring to markets, firms and their consumers; they are increasingly mindful of the risks for regulated firms.

What should you be doing?

There are a range of potential activities that IA can perform, some of which are captured below:

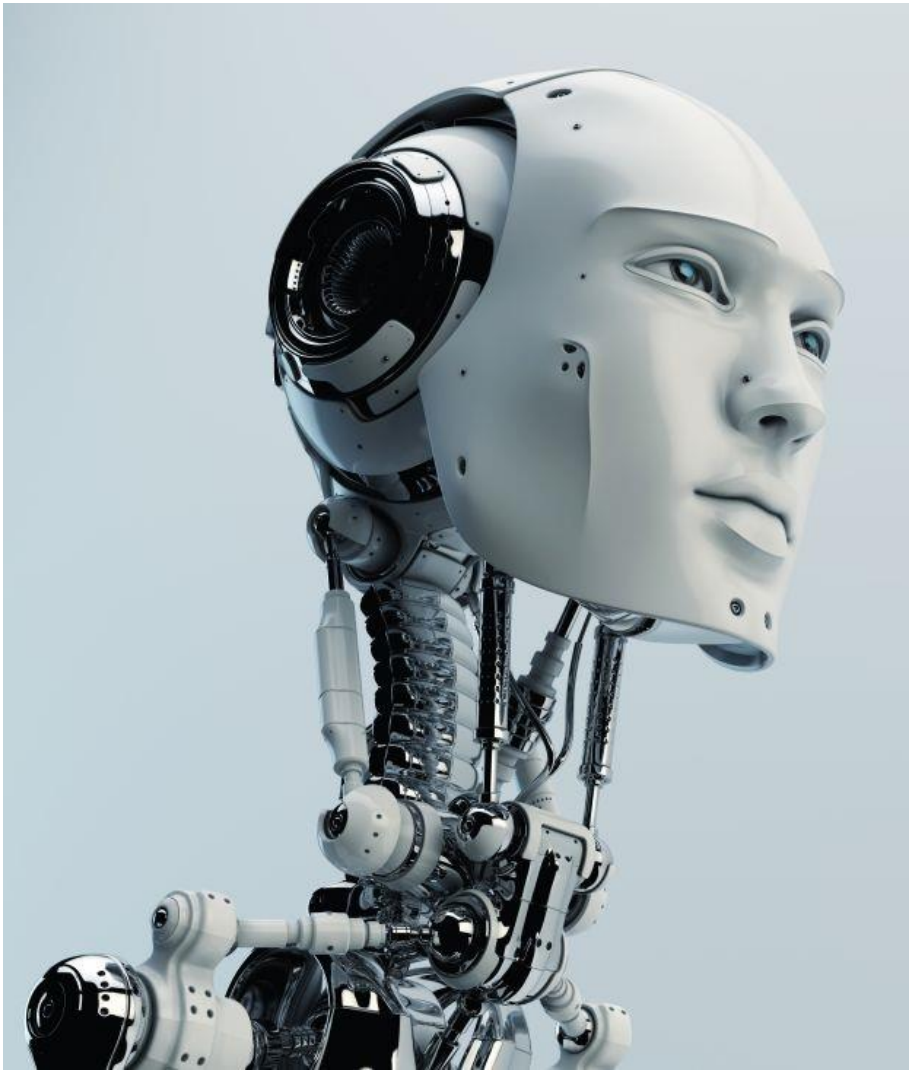
- IA can map AI and automation assets against their audit universe, paying particular attention to over-reliance on third party providers. Challenging management on continuity arrangements in these cases will be key.
- IA should consider establishing a framework and methodology for auditing technologies; this should be based on a multi-disciplinary approach to risk, and not rely purely on technology risk domains. AI is less about completely new risks, more about existing risks that may be harder to identify, given the complexity and speed of solutions.
- IA should stay close to global regulatory developments as these may influence the approach to adopt. In anticipation of clear supervisory guidance, IA can leverage the principles of existing supervisory statements relating to the use of algorithmic trading, supervision of models, operational, cyber and technology resilience, the Senior Managers and Certification Regime and general requirements on IT controls.



Potential Challenges?

There are a number of challenges to auditing AI & automation solutions, some of which are set out below:

- ***Auditability*** – AI solutions are developed to 'learn' and evolve their capabilities over time, making it inherently challenging to completely decode their decision processing layers, which in turn makes auditability and traceability of the decision-making rationale challenging.
- ***Skillset*** – It is recognised that the industry suffers from a lack of in-house skills to appropriately supervise or audit solutions that are being adopted. Lack of cultural integration of such resources may also pose a challenge for IA functions seeking to upskill their teams and complement their resource base.
- ***Full participation*** – A shift to using a "sandbox" environment across the organisation, and involving IA, as well as other risk and control functions may be required. Full participation will allow IA to help shape an appropriate and pragmatic governance, risk and audit approach.



Please also refer to Section 2 – Innovation, where we discuss the ways that IA can use similar technologies to support delivery.

Cyber

Shielding digital assets

Why is it important?

Cyber risk remains a key priority for all stakeholders in FS, emphasised by the fact that the new Chairman of the US Federal Reserve identified cyber threat as 'maybe the single most important' risk to FS today.

Our recent report on Cyber Risk identified that in 2019 we expect FS regulators in European jurisdictions to pursue a combination of the following:

- Develop and communicate clearer standards and cyber resilience expectations;
- Formalise incident identification and breach reporting procedures;
- Place increased pressure on banks' Boards to demonstrate ability to provide effective challenge, through access to independent expertise; and
- Focus on risk and control frameworks and quantification of cyber risk.

What should you be doing?

As cyber risk has remained a key focus area for several years, the majority of functions have put in place plans or actions to address the fundamentals of prevention and detection.

IA should consider a shift in focus from assessing the adequacy of cyber defences to "recoverability" and the ability of an organisation to adequately respond and recover from an attack. This should include:

- Assessing whether the organisation has an understanding of the digital assets that are fundamental to survival and whether measures are in place to ensure these are available to enable recovery;
- Challenging management on their ability to understand and map exposure to cyber risks through risk management frameworks and their efficiency in detecting and reporting data breaches rapidly; and
- Utilising new technologies, such as AI, which amplify the awareness of threats to the cyber resilience of the organization.

Potential Challenges?

IA should consider the following challenges:

- ***Flexibility*** – Executives need to anticipate what supervisory developments may mean for their organisation and make decisions based on these, as well as their own threat analysis and cyber programmes. Equally, IA functions need to stay close to these developments and have a clear plan on what to do next.
- ***Timeliness*** – Many cyber initiatives have the objective of improving cyber maturity over a period of years. This makes determining the appropriate time to perform an audit challenging. IA should focus on their responsibility to provide the Board with timely insight into the appropriateness of the organisation's approach to, and execution of, their cyber strategy.
- ***Resourcing*** – IA may find resourcing cyber audits with staff who have had exposure to cyber specific risks difficult. This could impact IA's ability to provide an appropriate level of assurance.

Data Privacy and GDPR

Ensuring ongoing compliance

Why is it important?

Data protection continues to be a topic of ongoing discussion, challenge and focus by management, Boards, and IA alike.

While GDPR came into force on the 25 May 2018, many organisations had "risk-accepted" long before that date that they would not be fully compliant with the legislation. As such, many have focused on what they deem as their "high risk" areas to establish what they hoped would be a defensible and pragmatic approach for when the new legislation became enforceable.

Now the legislation is fully enforceable, the focus for organisations is primarily two-fold:

- One, to undertake the remedial activities required to ensure they become fully compliant with GDPR; and
- Two, to transition their ongoing projects into BAU activities once firms have reached a position of full compliance.

What should you be doing?

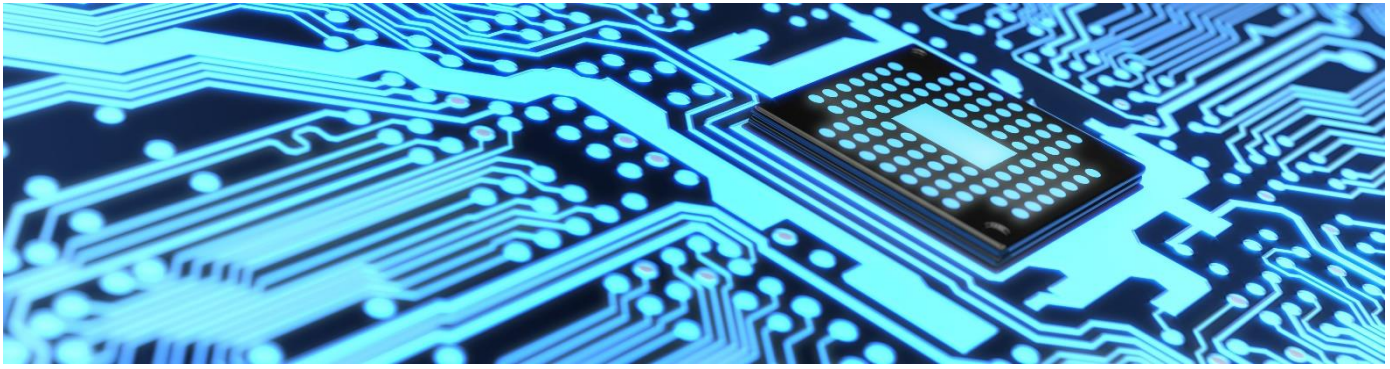
Now that GDPR is fully in force, we suggest that IA consider the following activities:

- Understand the "next steps" in an organisation's GDPR journey; consider the gaps between the current state and full compliance and understand the risks associated with the project to achieve full compliance; and
- Challenge how management aims to ensure ongoing compliance, covering the "people" perspective – what training is in place? How are they managing the expected – and necessary – cultural shifts?
- IA will have a role to play in ongoing monitoring, for example through audits of data processes; IA Heads should be part of the early conversations in establishing this ongoing role.
- IA should be at the forefront of the aforementioned activities, challenging management and structuring an audit plan that focuses appropriately on the above, commensurate to the risks.

Potential Challenges?

Continuous audit activity may be most appropriate in this area as the challenges surrounding GDPR will remain. This could amplify the following risks:

- ***Scoping*** – Many organisations have not yet fully scoped the projects or the resources needed to ensure compliance in a post 25th May world. Many are unsure how large the gaps between current state and full compliance are, challenging IA's ability to scope their work.
- ***BAU phase*** – The transition from project to BAU is often complicated and this is expected in the case for GDPR. While initially some IA teams may have seen May 2018 as the end of their GDPR related activities, in reality, it is only the beginning of an ongoing journey.



Cloud

Backing up data safely, securely and efficiently

Why is it important?

The FS sector has seen rapid growth of cloud services and "cloud first" strategies. As a result, IA's ability to understand the impact of migrating data to, and use of, the cloud as part of the organisation's operational risk profile is critical.

Use of the cloud exposes firms to a number of risks. There is typically less visibility of security and governance controls, differing cloud standards and guidelines to consider, and multiple implementation approaches. All of these can expose a firm to significant brand, reputational or privacy breach risk.

What should you be doing?

IA's focus will vary depending on the level of cloud adoption by the business and the maturity of existing third party management processes. Three possible approaches are:

- For organisations with a limited cloud footprint, IA should challenge management on the appropriateness of their cloud strategy and the capability of existing risk management functions to address cloud specific risks. This will include engaging with business stakeholders to identify and discuss cloud specific risks.
- In more mature cloud environments, IA should perform reviews that assess the effectiveness of controls to protect services delivered from/ assets managed in the cloud and consider reviews that assess the degree to which the stated benefits of cloud migrations have been realised.
- Where firms have a fully embedded cloud solution, IA's work can centre on risk mitigation activities, to ensure associated risks are minimised. This may include evaluation of the cloud provider to ensure stability and data storage and ownership are considered.

Potential Challenges?

IA may face challenges in the following areas:

- ***Resourcing*** – The limited availability of resources with exposure to cloud technologies and an understanding of cloud specific risks will make auditing this area challenging. While guidance from organisations such as the Cloud Security Alliance (CSA) can assist technology auditors in scoping cloud audits, an understanding of cloud business models, the shared responsibility model of controls and the technology that supports cloud environments is required to perform robust reviews of cloud controls.
- ***Cloud migration*** – One of the challenges for IA can be involvement in the initial cloud migration project setup. Lack of visibility of key controls in this crucial design stage may hamper IA's ability to identify control weaknesses until these are being implemented by the business.

Countdown to Brexit

Navigating a fast changing environment

Why is it important?

Many larger firms have spent considerable time and effort to design and implement new European or UK operations that will safeguard their business in a post-Brexit environment. It is important that these plans are now translated into efficient and workable businesses solutions to ensure implementation prior to the 1st March 2019.

Brexit will impact the current operating model of an IA function drastically. This will lead to a number of impacts on IA's scope, which will need to adapt accordingly given the dynamic environment Brexit creates.

Potential Challenges?

Brexit is a constantly evolving topic which has made it challenging for IA functions to effectively plan their work. We have seen IA teams encounter the following challenges throughout 2018:

- ***Talent*** – IA will need to assess if they have the right skillset, calibre of people and appropriate staff in the correct location to properly understand Brexit related risks, and then challenge the business on these risks.
- ***Agility*** – IA will need to ensure that they can work dynamically and adapt their scope and risk assessment to changeable Brexit plan. This may include undertaking audit activity for a standalone legal entity at short notice.
- ***Communication*** – IA will need to check meeting minutes in order to review attendance at Board and other committees to ensure key stakeholders are present, and that there is sufficient demonstration of effective governance.

What should you be doing?

Despite the Brexit deadline rapidly approaching, there are a number of activities that IA functions can perform in the coming months:

- IA can assess the appropriateness of project initiation documentation, which has been lacking in some firms. This indicates that projects are not being thoroughly planned prior to their initiation. Further, it has often been observed that these planning documents have been reverse engineered.
- IA can assess if there is sufficient project management resource to deliver the Brexit programme. We have observed that, in a number of instances, firms found it difficult to recruit individuals with the required skill level in the new market they are moving to.
- Firms need appropriate senior management who retain a big-picture overview and challenge specific work streams. Firms also need to engage with IT specialists to assist with the implementation of the Brexit operational model. IA can evaluate whether these have been used sufficiently.
- IA can assess the appropriateness of the Brexit project management. This includes reviewing whether there is sufficient budget and budget management in place to avoid firms adopting a 'whatever it takes' cost perspective, resulting in limited governance over spending.

IA will need to ensure that they remain close to the business to be aware of, and respond to, changes prompted by Brexit. For Banks subject to Structural Reform (please see the Ring-Fencing slide on page 18), Brexit will add further uncertainty.

For those firms who have set up a new, standalone entity within the EU, IA can assess the clarity of the strategy between the centralised business and the new entity. An alternative approach would be for IA to identify and assess the feasibility of delivering key dependencies required for the entity to be fully operational by the Brexit deadline.

Crisis Management

Actively protecting brand value and reputation

Why is it important?

In a rapidly evolving world, organisations find themselves operating in a landscape of uncertainty with heightened risk and stakeholder scrutiny. These risks can come from geopolitical, economic, financial and societal events through to corporate misdeed and high impact operational or technological failures.

Crises present the biggest and growing threats to corporate value and executive reputation and 2018 has been characterised by a number of such events in the market.

Organisations that fail to effectively deal with the risk of crisis can see their reputation, strategic interests, bottom line, and even their existence, threatened or destroyed.

What should you be doing?

A range of approaches can be taken by IA, outlined below:

- A review of the process and controls set out in the firm's crisis management policy and procedures manual;
- A review of lessons learned stemming from crisis management test scenarios; and
- A review of progress against remedial activity identified through initial gap analysis/ test scenarios.

Alternatively, a framework evaluation tool can be used to audit the current crisis management capabilities across the entire crisis and risk lifecycle. This will allow IA to:

- Identify any vulnerabilities in the lifecycle;
- Benchmark against existing best practice; and
- Make recommendations with regards to focus areas moving forwards.

Potential Challenges?

IA may find challenges in the following areas:

- ***Senior audit sponsor*** – Lack of an obvious C-suite level audit sponsor, which could potentially impact business buy-in.
- ***Organisational bias*** – IA will face challenges in delivering difficult messages when findings are identified in conflict with organisational bias in the area.
- ***Lack of transparency*** – Often areas of weakness (business units, subsidiaries, etc.) do not want to share details of failings in operational discipline. IA will face challenge in auditing these areas.

Disruption: Challengers, Fin & Reg Tech

New ideas, new players, new risks

Why is it important?

Disruption is happening across the FS landscape, with new technologies enabling challenger firms to reduce costs, develop rapidly, and revolutionise the value chain.

Reg Tech businesses in particular are providing simple, cost effective ways to deploy technologies that can simplify and streamline system processes and procedures, dramatically reducing the burden on a firm's control function.

This has prompted significant disruptive activity, with acquisitions, investment in start-ups and outsourcing increasing as firms seek to improve the customer journey.

As firms move towards an increasingly tech-driven, innovative and disruptive future, IA will have to adapt to changing landscapes and new risks.

What should you be doing?

Whilst this is an emerging area, there are a number of activities that IA can consider to begin to address risks in this field:

- Where a business may have recently acquired or invested in a start-up or Fin/ RegTech business, IA may wish to undertake an audit covering a range of key risk areas. One solution is to treat the entity as a branch, as this can often leverage an existing audit approach that is familiar and understood by the team.
- IA can also undertake dedicated work over the third party outsourcer through exercising the contractual right to audit (where this exists). As part of this audit IA should consider whether the primary business understands the complexity of the outsourcer, for example the use of algorithms. IA could also consider what software platforms are used by the outsourcer and whether considerations such as data security and data access have been addressed.

Potential Challenges?

Where IA are faced with auditing this area, there are a number of emerging challenges:

- ***Skillset*** – IA will need to assess if they have the right skillset to address risks driven by disruption. This may include individuals that understand emerging technologies, particularly where firms are acquiring or investing in new players where there is no precedent for the risks that may exist.
- ***Oversight framework*** – IA may struggle to define the scope of its work in respect of newly acquired businesses as there may be no clear framework against which to audit, and in many cases Fin or Reg Tech businesses may not have a fully embedded control culture.
- ***Outsourcing*** – With increased scope to outsource key processes (refer to slide 36), do IA have the ability to evoke the right to audit, and if so, do they fully understand the associated risks, such as the use of potentially complex algorithms?

Ring-Fencing

Protecting businesses and creating a safe environment

Why is it important?

The largest UK banks are required by law to separate their retail banking services from their investment and international banking activities with effect from 1 January 2019.

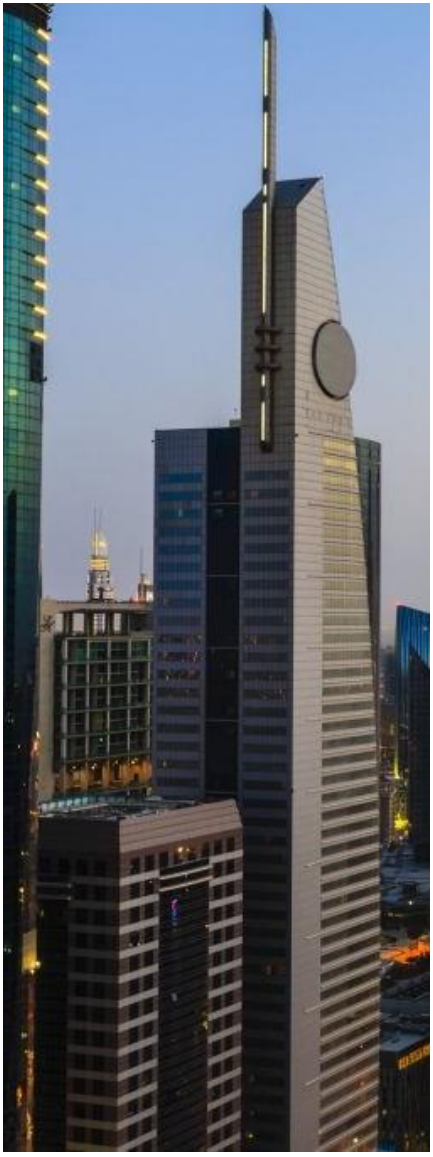
The PRA's Ring-fencing Rulebook and other statutory legislation introduce a number of additional requirements that will require ring-fenced banks to take additional steps to ensure that their governance documentation and processes enable compliance with ring-fencing. The key features of the ring-fencing regime include:

- A ring-fenced bank must ensure that it is able to take decisions independently of other members of its group.
- Where a ring-fenced bank enters a transaction with a non ring-fenced member of its group, this must be done on an arms length basis.
- A ring-fenced bank can only receive services that it requires on a regular basis from an entity in its group which is a ring-fenced affiliate or is an independent, dedicated group service entity.
- There are legal restrictions over services that can be provided by ring-fenced banks and also on the exposures ring-fenced banks are allowed to have with certain types of customer/ counterparty.

What should you be doing?

There are two different types of reviews that can be performed by IA in relation to ring-fencing:

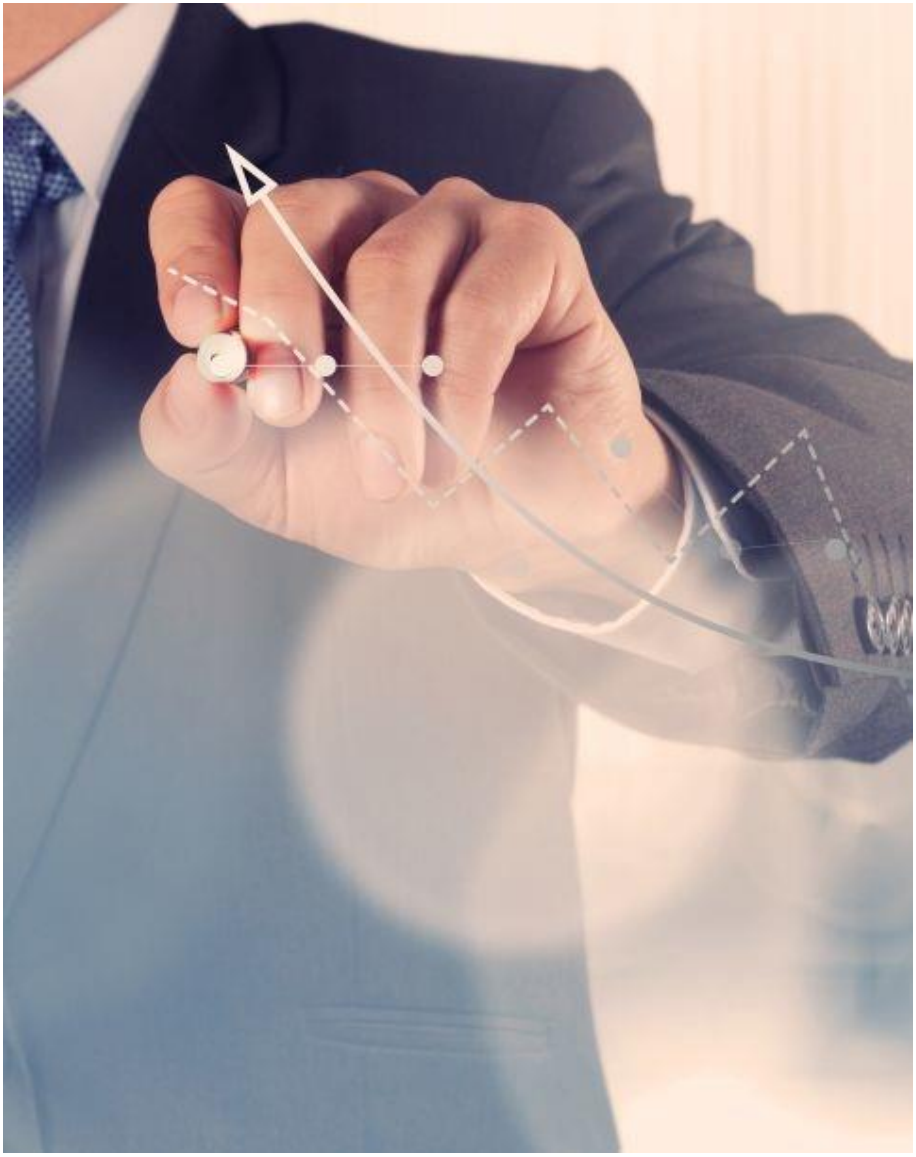
- A ring-fencing implementation readiness review, with a scope focused on the design of new control processes being established to ensure ongoing and sustained compliance with ring-fencing rules.
- A ring-fencing compliance review, focusing on providing assurance of compliance against applicable rules. This should include an assessment of the sufficiency of documentations to support management views.



Potential Challenges?

IA may find challenges in the following areas:

- ***Scope & complexity*** – Ring-fencing introduces a broad set of requirements that are difficult to audit through a single review. IA should consider the best approach to reviewing compliance given the level of detail in the requirements.
- ***Resourcing*** – Ring-fencing will create challenges for IA functions, with potential new entities established as service vehicles and with the need for new senior roles within the function which are independent of the non ring-fenced bank. Audit teams need to be sufficiently resourced and independently managed to cover the various requirements, which will involve access to a number of new senior function holders and review of new systems and controls.
- ***Appropriate evidence*** – Auditing how banks evidence compliance with all the requirements may be challenging. This is likely to broaden the scope of review to look at the firm's wider governance arrangements and the use of the relevant committees.



Financial Crime

Assurance over an evolving financial crime environment

Why is it important?

The embedding of relatively sophisticated conduct risk frameworks, coupled with an evolution in geopolitical sanctions regimes and changing legislation has contributed towards firms reconsidering the sophistication of their financial crime frameworks. This has been driven by some of the following factors:

- New enforcement powers for the Office of Financial Sanctions Implementation (OFSI) and the 4th Money Laundering Directive;
- Increases in regulatory focus such as recent s166 reviews into firms' Financial Crime and ABC controls;
- Ongoing geopolitical changes and the impact of evolving sanctions programmes; and
- Framework sophistication with the focus on developing a more risk-based approach, embedding ownership and accountability and developing MI.

What should you be doing?

Key areas that IA should consider in respect of financial crime are as follows:

- Review of the firm's financial crime framework, with particular focus on the design of the framework and the change controls embedded to identify and address emerging legislation and sanctions.
- Review of sanction reporting/breach reporting tools with a view to providing assurance specifically over the operational effectiveness of associated controls. This approach is focused on assessing the sustainability of existing service software and its ability to address a rapidly changing sanctions landscape.
- Other areas to consider include review of known gaps/ areas of weakness, including validation of actions to remediate the areas.

Potential Challenges?

IA may face challenges in the following areas:

- ***Governance*** – Assessment of how effectively the governance framework supports the ongoing changes required by financial crime legislation or sanction regimes.
- ***Culture*** – Assessment of the framework's ability to embed a culture which prevents and/ or detects financial crime, minimising this risk.
- ***Talent*** – IA may not have the in-house skillset and knowledge to review and assess the compliance with emerging legislation.

SWIFT Customer Security Programme (CSP)

Creating a more secure payment environment

Why is it important?

The CSP is an initiative led by SWIFT to develop core security standards and an assurance framework applicable to all customers. The initiative is intended to identify mandatory controls that all SWIFT users must comply with, as well as additional advisory controls to be implemented at the user's discretion.

SWIFT users were required to submit an initial self-attestation by the end of December 2017, with a second self-attestation demonstrating full compliance being required by the end of 2018. Failure to comply can ultimately result in exposing the organisation to reputational risks, especially in instances where SWIFT publicly report non-compliant firms.

Potential Challenges?

IA may face challenges in the following areas:

- ***Scoping*** – SWIFT CSP requirements may be applicable to various IT solutions, hence it can be challenging to understand the exact processes relevant to the audit.
- ***Multiple SWIFT instances*** – Some larger organisations have multiple SWIFT gateways which may need to be separately considered.
- ***Geographical differences*** – The approach to securing a SWIFT environment can differ depending on the location. Ensuring a uniform and consistent audit on a multiple country basis can be challenging.
- ***Subjectivity*** – SWIFT CSP allows for bespoke solutions to be applied to address the mandatory requirements. It is important to ensure that differing approaches meet the standards required by the CSP.
- ***Advisory controls*** – Some advisory control areas may become mandatory in the future. This should be considered when looking at controls to address the CSP framework and how these may need to be modified in the future to address advisory requirements.

What should you be doing?

IA should perform its work against the backdrop of the mandatory SWIFT CSP requirements, this should both inform and guide the work that IA does. Particular audits can include the following:

- IA can review the initial compliance submission from 2017 to understand their firms approach, the work done and the gaps identified. Depending on the outcome of this, the following compliance review options can be considered:
  - i. End to end assessment of specific areas, including areas of weakness identified in the gap analysis;
  - ii. Specific review activity to provide assurance over the preparation of any future self-attestation submissions; and/ or
  - iii. Review of the control and change management procedures in place to ensure ongoing compliance and continuous oversight.
- Alternatively, IA can focus its work on undertaking a review to validate remedial actions identified as being required in the initial 2017 submission.

Customer Vulnerability

A key area of focus for the FCA

Why is it important?

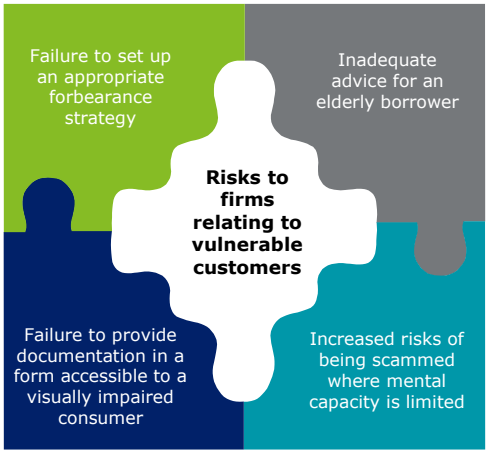
Vulnerability is not set in stone, nor is it a permanent state. It can range from physical disability, mental illness, financial literacy challenges, and also age. Firms must cater to a broad range of customers, designing their processes around this range, and not just the 'perfect' customer.

Risks surrounding customer vulnerability can present themselves in a variety of ways, for example: inadequate or inappropriate advice for an elderly borrower; customers being at an increased risk of being subject to financial crime; failure to provide documentation in a form accessible to a visually impaired consumer; or failure to establish appropriate forbearance strategies; etc.

Potential Challenges?

IA may face a number of challenges when auditing this area, such as:

- ***Subjectivity*** – Vulnerability is a state and not a trait, meaning customers can be vulnerable in some customer journeys and not others, and for various periods of time. Distinguishing who needs additional support can be challenging with different people taking different views. This challenge may be exacerbated if staff in IA teams have not undertaken sufficient training required for customer facing staff.
- ***Sample selection*** – When identifying cases to assess as part of IA work it is not correct to identify just vulnerable customers to test – it is often not possible to do so and it would also mean that customers who have not been identified would not be considered which would not allow IA to assess whether staff are implementing policies and correctly identifying vulnerable customers. Sample selection would need careful consideration in any IA reviews involving outcome testing.



What should you be doing?

There are number of ways IA can audit customer vulnerability. Potential scope areas include:

- Assessing how vulnerability has been factored into new and existing products, including how the products are distributed and managed, and if the pricing practices safeguard vulnerable customers against the risk of unfair price discrimination;
- Reviewing how the firm identifies vulnerable consumers especially in the less risky areas such as branch interactions or correspondence where key triggers may be missed;
- Reviewing the process to review the state of vulnerability of customers at a point in time. IA can also assess if system capabilities allow for proper identification and record keeping to ensure appropriate management in this area;
- Reviewing how consistency around vulnerability is monitored. IA can also review how the firm manages risks to vulnerable consumers when considering new technology and innovation and whether the plans in place to safeguard vulnerable customers in the face of fast paced change are appropriate; and
- Reviewing whether the firm is adequately evidencing the above.

Pricing

Pricing practices that support fair customer outcomes

Why is it important?

The FCA is currently undertaking a thematic review of pricing practices in the General Insurance market. This review represents the culmination of its focus in three linked areas across the past couple of years; value in the distribution chain, the use of Big Data by insurance companies and its impact on customers, and the market's treatment of vulnerable customers.

With the FCA conducting this review, and a clear view that customers should not be charged different prices for products where there is no clear cost difference to the firm, IA is increasingly being tasked with reviewing the firm's pricing practices to provide assurance to the Board in this area.

Potential Challenges?

There are several key challenges to IA in this area:

- ***Distribution channels*** – Distribution models are rapidly evolving in the general insurance market and IA can therefore face a challenge in identifying, and testing, the complete suite of products. Considerations include distinguishing between direct (web-based, face-to-face, call centre) and broker sales.
- ***Oversight of algorithms*** – The use of complex algorithms to price products is increasingly common. Understanding this complexity, and having the right skillset to both test and, where required, challenge management is a common issue in this area.

What should you be doing?

Given the regulatory scrutiny in this area, there are a number of potential reviews that IA can perform. These include:

- Review of Pricing Governance and Strategy – IA can consider whether the board and senior management understand the firm's potential exposure to existing pricing practices and whether there is a clear, defined, and sustainable pricing philosophy in place. This audit would also include consideration of the sufficiency of the oversight of pricing practices across the value chain.
- Control Framework Review – An audit to ensure there are appropriate, fully-embedded controls covering pricing risk. Focus areas include testing the operational effectiveness of these controls, and the extent to which actions arising from legacy/ look-back reviews have been incorporated into the pricing model. In light of new IDD requirements, this audit would also consider training and, where necessary, the upskilling of 1st LoD staff.

Provision of Credit

Ensuring affordable and sustainable lending decisions

Why is it important?

Whilst the FCA have specific requirements around affordability and creditworthiness, it is largely up to firms to determine when to advance or amend a customer's access to credit. The onus is therefore on the lenders to ensure customers are able to repay credit balance both now, and in the future. Assessing the risk to the customer in these two ways brings an added ambiguity to the process.

With interest rates expected to increase further, today's lending decisions must be sufficiently robust to protect both the customer and lender and manage future arrears levels.

What should you be doing?

Organisations should plan to include reviews of their lending policies and processes on a cyclical basis. Accounting for impairment (IFRS 9 – refer to slide 31 for further detail) has changed and this may drive different lending practices.

Conduct specialists should be used given the subjective nature of the topic. Their focus should be in ensuring good industry practice and the provision of an independent view on internal policies and practices.

The scope of audit activities should consider the initial lending decision and any decision to adjust credit through the product lifecycle. Additionally, vulnerable customer identification/ treatment should be considered across the audit. Other specific areas to include in an audit are:

- Policies and procedures – Do these encourage responsible lending, such as the provision of interest only credit where appropriate? IA should include consideration of the use of credit reference agency (CRA) data and affordability calculations, which include any future known increase in interest rates.
- Governance and controls – IA should consider a review of the design of governance and controls, mandates and escalated decision making and monitoring across the first and second lines of defence (in areas such as sample size, risk cohorts and focus of such reviews).
- Implementation – IA should look at customer files with a focus on testing of key risk areas, customer segments and product types. IA should also look at cases tested by other lines of defence to provide assurance here. The flow of MI through to management committees should also be included.

Potential Challenges?

The provision of credit is a subjective area, and will change dynamically in line with the market. IA teams may face challenges in the following areas:

- ***The Black Box model*** – Often organisations understand what goes into their own affordability and creditworthiness calculations but do not have the same knowledge of results provided by CRAs. Firms need to understand the accuracy, timeliness and consistency of this data in order to assess how this impacts lending decisions. IA will need to understand how the data is used so that they can assess the fairness of the lending decisions made.
- ***Evolving lending criteria*** – Lending criteria may change frequently, therefore IA will need to ensure they have a clear timeline of changes over the period of their review to ensure they are considering customer files against relevant criteria.
- ***Identifying unfair outcomes*** – Unfair customer outcomes may take a number of years to materialise, therefore IA will need to ensure they select files over the relevant time period.

Insurance Distribution Directive (IDD) 2018

Assurance over a changing financial services ecosystem

Why is it important?

IDD is a full recast of the Insurance Mediation Directive (IMD). Firms either designing or selling (re)insurance products are now subject to new organisational and conduct of business rules, aiming to enhance consumer protection and ensure a level playing field. IDD also aims to ensure that consumers benefit from the same level of protection regardless of the distribution channel.

The introduction of IDD was initially delayed to allow EU countries until July 2018 to transpose its requirements into national law. The new rules will apply to firms from October 2018, with no transitional period.

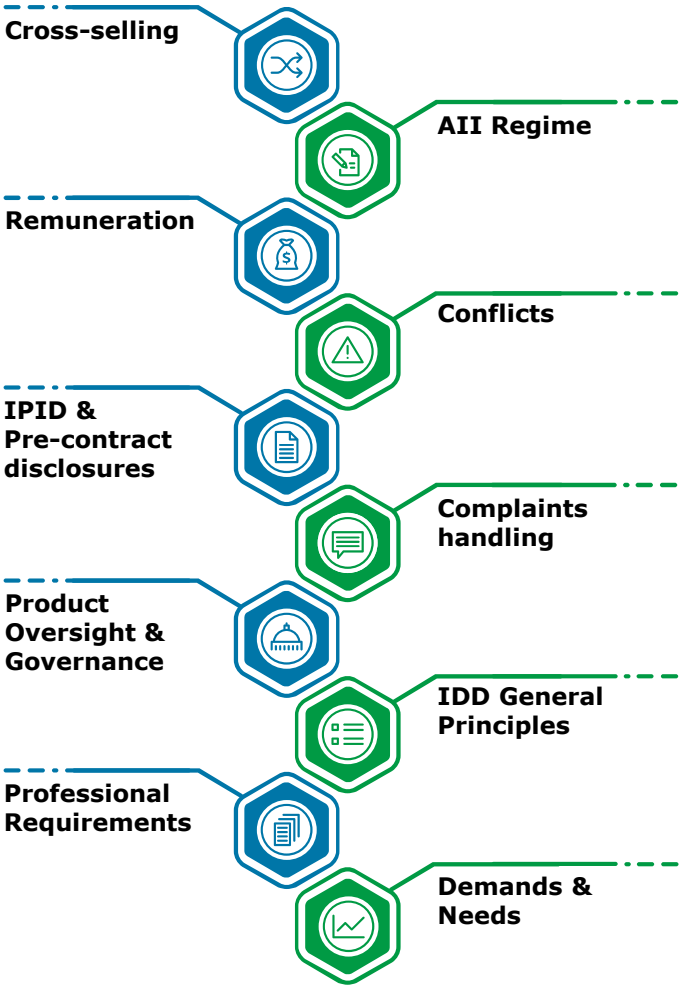
What should you be doing?

Most firms are in the final stages of their IDD implementation programmes and therefore will likely be focused on embedding new or revised processes and controls. IA should focus its work in two key areas:

- Review the firm's gap analysis to assess both the completeness and adequacy of the proposed IDD implementation plan; and/ or
- Perform a post-implementation assessment of the controls and governance framework to ensure ongoing compliance with the new IDD rules.

Areas of particular focus for scope consideration, reflecting the change in IDD requirements, include the following:

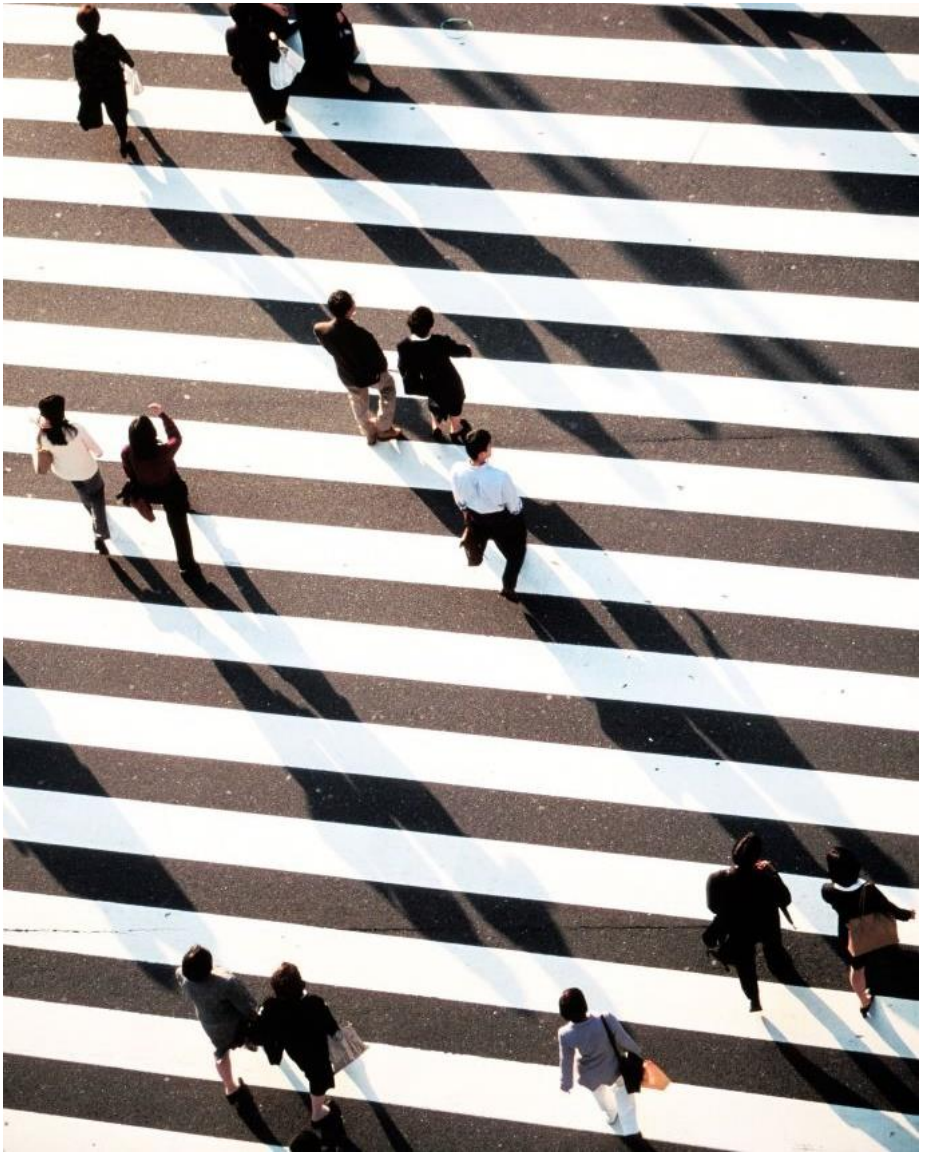
- Complaints handling activities
- Product Oversight and Governance
- Employee Professional Requirements (e.g. CPD)
- Assessment of customer Demands & Needs
- Ancillary Insurance Intermediaries Regime
- Remuneration of staff (including commission structures)
- Potential conflicts of interest
- Insurance Product Information Documents (IPIDs)



Potential Challenges?

Firms may find challenges in the following areas, which should therefore be a focus for IA when assessing compliance with IDD:

- ***Product governance*** – Firms have struggled to classify whether they are the manufacturer and/ or the distributer of products. This inherent challenge, and the lack of clarity, makes it difficult for IA to determine the level of review required.
- ***IPIDs and other pre-contractual disclosures*** – Firms face the challenge of updating the customer journey to ensure that appropriate disclosures are provided before a sale is concluded. Consequently, for most firms, this will require substantial re-design of disclosure documentation and IA may not have requisite in-house skills to assess these against requirements.
- ***Professional requirements*** – IDD brings an increased CPD requirement, with a far larger population of employees now captured. Firms will need to ensure that minimum CPD requirements are met and without systems to capture this information, it may be difficult for IA to undertake validation activity in this area.



Markets in Financial Instruments Directive (MiFID II)

Providing assurance post implementation

Why is it important?

MiFID II is one of the core regulatory pillars of the European FS market and will impact everyone engaged in the dealing and processing of financial instruments.

MiFID II encompasses a broad set of requirements and obligations for firms that are linked through a number of overarching objectives: increased market transparency and transaction reporting, improved execution, greater clarity on trading and investment costs, orderly trading behaviour within markets, enhanced product governance, and improved conflicts of interest management.

Key requirements that MiFID II brings are outlined below:

- Increased market transparency and transaction reporting
- Improved best execution
- Greater clarity on trading and investment costs
- Orderly trading behaviour within markets
- Enhanced product governance
- Improved conflicts of interest management

What should you be doing?

Most firms are in the final stages of their IDD implementation programmes and therefore will likely be focused on embedding new or revised processes and controls. IA should focus its work in two key areas:

- Programme assessment:
  - Review documentation to demonstrate compliance with specific regulatory requirements as well as areas of key judgement or adoption of principle-based approaches.
  - Consider the tactical nature of solutions proposed against the need for long-term viability and sustainability.
  - Review and conclude on the extent to which requirements have been embedded by the business as BAU.
  - Assess the effectiveness of the MiFID II programme with a view to identifying lessons learnt for future large-scale programmes.
- Integration into existing review(s):
  - As MiFID II becomes fully embedded, IA can start to consider requirements as part of other audits. This mirrors the 'each and every' audit approach taken by many functions in respect of cultural audits.
  - The wider IA plan should add value by providing real challenge and assessment on a continuing basis.

Potential Challenges?

IA may find challenges in the following areas reflecting the level of complexity faced by firms:

- ***Scope & complexity*** – MiFID II brings together an extensive and broad set of requirements that are difficult to audit as part of a single review. IA should therefore consider the best approach to reviewing compliance with regulation given the level of complexity and detail in the requirements in a given area.
- ***Regulatory uncertainty*** – There are still some areas of the requirements that lack certainty and this can present challenges when scoping audit reviews, especially where the regulation being audited against is not transparent.
- ***Skills & knowledge*** – As MiFID II comprises such a broad range of topics, firms can struggle to identify the relevant expertise to complete a thorough and challenging audit of how the business is meeting various requirements.

Payment Services Directive (PSD2)

Developing a new payment landscape by 2020

Why is it important?

PSD2 came into effect in January 2018, bringing significant new compliance responsibilities in relation to the provision of payment services to consumers and corporates. The major changes to the payments landscape include Third Party Providers (TPPs) having the ability to initiate payments, access account information on behalf of customers and apply Strong Customer Authentication for electronic payments.

PSD2 poses significant regulatory and operational risk to Payment Service Providers (PSPs) and will impact a range of business areas. Its implementation requires cross-functional collaboration to achieve compliance, owing to a high level of complexity and inherent risk.

What should you be doing?

PSD2 is thematically split into 10 key pillars and different requirements are applicable to firms based on their licences and service provision. Careful scoping is important for IA, and engagement of key stakeholders is vital to understand the business processes, products and platforms in scope.

Depending on the work done by the organisation to ensure compliance on primary PSD2 requirements, the following different approaches can be considered by IA:

- Follow up of gaps from initial PSD2 compliance assessments;
- Full assessment against PSD2 applicable requirements including conduct of business, reporting and RTS requirements against all payment services provided;
- Full assessment against applicable PSD2 requirements implemented post January 2018 (RTS); and
- Assessment against new or changed payment products.

Potential Challenges?

Reflecting the challenges and level of complexity being faced by firms in this space, IA may find challenges in the following areas:

- ***Scoping*** – PSD2 requirements can cover several areas of an organisation and it can be challenging to understand all impacted products and processes to be covered by the audit.
- ***Identification of stakeholders*** – Some business and technical processes may not have clearly assigned owners making establishment of responsibility difficult to assess and to audit.
- ***Documentation*** – Lack of knowledge sharing and complete documentation can lead to inability of the business to clearly evidence compliance to IA.
- ***Technology*** – This may include challenges around legacy systems limitations, limited storage of historical information and difficulty in development of compliance solutions. IA will need to have the right skills mix to audit these areas where they are identified in the business.

IFRS' 9, 15, 16 & 17

IFRS changes will bring operational and implementation challenges

Why is it important?

With the already introduced IFRS 9 & 15, and the scheduled introduction of IFRS 16/ 17 in the coming years – the accounting landscape is rapidly evolving. All of these accounting standards will have a major impact across organisations and, with each of the standards at a different stage of transition, businesses will have choices to make around prioritisation and the extent to which the new standards are material to the organisation.

To consider

There could be forthcoming changes in the credit cycle with rising interest rates and uncertainty in the economy and therefore the performance of IFRS 9 against the much criticised IAS 39 standards during the 2008 credit crunch will be of interest.

What should you be doing?

Since the timing of implementation and impact to current practices will vary by firm, two approaches to audit could be considered for 2019:

- IFRS 9 (non-insurers), IFRS 15 and IFRS 16
  - The new standards will lead to changes in organisation's processes and their systems. IA should focus on reviewing both the (re)design and operational effectiveness of first-year controls. Additionally, IA's work should also focus on documentation of key judgements.
  - For non-insurers and insurance companies not deferring adoption of IFRS 9, financial reporting will be affected in the current period, with IFRS 9 and 15 being fully embedded and operative while IFRS 16 will require transitional disclosures.
- IFRS 9 (deferring insurers) and IFRS 17 – The priorities for IA in respect of standards with an effective date in the future are two-fold:
  - Understanding 'readiness' of the business for the new standards from a project governance and resourcing perspective, including second-order impacts such as Investor Relations and Reward; and
  - Ensuring a holistic risk-based audit plan is prepared which covers the length of the implementation period of the standards and covers all significant areas, whilst including time for remediation findings where necessary.

Potential Challenges?

Changes to these key accounting rules is a significant change project for the majority of organisations and will be a key focus area for internal auditors in 2019 and beyond. IA may find challenges in the following areas:

- ***Evolving approach*** – IA will need to adapt their approach over the lifetime of the implementation of the new standards and then move towards a BAU methodology while still challenging the business appropriately from a technical perspective.
- ***Talent*** – Organisations will need to ensure that audits are resourced with the necessary specialists in finance, change, IT/ technology, actuarial, risk/ regulation/ compliance, as well as teams with appropriate technical accounting skills.
- ***Collaboration*** – Interaction with external audit and other key stakeholders is important to ensure that the work performed by IA adds value.

IFRS' 9, 15, 16 & 17 continued

Key IFRS Changes

IFRS	Title	What does this mean?
9	Financial Instruments	• Hedging rules relaxed enabling hedge accounting to be applied in a way that more closely reflects economic realities – but with additional documentation requirements. • Impairment models changing from an 'incurred loss' model to an 'expected loss' model with the effect of bringing write-downs earlier in the downward arc of a credit cycle. • Some changes in classification of financial assets on the balance sheet.
15	Revenue from Contracts with Customers	• Significant changes to the framework for revenue recognition, introducing a 5-step model. • Requires recognition of revenue estimates to be limited to an amount that is highly likely not to experience reversal. • Additional rules around aligning recognition of income and expenses.
16	Leases	• All lease liabilities will be brought on balance sheets, with corresponding lease assets. • Profiles for recognising the asset and liability in income are not aligned. • Additional capture of data points related to leasing documents, and processes to maintain data integrity, may be needed by some organisations. • Changes to the rules for determining discount rates to be used.
17	Insurance Contracts	• Fundamental change to insurance contract accounting, bringing income statement accounting closer to other IFRS standards. • Many insurers face significant changes to systems and processes to adapt to requirements to calculate Contractual Service Margin, Risk Adjustment, and to track contracts by portfolio in a new way. • The standard is complex and brings in a large number of accounting policy choices. • The accounting for reinsurance contracts can differ between inward and outward risks resulting in misalignment and unexpected income statement effects.

Exposure Management

Minimising catastrophe risk

Why is it important?

Exposure management is a key element of any insurance firm's risk management strategy. A well formulated exposure management framework is a key contributor in the effective pricing of risks, risk retention, reinsurance management, and solvency and capital management.

Given the competitive pricing landscape, an increased reliance on data and increased regulatory scrutiny on capitalisation, exposure management is now, more than ever, at the top of Boards' agendas. A fully embedded and well understood suite of exposure management controls will allow a firm to achieve the full benefit of the exposure management activities and will ensure the company is in compliance with regulatory expectations.

What should you be doing?

Given the regulatory scrutiny in this area, there are a number of potential reviews that IA can perform. These include:

- Data Quality and Modelling: IA's work would focus on the controls in place to ensure data quality is maintained, including a review of the firm's data validation and reconciliation controls and the overall end-user computing (EUC) environment. Additionally, as many firm's rely on the use of third-party modelling software, this audit could also look to ensure there are adequate model security and access controls.
- Assumptions and Judgements: There are often inherent subjectivities in a firm's approach to exposure management. IA can seek to understand where these subjectivities exist and the extent to which these are understood and challenged. This audit could also consider changes to these key assumptions and judgements, with particular focus on the governance controls in place to ensure decisions are documented and approved.

Potential Challenges?

There are several key challenges for IA in this area:

- ***Skillset*** – Exposure management is a complex area of a business's operations and IA functions can typically find it to be a challenging area to audit where they do not have the requisite in-house skillset. Seconding an actuary or utilising external SME support are two potential ways to address this challenge.
- ***Reporting*** – IA may struggle to 'land' observations with management, particularly where these relate to the use of assumptions or the application of judgement and there is no clear control/ process failure to point to.

Model Risk Management

Enabling active management of model error risk

Why is it important?

Model Risk Management and consideration of the end-to end modelling process is a key priority within the FS market.

The Federal Reserve System has recently announced regulation (SR11/7) aimed at formalising model governance in banking. In addition, the ECB launched a Targeted Review of Internal Models initiative, and the Bank of England PRA Stress Test 2017 guidance aimed to create more risk-focused model management in the market.

As a result, the Boards and Regulators are becoming increasingly focused on addressing model risk before it becomes a problem. Key issues which seems to prevail are the fact the model environment and end-to end process is not fully understood and there is usually a lack of clarity over the responsibility of the individual models. Hence the need to set up an effective and robust MRM Framework.

Models of varying sophistication are pervasive to all FS organisations, including areas such as; capital, managing and reporting credit risk, valuations and market risk, regulatory reporting, reserving, and consolidation.

What should you be doing?

Effective audits of model risk are often aligned to a model risk management framework (MRMF). Where a firm has a well articulated MRMF, this can:

- Provide a consistent framework against which IA can audit key process and controls; and
- Serve as an outline for thematic deep dive activity by IA in areas of significant or pervasive risk where the firm does not have a MRMF. IA will need to articulate an approach against which to perform their reviews, this should focus on areas of weakness such as; end-user computing controls, common modern governance and model map completeness.

Where an entity does not have a MRMF, IA can still consider a range of activities. These can include work to map out the full range of models in use in the business, a review of the completeness and accuracy of data in/ outputs and a review of the general EUC environment to ensure model integrity.

Potential Challenges?

IA may face challenges in the following areas:

- ***Consistency*** – Risk management activities focused on model risk can be inconsistent and lack formal framework. This can challenge IA's ability to test model risk in a consistent manner.
- ***Materiality*** – Firms will often focus risk management activities on 'high profile' models (e.g. Capital and Pricing), this may compromise IA's ability to identify or review a complete model suite.
- ***Ownership*** – There is often a lack of clarity surrounding the ownership of models and especially model risk within firms. This can affect IA's ability to identify, review and challenge model risk management.

Solvency II – Matching Adjustment

Demonstrating ongoing compliance with Solvency II

Why is it important?

The Matching Adjustment (MA) is an important tool for insurers with annuity portfolios. It results in a material reduction in the best-estimate of liabilities (BEL) and the solvency capital requirement (SCR) for a business through discounting at a rate higher than the risk-free rate.

The MA is only available after a firm has successfully applied to the PRA and demonstrated that it meets, and has the processes and controls in place to continue to meet, the Solvency II regulations and PRA requirements. This includes ensuring a close ongoing match between annuity cashflows and the cashflows from its assets.

A breach of these conditions must be immediately reported to the PRA and failure to rectify any breach within two months could result in the firm losing its MA approval for two years. Given this, it is imperative that a company has strong processes, controls and governance in place to ensure ongoing compliance.

With many firms having now met the PRA's requirements, there is an increased use of the tool within the insurance annuity market, increasing the risk of non-compliance.

What should you be doing?

There are a range of potential activities for IA to perform in this area:

- As part of the MA approval process, there will be a number of conditions which need to be met for the MA to remain valid. IA can therefore provide assurance that the firm has controls in place to monitor compliance with these conditions, as well as monthly reporting processes to demonstrate that annuity and asset cashflows remain closely matched.
- IA can also look at the governance controls required to maintain a MA approval, particularly those around the use and the monitoring of internal credit ratings. This activity should also include the management of actions in respect of breaches, including escalation.
- IA can also undertake more detailed activity such as reviewing the operational effectiveness of controls around asset eligibility, a key consideration of the MA in the SCR calculation.

Potential Challenges?

Areas of particular challenge for IA can be:

- ***Regulatory uncertainty*** – Firms need to continuously ensure that the assets used in its MA portfolio are eligible, in line with the terms of its MA approval. Care must be taken to demonstrate that assets which are not gilts or corporate bonds (e.g. illiquid or bespoke assets) meet the eligibility criteria for inclusion in the MA portfolio. This can be a complex area for IA to navigate and test.
- ***Complexity*** – It is important that firms have a robust credit monitoring process in place to ensure changes in credit ratings are identified as these arise. Particular care should be taken around assets where internal ratings are used as opposed to external published ones (e.g. equity release mortgages). The methodology underlying internal credit ratings is an expected, yet technical, focus area for IA.

Oversight of 3rd parties (Part A – General)

Identifying and mitigating third party risk

Why is it important?

Recently, there have been several high profile cases where third party supplier failure, or the inappropriate actions of suppliers, have caused either monetary loss or reputational damage. The issue of oversight of 3rd parties has been an issue raised in previous iterations of this publication, however, given these high profile failures it is clear that the risk has crystallised and concern in the market continues to be well placed.

Additionally, FS firms continue to increasingly outsource activities which traditionally would have been undertaken internally, exposing them to additional third party risks (TPRs). This can be due to inadequate controls being in place at, or performance failure of, the third party, or inadequate oversight by the outsourcer.

Regulators are increasingly imposing requirements to examine a firm's framework for identifying, managing, monitoring and reporting of TPRs. Our experience has shown that there is sometimes a cultural misunderstanding in firms, with firms not having as much control or oversight of their third parties as companies have over their own operations. This makes this a key area for IA moving into 2019.

What should you be doing?

IA should consider if the firm has an adequate Third Party Risk Management (TPRM) framework embedded across the business and should examine this from both a design and an operating effectiveness perspective:

Design effectiveness

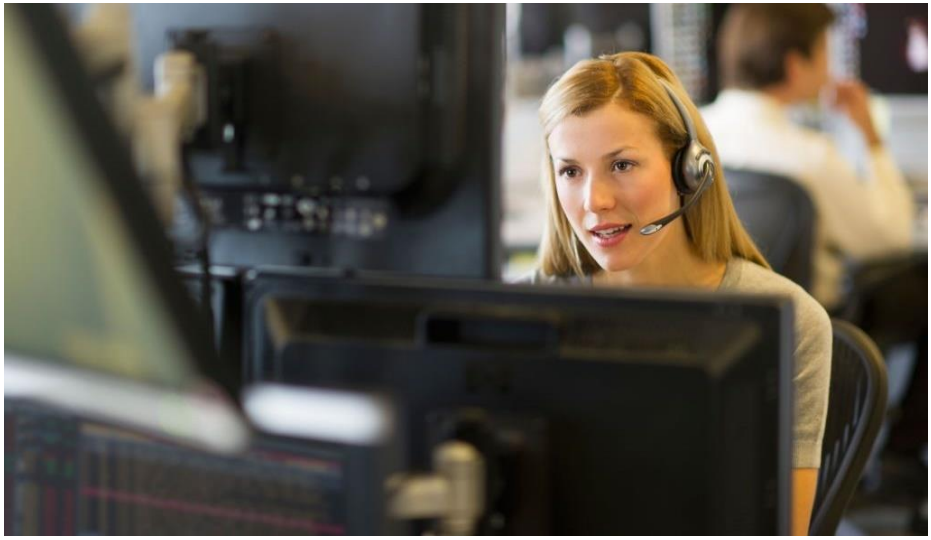
Assess if the following factors are designed adequately:

- Overarching governance framework
- TPR framework and associated policies
- Appropriate allocation of roles and responsibilities
- Processes and controls to manage TPRs throughout their lifecycle
- Tools and technologies supporting the TPRM process
- Appropriateness of metrics used to measure effectiveness of TPRM framework

Operating effectiveness

Assess control performance in the following areas:

- Risk identification and assessment
- Third party selection
- Contract execution
- Role and responsibility allocation
- Ongoing monitoring and reporting assessment appraisal
- Contract termination and exit or renewal management



Potential Challenges?

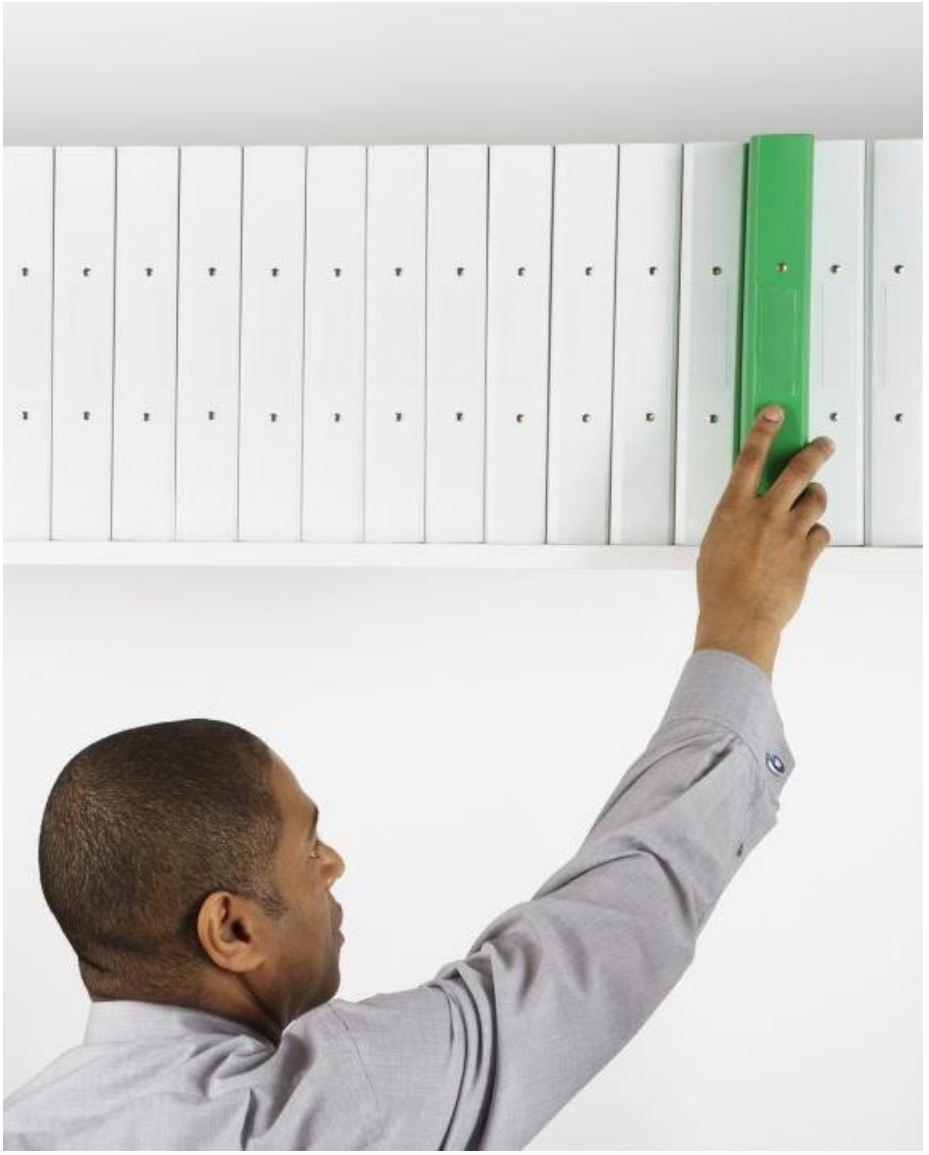
Organisations will have to decide on implementing either a centralised or de-centralised TPR operating model. Most firms will not adopt a purely centralised model, meaning challenges for IA will lie in:

- ***Inconsistency*** – A decentralised model may result in inconsistent application of third party policies and procedures and a lack of a holistic view of risks. Hence IA should seek to challenge instances of inconsistency in application of policy/ methodology.
- ***Complexity*** – Firms may have partially or fully outsourced the management of TPM/ TPRM to external providers. This will lead to additional complexity when undertaking an internal audit of the framework.

To consider

Additionally, IA will face challenges in ensuring they have the technical skills to ensure they can audit compliance with the following new standards in this area:

- FCA's Senior Management Arrangements, Systems and Controls (SYSC) 8;
- PRA's Rulebook requirements on Outsourcing; and
- PRA's Chief Operations Senior Management Function (SMF) 24.



Oversight of 3rd parties (Part B – IT & Technology)

You can't outsource risk

Why is it important?

The trend in outsourcing IT functionality is increasing, and will likely continue to do so given the availability and value of IT outsourced services.

There are various levels of IT outsourcing, with the risk increasing as the provider has greater levels of access to a firm's data and/ or systems configurations.

Services provided should fit the business need (for example continuous access by the provider versus access granted on an ad-hoc basis).

Whatever the level of outsourcing, firms should be clear that the risks will continue to reside within the business.

What should you be doing?

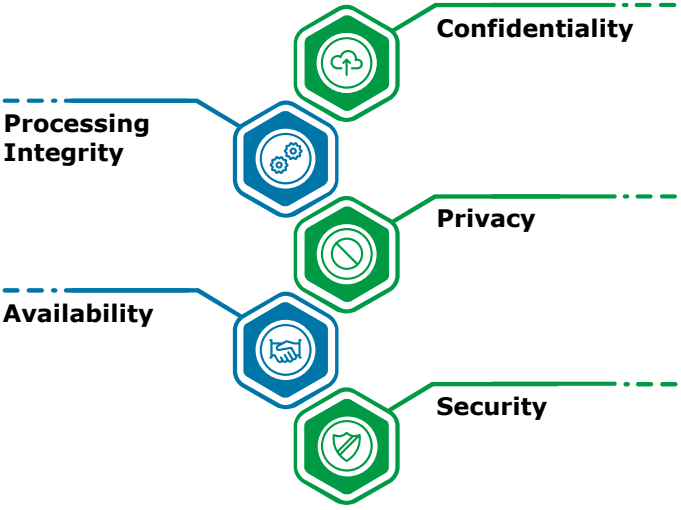
There are a number of activities that IA can perform specifically in the outsourcing of IT area, we have detailed a selection of these below:

- IA can undertake an assessment of the internal function (e.g. IT/ Risk) holding responsibility for governance and oversight over 3rd parties. The objective of this review is to ensure that there is a comprehensive 3rd party risk management framework embedded to ensure risks are sufficiently mitigated.
- IA can also undertake dedicated work over the 3rd party through exercising the contractual right to audit (where this exists). As part of this audit IA should consider reviewing the sufficiency and appropriateness of MI and other ad-hoc reporting provided by the 3rd party.
- IA can also undertake direct testing, or engage an independent 3rd party to review an IT providers control environment (e.g. through specific technology certifications such as ISO27001 /SSAE18 / or assurance reports).

Potential Challenges?

Due to the high number of potential risks in this area, IA may face any number of challenges when conducting their work. Examples include:

- ***Documentation*** – Insufficient documentation of required internal procedures that outline required oversight of the provider. This makes it difficult for IA to audit against an agreed set of principles.
- ***Certification*** – Insufficient clarity over required independent certification, and certification frequency from the IT Provider.
- ***Right to audit*** – The absence of a contractual 'right to audit' can prevent IA from fully discharging its remit where pervasive issues with the provider have been identified.



SSAE18 SOC2 Trust Principles

Risk Culture

Proactively assessing a firm's risk management sophistication

Why is it important?

Risk Management, driven by regulatory pressures and the desire for competitive advantage, is at the heart of why risk culture is at the top of many Boards' agendas.

Increasingly, risk culture is seen as a priority measure for IA (acknowledged by reference within the recently updated FS Code). In particular, a risk intelligent culture is seen as the 'invisible glue' that makes financial institutions work. Also, auditing and assessing risk culture profiles across population demographics is critical for monitoring traction on transitioning towards a desired risk culture.

The risks of not getting risk culture right are:

- Not achieving the organisational purpose, strategy, philosophy, and longer term business objectives; and/ or
- Breaches in risk appetite and/ or regulatory compliance.

Any indication of poor culture can be expected to drive far more intrusive supervisory scrutiny of firms and so increase the regulatory "overhead" borne by a firm.

What should you be doing?

There are a variety of ways to audit risk culture in your business, this includes performing a cultural assessment for each and every audit on the plan, or a dedicated 'big bang' audit. The one-off approach is typically more challenging, however, we have seen success using this approach where IA consider the following factors:

- Align IA's work to an existing risk culture framework (preferably internal to the business in question);
- Building of a repository of evidence;
- Consideration of interviews with key stakeholders; and
- Delivery of findings aligned to the business' strategic objective.

Potential Challenges?

Potential challenges for IA in assessing risk culture include:

- ***Risk culture indicators*** – One of the challenges for IA in auditing risk culture is that they can typically only move as fast as the business. Without a clear risk culture framework to audit against, IA will need to establish what indicators they should use.
- ***Audit approach*** – IA will need to develop a cost effective and efficient approach to audit an organisation's risk culture profile. This will need to be supported by tangible evidence that provides the required level of assurance for reporting to the Audit Committee.
- ***Benchmarking*** – IA will need to access an appropriate benchmark to compare risk culture in the firm against industry expectations. Actions will need to be focused on removing discrepancies between the firm's risk culture and that in the rest of the industry.

Senior Managers and Certification Regime (SMCR)

Strengthening accountability in financial services

Why is it important?

The Senior Insurance Managers Regime (SIMR) came into force in the banking sector in 2016. For insurers the new regime – SMCR – will replace the FCA's Approved Persons Regime and SIMR in December 2018.

In December 2019, all other FCA-regulated firms that are currently subject to the Approved Persons Regime will migrate to SMCR.

In insurance, SMCR will require Senior Managers to take additional steps to ensure the firm's governance and process documentation enable compliance with SMCR. The key features to note:

- Statutory duty of responsibility for senior managers;
- Extension of the Certification Regime; and
- Greater application of the Conduct Rules.

What should you be doing?

Given the difference in SMCR implementation timelines for firms, IA can apply one of two suggested approaches:

SMCR implementation readiness review

Including a focus on:

- Reviewing preliminary deliverables (e.g. gap analysis)
- Assessing delivery against SMCR requirements (and timeframes)
- Reviewing the implementation programme (resourcing, timelines and key objectives)

SMCR compliance review

Including a focus on:

- Completeness and accuracy of the responsibilities map
- Review of the certification population and certification process
- Review of the reasonable steps framework for senior managers
- Review of the sufficiency of the fitness and propriety assessment
- Reviewing the conduct rules breach reporting process

To consider

IA functions in insurance can look to their banking colleagues to leverage work done there over the past two years to assist with their work now.

Potential Challenges?

Audit's of SMCR can be relatively straightforward however, IA may face challenges in the following areas:

- ***Appropriate evidence*** – Auditing how Senior Managers evidence 'reasonable steps' may be challenging. This is likely to broaden the scope of the SMCR review to capture all key SMCR documentation including the firm's wider governance arrangements and the use of the relevant committees to support the senior managers.
- ***Access to key stakeholders*** – Additionally, IA must factor time to interview a sample of senior managers, certified individuals and conduct staff. This may be challenging for IA in the context of ongoing project activities and existing BAU commitments in many firms.

Indirect Taxation

Addressing a changing regulatory landscape

Why is it important?

Indirect taxes are becoming more relevant for FS firms with the introduction of new VAT/ Goods and Services Tax (GST) regimes in places such as the Middle East.

In a similar manner, there is a growing expectation from HMRC in the UK that a companies' tax position is proactively managed and that a greater emphasis is placed on tax at board level – this has led to the introduction of new reporting regimes such as the Senior Accounting Officer ("SAO").

As a transactional tax, VAT is potentially payable on all transactions that a business carries out. It will therefore impact on every aspect of a companies' supply chain, and potentially could be included within the scope of a wide range of audits. Failure to ensure that the correct process is followed and that controls are designed and operating effectively, will likely result in a company being penalised by HMRC.

What should you be doing?

Key areas that may be covered during an IA review of indirect tax include:

- Implementation of new HMRC guidance and legislation. It is important for IA to understand the process by which a business identifies and implements changes to its indirect tax accounting processes.
- From 1 April 2019, new rules are being introduced to make it compulsory for businesses to automate the VAT return completion process. IA should therefore focus on how data is extracted from key systems all the way through to submission of tax returns, focusing on areas of weakness or a lack of control.
- IA should consider reviewing correspondence with HMRC to understand the extent to which the business has complied with required rules and agreed procedures.

Potential Challenges?

IA may face a number of challenges when auditing indirect tax processes and controls, including:

- ***Evolving legislation*** – Tax legislation changes frequently and therefore it is critical that subject matter experts are included on the team. This will ensure that knowledge is accurate and up to date, and that management are challenged in areas of subjectivity.
- ***Systems expertise*** – An array of different accounting systems are used to record accounts payable/ accounts receivable data and for the production of VAT returns. Knowledge of these systems is required in order to understand the robustness of the VAT return completion process, including identifying key controls.
- ***Access to key individuals*** – It is likely that only a few individuals within the business will have an understanding of a group's VAT accounting procedures. Ensuring access to these individuals within a reasonable time-frame will be critical to the success of the audit.

Transfer Pricing

Ensuring a globally consistent approach

Why is it important?

A transfer price (TP) is the price charged in a transaction between two related legal entities. As businesses become more global and with international tax issues high on the political and regulatory agenda, TP issues are a re-emerging area of concern.

HMRC and other tax authorities have increased their functional capabilities, incorporating technological developments (such as analytics) when undertaking transfer pricing reviews.

Additionally, the Base Erosion and Profit Shifting ('BEPS') Action 13 Report, issued in 2018, introduced templates requiring multi-nationals to report annually for each tax jurisdiction (so-called 'country by country' reporting). In many countries, these requirements have been adopted into local legislation, with penalties for non-compliance/ non-filing.

What should you be doing?

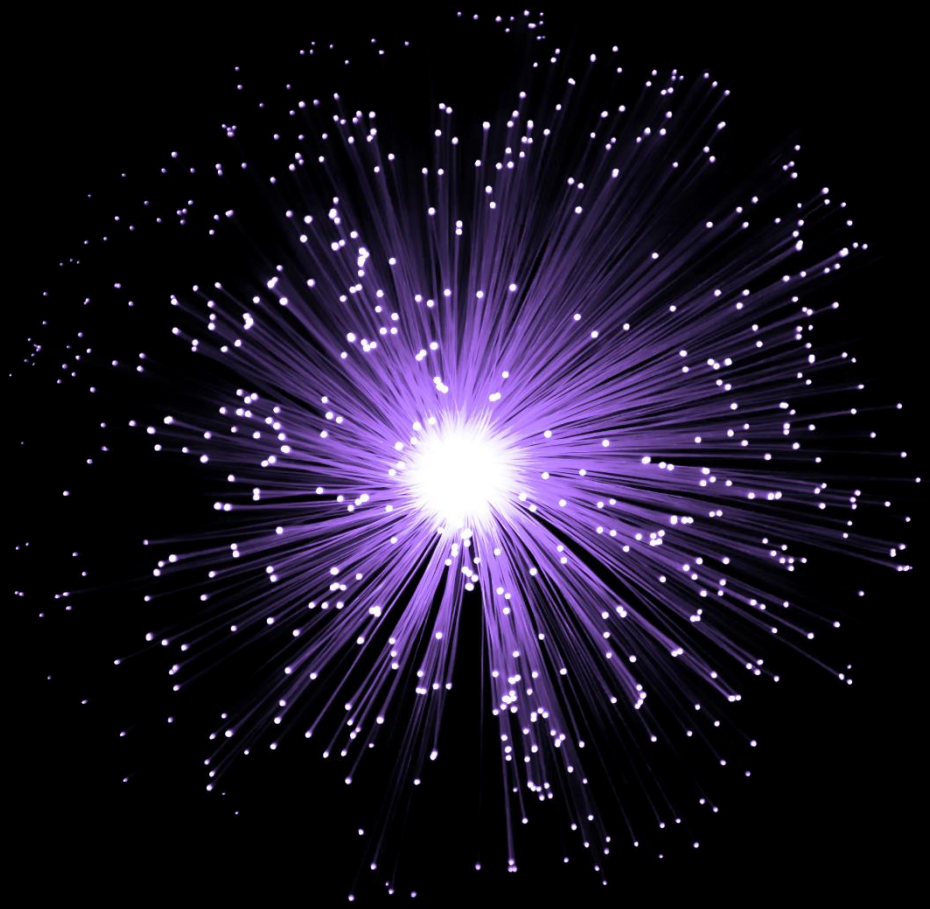
IA should consider performing a risk assessment to determine the scope of transfer pricing risk in the business. The following factors should be considered as part of the risk assessment:

- Whether the company's profits or losses appear inconsistent with its business activities or with worldwide group results over a cycle; whether reasonable levels of interest are being charged on intergroup loans; and any transactions with related parties in low tax territories.
- IA should not only assess the adequacy of the policies and controls in place, but also ensure that these have been implemented appropriately. This can be done by assessing evidence of TP policy reviews being undertaken, the evidence of communication of TP policies, and whether there is a robust review process in place before postings are made.
- IA should assess the dependency on key personnel and the appropriateness of continuity plans should these personnel leave.

Potential Challenges?

Transfer Pricing is a specialist topic, and IA will need to have the skills within their team to perform their work. This could present challenges for IA in the following ways:

- ***Resourcing*** – There may be insufficient understanding of TP risks and tax-technical terminology within the IA function. Due to the often small number of tax specialists within the business, seconding individuals with this knowledge from the business to IA may not be viable.
- ***Difficulty in obtaining information*** – IA will typically have to gather information and evidence from multi-jurisdictional business units and systems. This makes following the audit trail, particularly when trying to re-perform calculations, challenging.



Section 2:
New Methodologies for Internal Audit

Agile Internal Audit

Better, faster, happier

Why is it important?

In our 2018 publication, we highlighted Agile as an emerging topic, where leading functions had begun applying the values and principles to their internal audit work. Since then, there has been a significant increase in the number of IA departments adopting Agile across FS.

Agile IA is a mind-set supporting a collaborative environment for audit and the business to solve audit problems through taking an iterative, time-boxed approach.

Agile may not be for everyone and careful consideration should be given to the potential benefits to each specific financial institution of adopting such an approach, comparing to the costs involved. Hence many IA functions have taken a workshop and pilot approach to assess these factors before deciding whether to undertake more significant investment. Once you have clarity on your vision and Agile IA blueprint, the next step is to pilot.

How can IA use it?

Agile is a proven framework that places focus on teams value and impact. Through the application of Agile techniques, audit teams can deliver better, faster, and happier audits by:

- Helping functions create more value and impact through better interactions with IA's stakeholders;
- Surfacing problems sooner, forcing teams to address and improve areas that could lead to quality issues and driving better quality audits;
- Focusing on team performance, increasing productivity, creating more sustainable working practices and building trust through empowering staff;
- Reducing the input effort required to deliver value and minimising the time between work and providing assurance;
- Allowing IA to adapt rapidly to the changing needs of the business through an iterative and collaborative approach; and
- Creating an ownership culture where teams are empowered to make decisions, learn from each other and feel valued.

Potential Challenges?

IA may find challenges in adopting Agile in the following ways:

- ***Tone from the top*** - Agile is not a methodology, it's a mind-set and framework, supported by techniques and processes. Adopting Agile requires a transformation in leadership behaviour.
- ***Coaching*** - To deliver true mind-set shifts and transformations there needs to be an executive level mind-set shift, and an Agile Champion within the function. Those functions who have been most successful in their adoption of Agile have been supported by Agile IA coaches to help teams change their behaviours.

Talent

Addressing the Internal Audit resourcing needs of the future

Why is it important?

As this document clearly demonstrates, there is an increased focus on the role and remit of IA, and audit committees are increasingly challenging functions to provide more complex assurance. With this, there is greater emphasis on hiring from non-traditional IA backgrounds (e.g. accountants) in favour of industry and subject-matter specialists (e.g. actuaries, conduct and risk specialists, data scientists, etc.).

Addressing IA's talent needs through diversification of the team will allow IA to respond to both today's and tomorrow's challenges.

How can IA use it?

Whilst it is increasingly common for larger IA functions to have in-house data analytics, cyber security and actuarial capabilities, many functions will not be able to draw on these resources. For those functions with a more traditional resource base, consideration of the following will help to address this challenge:

- Identify skill gaps – IA functions should perform a preliminary assessment of potential skill gaps. Discussions with direct reporting lines and audit committee members will help to identify which gaps are deemed to be a priority.

- Use of co-source partners – many external providers can offer access to specialise skillsets on a 'pay as you go' basis. This option is attractive for IA functions with limited budgets and/ or one-off engagements requiring specialist support.
- Leverage existing firm skillsets – the use of business secondees is a popular option to plug skill gaps. Leveraging in-house skills from established IT, data analytics and other teams is a cost effective way of addressing gaps on a short term basis.

Potential Challenges?

With a number of topics in this document, we have identified talent as an area of concern. In an evolving FS market we expect this trend to continue, however, this highlights several key challenges:

- ***Budgets*** – Specialist resources often come with a high price tag. With IA budgets typically remaining static, recruitment of specialist resources may be considered a luxury.
- ***Timing*** – Identifying the right individuals at the right time may take time.
- ***Training*** – Individuals transferring to their first role in IA may require a period of training to understand key working protocols and terminology.

Quality Assurance (QA)

Continuous improvement, value creation and culture

Why is it important?

The remit, scope and approach of audit functions is under increased focus, with stakeholders and regulators looking to assess the value, the reach and the impact of IA.

In response, IA functions (large and small) are refreshing their approaches to QA to focus on all aspects of audit quality. Correspondingly, the scope of audit QA now typically includes:

- Methodology compliance;
- Audit risk;
- Continuous improvement opportunities;
- IA value creation;
- Learning and development; and
- Culture.

Our experience suggests that some functions have embraced a supportive QA approach incorporating "quality coaching" that is supportive yet still maintains independence and objectivity.

Other firms continue to take more of a "policing" approach, focusing on methodology compliance and ensuring strict independence between IA staff.

How can IA use it?

Increasingly, IA teams are using different types of QA which, in combination, are designed to embed audit quality at all stages of the audit process. The goal of this activity is to also support ongoing development and continuous improvement of the audit team. Typical examples include:

- In flight reviews – Shadowing of reviews at key points of the audit cycle with active engagement and real time feedback to the team.
- Thematic reviews – Focused post-audit reviews of high risk/ high impact areas across a sample of reviews.
- Continuous monitoring – Tracking of QA KPIs, identification of emerging trends, and/ or material issues and visibility for the whole function.
- Analytics - Use of data analytics in some larger functions to provide real time sight of quality hot spots (e.g. timing of review, quantity of documents retained on file, timeliness to archive). Use of this continuous monitoring capability will help build a forward looking, proactive role to drive improved standards.
- Reporting – In larger functions, formalisation of regular meetings between Heads of QA and AC Chairs to support their stewardship of this role.

Potential Challenges?

IA may face challenges in adopting a revised QA approach in the following ways:

- ***Resourcing*** – The adoption of a new QA approach may require increased resources, technical skills or SME capability. In some cases, IA functions have looked to outsource this activity.
- ***Communication*** – A new approach may bring changing requirements. Any changes will need to be proactively managed with clear communication amongst all those involved.
- ***Approach*** – IA functions with a well developed and clearly articulated QA approach may benefit from a regulatory dividend where confidence in IA may lead to a less intrusive approach.
- ***Responsive*** – With the introduction of Agile IA, audit teams will need to consider development of a responsive QA approach reflecting the values and principles of this methodology.

Web-Based Risk Sensing (WBRS)

Using open-source data to identify emerging risks

Why is it important?

The increase focus on data has prompted new, efficient and targeted ways of accessing and analysing information. Risk sensing, the practice of analysing open-source data, can help identify emerging risks.

It can also help a firm address a number of challenges, including:

- Monitoring and tracking the regulatory environment, including identifying changing regulatory regimes across the globe;
- Identifying risks specific to the business and "connecting the dots" across different risk areas;
- Generating insights by analysing the data to create actionable intelligence for key business decision-makers; and
- Understanding the extent of a firm's digital footprint.

How can IA use it?

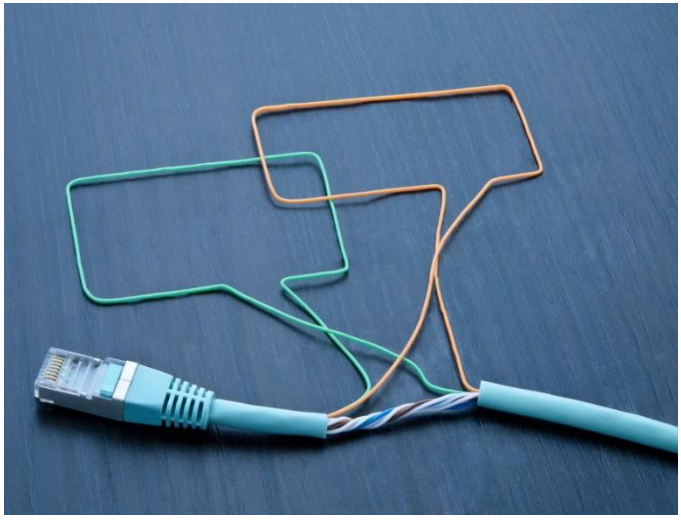
Whilst WBRS is an emerging technology, it can produce actionable intelligence for IA and can be used throughout the annual planning and audit lifecycle as follows:

- Risk assessment and annual planning: IA can use WBRS as a tool to identify emerging risks. Additionally, it can be a useful tool to provide the audit committee with a view of potential hidden risks;
- Audit scoping: WBRS can also be used during the audit planning process to identify key priorities and potential scope areas; and
- Audit fieldwork and reporting: Additionally, WBRS can be used to supplement IA's fieldwork and reporting to analyse data and provide additional insights on the business.

Potential Challenges?

IA may face challenges in the following areas:

- ***Impact*** – WBRS relies on these open-source data including results derived from scanning social media platforms such as twitter and Facebook. A potential challenge with its use as a tool for IA can be that it relies on this information, perceived, often incorrectly, as less accurate than internally generated management information.
- ***Knowledge gap*** – WBRS is an emerging technology and one of the perceived barriers to its use by IA functions is ease of access. WBRS tools typically exist as a managed service and there are a several providers in the market. Discussion with these providers can provide greater clarity on WBRS capabilities and potential uses for IA.



Behavioural Analytics

Technologies designed to quantify conduct risk

Why is it important?

Companies are facing unprecedented levels of regulatory scrutiny, with a particular focus on conduct risk and firms' ability to identify and monitor the risk of poor outcomes for customers.

Behavioural analytics solutions allow companies to:

- Move beyond traditional monitoring methods and focus on a more data-driven, automated outlook to assess risk across the organisation;
- Extract patterns of unusual behaviour that require further investigation, using historic behavioural indicators as a basis to assess conduct risk more holistically over a given period;
- Move away from time and resource intensive review processes to a more efficient methodology; and
- Identify financial crime, prevent fraud and money laundering, ensuring regulatory compliance as well as monitoring high-risk areas such as trading or brokerage.

How can IA use it?

Behavioural analytics represent the cutting edge of technological innovation and can be used by both the business and IA to improve the way they work. There are two areas of focus for IA to consider:

- As a tool for the 1st and 2nd lines of defence, IA need to be able to challenge whether the use of the technology is appropriate. The most effective way to do this is to understand whether the algorithms underpinning the business operations have introduced bias. IA also need to challenge the business as to whether nuanced outcomes, such as "fairness", are appropriate; and
- As a tool for IA, behavioural analytics can look beyond more traditional testing methods in areas of potential risk. This allows for increased coverage of populations, as well as additional insights that can be leveraged through reviewing interactions that are inaccessible with standard methods.

Potential Challenges?

Challenges for IA in auditing behavioural analytics platforms lie in:

- ***Benefits vs costs*** – Finding the balance between the cost of labour, implementation and maintenance of behavioural analytics tools and the benefits these tools bring.
- ***Actionable results*** – Validating analytics driven insights to make sure they provide clear and actionable outcomes for the business.
- ***Exceptions*** – Defining exceptions may be difficult as there are often no clear lines delineating issues/ risks.
- ***Security considerations*** – Using behavioural analytics tools may require data collection. IA must ensure all regulations are complied with, and that the data collected is not misused.
- ***Good quality data*** – Getting access to appropriate quality data in a timely manner remains an issue for IA analytics teams.

Call Monitoring Technology

New insights through the deployment of innovative solutions

Why is it important?

There is a growing level of expectation from the FCA's conduct risk agenda to ensure that services offered achieve a positive customer outcome. Current review processes are typically resource intensive, with large teams devoted to reviewing customer interactions.

The use of technology provides an opportunity to review and enhance existing business processes and controls in this area. Voice analytics platforms use cognitive technology and risk algorithms to monitor voice interactions based on tone of voice and behavioural and human emotional tendencies.

How can IA use it?

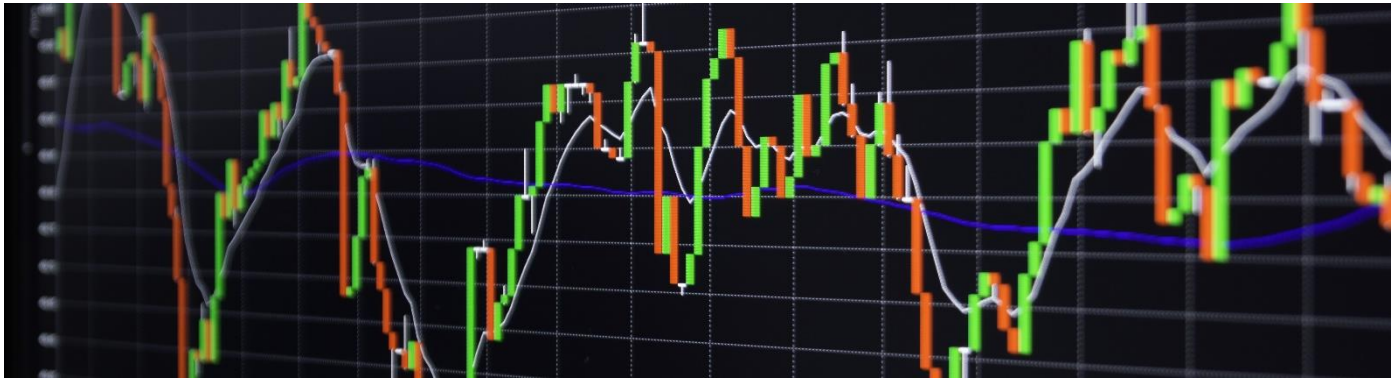
Call monitoring technology solutions provide multiple benefits over traditional sampling/ testing approaches, and have been designed to support multiple use-cases. These include:

- Increased coverage of call monitoring, potentially replacing traditional audit sampling;
- Reduced manual effort and cost, enabling resources to focus on high-risk interactions;
- Improved customer service outcomes through proactive identification of high-risk calls and detailed visibility over interactions;
- Can be deployed with minimal integration to existing architecture enabling rapid benefit realisation; and
- The use of technology brings greater accuracy to call listening and assessing regulatory compliance.

Potential Challenges?

Firms have thousands of hours of call data that can be used by IA using call monitoring technology to gain clearer insight into sale practices and provide assurance around treating customers fairly (TCF) responsibilities. However, use of these tools may still give rise to following challenges:

- ***Integration*** – Integrating into the audit plan on either a specific audit or 'each and every' audit basis may be challenging. This will rely on advanced scoping prior to work commencing.
- ***Sample population*** – Selection of an appropriate, representative sample population will allow IA to get the most out of the tool.
- ***Access*** – Access to data may prove to be a challenge as without this IA may not be able incorporate its use into the testing approach. Other considerations include data use and ensuring compliance with relevant regulations, e.g. GDPR.



Risk Assessments

Increased transparency in the assessment and audit of risks

Why is it important?

Some IA functions have found that a traditional planning model can lead to a lack of transparency in the risk assessment process with audit plans based on risk-assessing auditable entities not necessarily translating later in the audit cycle into detailed focus on the key risks.

Other suboptimal impacts found in traditional planning processes include inconsistencies in the size of auditable entities, in part as a result of:

- Irregular structuring of the audit universe;
- A lack of focus on individual auditable entities; and
- Inconsistent interpretation of which risks should be assessed on an entity-by-entity basis.

Consequently, many functions are revising their planning approaches to increase transparency and consistency in the identification and initial assessment of risks, tracking these through to individual audits.

How can IA use it?

IA functions should take the opportunity to review their risk assessment process and audit universe, using this exercise to increase clarity surrounding how the plan has been formulated and how the key risks are communicated to audit committees and other stakeholders. When undertaking this exercise IA should consider alignment with other assurance providers in respect of both risk taxonomy and reporting.

A starting point would be to review and re-establish the principals behind the audit universe and the audit plan – what is IA trying to achieve? The principal goal should be to reinforce the link between initial risk assessment and the risks covered in the planning and execution of individual audits.

Other benefits can include greater comfort over the completeness and composition of the audit universe, increased efficiency through greater focus on only key risks, and greater clarity of roles and responsibilities within the audit function for individual risks or auditable entities.

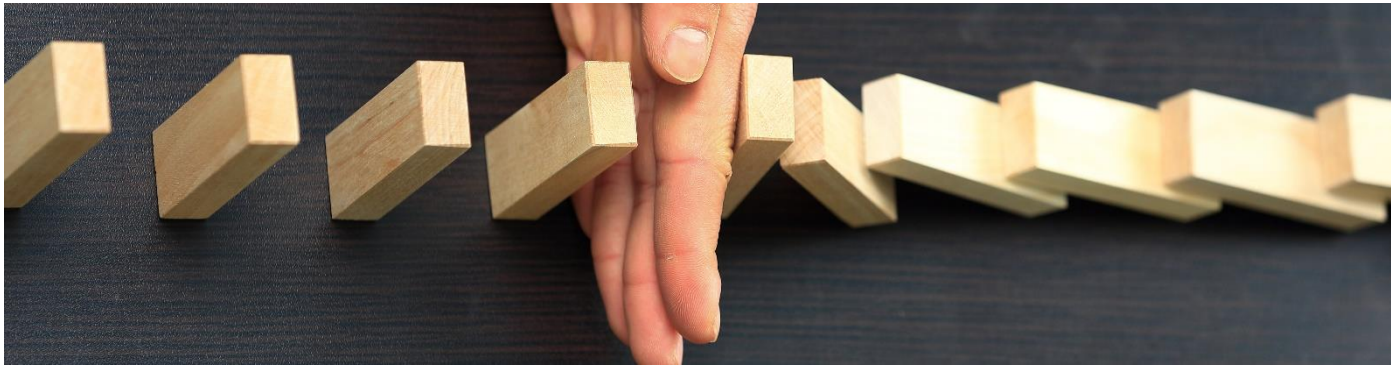
Potential Challenges?

IA may face challenges in the following areas:

Change – Revising an established risk assessment and planning methodology can be time-consuming, especially for larger functions and those that have an deeply-embedded and technology-enabled risk assessment and planning process.

Materiality – Establishing the level/ size of auditable entities within the audit universe is critical – each should be large enough to be meaningful and to contain material risks but should be sufficiently granular to focus attention on key risks and to facilitate detailed operational planning (and to cover specific areas of focus such as regulated subsidiaries).

Transition – Changes to the audit plan may require a transitional "catch-up" period to adjust from previous the previous coverage model to the new audit model.



Contacts – Financial Services Internal Audit

Russell Davis

Partner, Banking and Capital Markets

020 7007 6755

rdavis@deloitte.co.uk

Matthew Cox

Partner, Insurance

020 7303 2239

macox@deloitte.co.uk

Terri Fielding

Partner, Investment Management and Private Equity

020 7007 6755

rdavis@deloitte.co.uk

Mike Sobers

Partner, Technology

020 7007 0483

msobers@deloitte.co.uk

Matt Cheetham

Partner, Regions (South)

0117 9841 158

mcheetham@deloitte.co.uk

Jamie Young

Partner, Regions (North)

0113 292 1256

jayoung@deloitte.co.uk

Notes

Deloitte.

Important notice

This document has been prepared by Deloitte LLP for the sole purpose of enabling the parties to whom it is addressed to evaluate the capabilities of Deloitte LLP to supply the proposed services.

Other than as stated below, this document and its contents are confidential and prepared solely for your information, and may not be reproduced, redistributed or passed on to any other person in whole or in part. If this document contains details of an arrangement that could result in a tax or National Insurance saving, no such conditions of confidentiality apply to the details of that arrangement (for example, for the purpose of discussion with tax authorities). No other party is entitled to rely on this document for any purpose whatsoever and we accept no liability to any other party who is shown or obtains access to this document.

This document is not an offer and is not intended to be contractually binding. Should this proposal be acceptable to you, and following the conclusion of our internal acceptance procedures, we would be pleased to discuss terms and conditions with you prior to our appointment.