

IDEAS | PEOPLE | TRUST

Internal Audit Support

Banking & Building Societies

July / August 2024



IBDO

BDO FS INTERNAL AUDIT CONTACT POINTS

BDO's Banking & Building Societies Update summarises the key regulatory developments and emerging business risks relevant for all banks, building societies and, where flagged, for alternative finance providers (i.e., peer-to-peer lenders, card providers, E-money services providers and debt management companies).

Our FS Advisory Services team are working with more than 50 banks and building societies as internal auditors and advisors, giving us a broad perspective on the issues facing the sector. We have aggregated insights from our in-house research, client base, the Regulators and professional bodies, including the Chartered Institute of Internal Auditors (CIIA), to support your audit plans and activities.

We hope this pack provides value to you and your colleagues; please do share with us any feedback you may have for our future editions.



Leigh Treacy
Partner

+44 (0)7890 562 098
leigh.treacy@bdo.co.uk



Chris Bellairs
Partner

+44 (0)7966 626 128
christian.bellairs@bdo.co.uk



Sam Patel
Partner

+44 (0)7970 807 550
sam.patel@bdo.co.uk



Bruk Woldegabreil
Associate Director

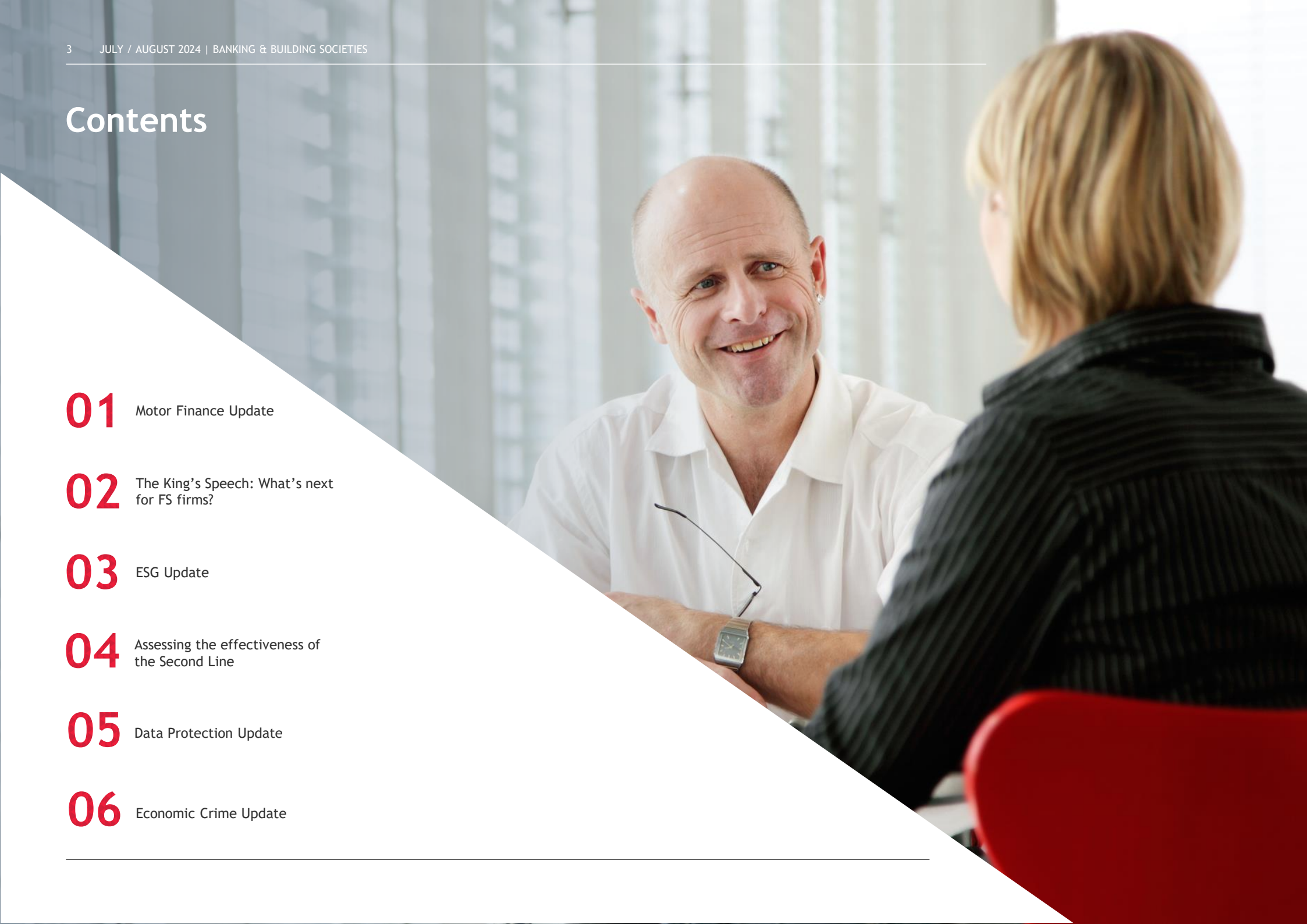
+44 (0)7467 626 468
bruk.woldegabreil@bdo.co.uk



Oliva Gledhill
Manager

olivia.gledhill@bdo.co.uk

Contents

- 
- 01** Motor Finance Update
- 02** The King's Speech: What's next for FS firms?
- 03** ESG Update
- 04** Assessing the effectiveness of the Second Line
- 05** Data Protection Update
- 06** Economic Crime Update
-

01

Motor Finance Update



Alison Barker
Special Adviser

alison.barker@bdo.co.uk



Motor Finance Update

In January 2024, the Financial Conduct Authority (“FCA”) announced a review into past sales of motor finance with discretionary commission arrangements. This caused a pause for breath by motor finance lenders as the potential for a remediation exercise, stretching back to 2007, loomed over the sector.

The FCA said it would communicate the outcome of its review, including next steps, by 25 September 2024. That now doesn’t seem too far away.

Since January, firms who provided motor finance, have been considering the potential impact. Some, such as Lloyds Banking Group, have made provisions against a possible remediation programme. Compared with Barclays who made a court application in April to quash the Financial Ombudsman’s decision on a case. The case involved the payment of commission to the credit broker and the customer was unaware commission had been paid.

The issue at stake is the divergence between decisions made on cases heard in the court, against decisions made by the Financial Ombudsman service. The Ombudsman is looking to block Barclay’s application for a judicial review and is quoted recently as claiming Barclays is arguing ‘academic points’.

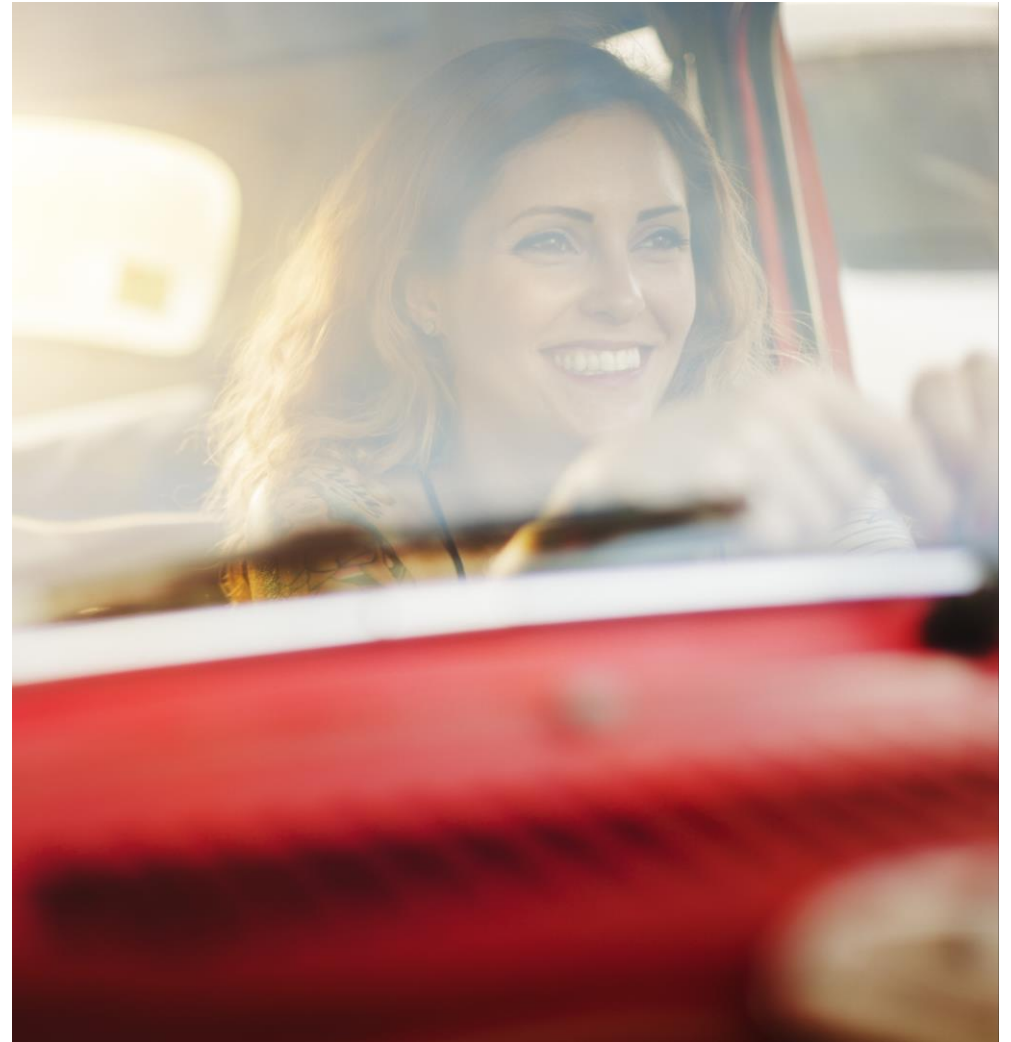
What does this mean for the FCA’s timeline?

Potentially, the Judicial Review case could extend beyond the FCA’s original date of 25 September 2024 and delay any meaningful announcement. However, consumers are still being urged to log complaints. This means there will still be many complaints that need to be resolved whether the Barclays case is successful or not.

What should Internal Audit teams think about?

We could see Internal Audit functions within regulated lenders being asked to provide assurance over motor finance remediation projects to cover the lending completed by firms, stretching back to 2007, as part of the FCA’s remediation exercise.

This could include providing assurance that the risks, processes and controls identified as part of any remediation projects are appropriate to manage the regulatory expectations. The Internal Audit function will need to assess that any regulatory changes have been factored into the remediation plans to ensure compliance with the FCA requirements. In addition, once the remediation projects have been implemented or alongside these, Internal Audit assurance may be required to ensure that firms are now operating in line with regulatory expectations and discretionary commission arrangements.





02

The King's Speech: What next for FS firms?



Alison Barker
Special Adviser

alison.barker@bdo.co.uk

The King's Speech and the potential impacts to the retail financial services sector

The King's Speech is used to communicate the legislative priorities for the new incumbent government over their next Parliamentary term and show how manifesto commitments are translated into legislative priorities.

It always takes some time for regulatory initiatives to flow from new Government policy and we will await the update to the Regulatory Initiatives Grid. For Heads of Internal Audit, it is important to note what upstream regulatory developments (and therefore, risks) should be on IA's radar for annual planning discussions.

Key financial sector bills from the King's Speech

There are plans to get Britain building, including through planning reform, as the new government seeks to accelerate the delivery of high quality infrastructure and housing (Planning and Infrastructure Bill). As a retail financial services firm, lending is a core activity and therefore, firms need to be aware of this and think about how their lending strategy/policy and plans may need to change.

The new Pensions Schemes Bill is set to provide legislative framework to improve outcomes for 15 million people who are saving in private pension schemes and release potential for investment to boost economic growth.

An ageing population and the prominence of defined contribution pensions create a need for reforms that address the risks of people not saving enough, not investing wisely or not being able to sufficiently and easily access pension pots. It's a complicated set of factors that require coordination of government and regulators to create an environment that enables individuals to successfully fund retirement. As a result in 2015, the government introduced the Pensions Freedom Act.

In the pipeline are measures to address the advice/guidance boundary in place and the FCA has set out a number of improvements through its recent Thematic Review of Retirement Income Advice which tackles standards for advice on deaccumulation. The new pensions bill will see consolidation of individuals' small pension pots, value for money standards applied to pensions, and address the cliff edge between accumulation and deaccumulation. For defined benefit pensions, proposals would see the ability to consolidate these.

Bank Resolution (Recapitalisation) Bill: This Bill will enable the Bank of England to recapitalise small banks who are in resolution through the use of FSCS funds which will be raised through a new levy on the banking sector. The objective is that by placing these costs on the banking sector, it mitigates the risk of taxpayer funds being used to resolve small banks.

Digital Information and Smart Data Bill: This Bill will enable new, "innovative" uses of data to help boost the economy. It is proposed to establish digital verification services, including digital identity products, to help people quickly and securely identify themselves when they use online services.

Cyber Security and Resilience Bill: an expansion in regulation to cover more digital services and supply chains, empower regulators to ensure cyber security measures are implemented, and mandate increased incident reporting to improve the government's response to cyber-attacks.

Artificial Intelligence (AI)

The King's Speech did not include an AI bill, which had been expected, but outlined how the government would "seek to establish the appropriate legislation to place requirements on those working to develop the most powerful artificial intelligence models". It is possible the Government needs to take stock of the current position before proposing further legislation.

Financial Sector Regulators previously outlined numerous challenges and few benefits of regulating AI. However, the new Digital Markets, Competition and Consumers Act 2024 received Royal Assent at the end of May 2024. This Act gives the Competition and Markets Authority ("CMA") broad powers across all sectors to address competition issues in digital markets. It applies to those firms designated as having 'strategic market status' i.e. Big Tech firms. The CMA has commented that "AI-powered products and services are likely to become increasingly prevalent across a wide range of sectors and are, therefore, potentially relevant to all of the CMA's current functions, which are not limited to specific sectors. AI is also clearly relevant to the CMA's anticipated new digital markets functions."

What should Internal Audit teams think about?

We are seeing Internal Audit functions utilise data analytics and AI to conduct audit testing on entire data sets to provide complete assurance as opposed to the traditional method of sample testing. With focus on data, cyber security, increased use of data analytics and AI as part of the core IA methodology and testing approach, there is a growing emphasis on the quality and integrity of the underlying data being used. Internal Audit functions need to be sure that they can rely on this data when forming their assurance opinions. As a result, we will see more businesses integrating data quality checks into their regular audit activities. With more firms using facial recognition and voice identification as their standard form of customer ID, the storage and accuracy of this data is critical to ensure compliance with GDPR regulations. The Pensions Scheme Bill could lead to enhanced scrutiny on governance and compliance over pensions schemes against the new legislation.

The King's Speech and the potential impacts to the retail financial services sector

Internal Audit will need to focus on how pension schemes are overseen within firms to ensure compliance with the new legislative requirements, this includes any risks associated with investment strategies and the controls in place to manage these risks. In addition, other audits we could see within firm's internal audit plans relating to the Pensions Scheme Bill could be:

- ▶ Advice and guidance
- ▶ Consolidation of Pensions Pots
- ▶ Value for Money
- ▶ Consolidation of Defined Benefit Pensions
- ▶ Transition from Accumulation to Deaccumulation.



03

ESG Update



Adam Soilleux
Director

adam.soilleux@bdo.co.uk



Gloria Perez Torres
Associate Director

gloria.pereztorres@bdo.co.uk



Four key ESG assurance considerations to move you closer to your ESG objectives

ESG data assurance helps financial services firms in ensuring data accuracy and reliability.

Obtaining third party assurance is a key milestone in a firm's ESG journey and a key factor in achieving your ESG objectives. However, the decision on what type of assurance to obtain is not an easy one.

What type of assurance is best

The two main types of assurance for ESG are Third-Party Assurance and Third Line of Defence Assurance (Internal Audit).

Third-Party Assurance

This is the highest level of assurance. The most widely used external assurance standards for non-financial data are issued by the International Auditing and Assurance Standards Board:

- ▶ International Standard on Assurance Engagements 3000 (ISAE 3000), Assurance other than Audits or Reviews of Historical Financial Information
- ▶ International Standard on Assurance Engagements 3410 (ISAE 3410) Assurance Engagements on Greenhouse Gas Statements
- ▶ International Standard on Assurance Reports on Controls at a Service Organisation 3402 (ISAE 3402) on the controls at a service organisation.

These Standards are internationally recognised for the verification of sustainability and ESG reports, including greenhouse gas KPIs.

There are two levels of ESG assurance, reasonable and limited. Reasonable assurance is a higher but not absolute level of assurance, in which the auditor affirms that the information reported is materially correct. In contrast, limited assurance states that the auditor is not aware of any material modifications that should be made, and the data was prepared in line with the methodologies or data gathering processes that you put in place, limited is the most common.

Internal Audit

Through Internal Audit, Boards can obtain assurance over the functioning of internal controls and the accuracy of ESG data which has been tested.

Internal Audit is independent from the governing body and the management of a firm, and thus assures the reliability of internal control processes for ESG data disclosure and reporting. It can objectively align the Board's data source with objective internal assurance, independent of management.

To provide assurance, Internal Auditors can test internal controls on ESG disclosure and assure that ESG data is collected consistently, to improve confidence in the data collection process and calculations carried out. Internal Audit is in a unique position to present clear opportunities to ensure two-way communication and feedback between the first and second lines, given that it is in the best interests of all to support the firm in achieving its ESG objectives. This is because Internal Audit already has an existing relationship with management, whilst the relationship with the Third-Party Assurance Provider will need to be developed from year one onwards.

The outcome is enhanced and reliable financial and non-financial reporting to internal and external stakeholders.

Key issues to consider when deciding the approach and level of assurance

1. The type of Third-Party Assurance

If the decision is to obtain limited or reasonable assurance, firms should ensure that the auditors providing assurance over the data, key business processes, and control areas are experienced in applying the relevant International Standards.

2. A flexible approach

Firms should ensure that the scope of the assurance provided can be tailored to its reporting needs and data universe, and it should be prepared in a manner that can be flexed in the future as the firm sets further ESG targets. For example, most firms are already reporting on carbon emissions and net zero goals. Going forward, the approach should be able to accommodate nature-positive commitments in line with the suggested recommendations by the Taskforce on Nature Related Disclosures.

3. The audience

Consider the audience of the assurance report. A Third-Party Assurance report is normally available to external stakeholders like customers, suppliers, lenders, or insurers, given that this will inform their decision making. Indirectly, the audience can include governments, regulators, or law firms. An externally available assurance report can reassure current and potential investors on the stability of your organisation.

Four key ESG assurance considerations to move you closer to your ESG objectives

In contrast, the Internal Audit report is only available to an internal audience. It will mainly provide assurance to the Board, and it will inform the Executive's strategic decision-making process.

4. What is next?

There is increasing demand for ESG assurance reports as a result of greenwashing cases, changes to regulatory requirements and expectations, and forthcoming legislation which will specifically demand formal assurance over data included within public disclosures, such as the EU Corporate Sustainability Reporting Directive.

What should Internal Audit teams think about?

The business, alongside the Internal Audit team, needs to decide on the best approach for conducting ESG assurance and whether this is completed by:

- ▶ the Internal Audit team
- ▶ the Internal Audit team in partnership with an external specialist
- ▶ a brand-new external third-party assurance provider.

This decision will not be made solely within the Internal Audit function but will involve input from the firm's key stakeholders to ensure that the correct assurance option is obtained. The decision will likely hinge on factors such as the maturity of the company's ESG capabilities, the specific need for an external assurance report to satisfy investors or regulatory demands, and the existing skill set within the internal audit team.

The Internal Audit team can provide key input into these discussions by providing a clear assessment of their skills relating to ESG, the firm's current ESG risk profile (from any prior work completed) and any regulatory requirements which may factor into this decision. Ensuring that people with the appropriate skillsets are conducting this assurance assessment is key to obtaining meaningful recommendations.



04

Assessing the effectiveness of the Second Line



MISELO MUMBA
Manager

miselo.mumba@bdo.co.uk



GURKIRAT SABERWAL
Assistant Manager

gurkirat.saberwal@bdo.co.uk



Assessing the effectiveness of the second line of defence

The importance of the Second Line in a firm's risk management arrangements

In the dynamic business of banking, the second line of defence is pivotal to managing risks and ensuring operations are conducted within safe and defined limits. Drawing on specialists in Risk Management and Compliance, an effective second line helps shape the risk management strategy, providing expertise, support, and a critical eye on business practices through its review, monitoring and challenge role.

Boards need a second line that is not only proactive and robust, but also practical and independent. They want to place strong reliance on the second line to pre-emptively identify risks, advise on risk controls, and ensure compliance with regulatory requirements. Boards view the second line as a strategic ally, providing insights into risk trends and emerging threats, and helping to drive the firm's risk management strategy and regulatory compliance.

In January 2024, the Financial Reporting Council ("FRC") announced several updates to the UK Corporate Governance Code ("the Code"). The changes under Provision 29 are the most significant and one of the key factors is that the Board should monitor their firm's risk management, internal control framework and at least annually, carry out a review of its effectiveness. As a consequence of this update, there is a growing importance for second line functions to carry out their activities more robustly to support the Board.

How does this impact Internal Audit?

Internal Audit needs to assure the Board by:

- ▶ providing an independent view of the Second Line's effectiveness
- ▶ considering the extent to which Internal Audit can place reliance on Second Line's activities, particularly those relating to assurance over the risk and control activities in the first line.

This will also ensure internal audit is meeting the expectations of the (IPPF) Standards and FS Code now, and established to deliver conformance to the incoming Global Internal Audit Standards and Code of Practice which will require greater documentation of combined assurance.

A mature and effective second line should enable internal audit to develop a more targeted internal audit plan, in particular, reducing some of its first line controls testing, and using the second line's output to inform IA's assurance work over areas that pose the largest risks to the firm.

Add to this a productive relationship between Internal Audit and the Second Line Risk and Compliance Functions, and a well-developed combined assurance plan, and we have a situation where the overall assurance provided to the Board is in really good shape. It also helps to avoid assurance fatigue in the business which can be a real issue where assurance activities are not coordinated, or are seen as duplicative or running concurrent, eg, back to back reviews of the same area regarding the same risks.

From our market experience, we note that many firms are at varying stages of risk management maturity and so Internal Audit must understand the challenges the second line may be facing and adapt its approach accordingly. To achieve this, Internal Audit should assess the factors that shape the effectiveness of the second line, particularly in small or medium size firms where there are more likely to be resource constraints and less mature risk management frameworks in place.

The challenges we often see from our advisory work include:

- ▶ A lack of capacity and/or technical skills to cover all of the elements of the risk universe. It's tough to get the appropriate breadth and depth of coverage in a relatively small team so how is the 'shortfall' addressed to ensure all higher priority risks get the right level of second line attention? Cyber and IT risks are commonly underserved given the specialist skills that are required
- ▶ A lack of tools and integrated reporting means the second line can spend too much time collecting and aggregating information/data and so has less time to assess what the information is telling them and provide plain-speaking insights to the Board
- ▶ Varying maturity and quality of first line risk and control self-assessment programmes and risk incident reporting can eat into second line effectiveness, ie, second line teams effectively carrying out first line risk activities
- ▶ Forming a view and defining what is 'proportionate' when it comes to risk management activities is somewhat subjective and can be difficult when seeking to balance cost considerations with business and regulatory needs and expectations. How do small to medium sized firms get a picture of what 'good' looks like for scale of risk management?

Assessing the effectiveness of the second line of defence

- ▶ The blurring between the first and second lines, particularly where the second line is providing a lot of support and guidance to the first line on its risk and control activities. This is very common where a firm's risk and control framework is less mature, and the first line risk and control awareness/discipline is not fully effective. In turn, this weakens the second line's ability to provide objective oversight, review and effective challenge to the business on how its managing its risks. It can also inadvertently hinder embedding risk and control accountability and culture in the first line
- ▶ A lack of alignment of assurance methodologies which reduce consistency and quality across the Three Lines.

These factors mean internal audit needs to apply a greater degree of judgment and appropriate scoping when looking at the second line, particularly where there are acknowledged shortcomings. In these situations, internal audit is likely to add more value by focussing on design effectiveness (and the associated enhancement plans), together with the interim controls or workarounds in place pending embedding of improvements.

What should Internal Audit teams think about?

Where internal audit is less likely to be able to place strong reliance on the second line's assurance activities, IA may, pending approval from the AC and safeguards to maintain IA's organisational independence, need to extend its coverage accordingly while facilitating the development of the Second Line. Teams need to think about how often to review the second line.

Internal Audit is also in the business of risk management, and so should feel confident in giving its view on the effectiveness of the second line. This works well when there is good two-way engagement between the second and third lines. Teams should also think about how they establish and maintain an effective relationship with the second line (for example, via regular meetings to share views).

In situations where there is a disconnect between IA and Risk, which we have seen through our team's EQA work, then an independent cosource specialist can help bring in a fresh and objective perspective on the Second Line's effectiveness and break through any logjams / difficult conversations to ensure the Board has what it needs to demonstrate effective review of controls taking place to support its corporate governance.



05

Data Protection Update



Christopher Beveridge
Managing Director of Privacy &
Data Protection

christopher.beveridge@bdo.co.uk



Data Protection Update

The surprise call for a General Election in May 2024, signalled an abrupt end to the passage of the Draft Data Protection and Digital Information Bill through the UK Parliament. The Draft Bill had proposed a number of changes to the existing data protection legislative framework in the UK; however, the bill was not included on the list of priority legislation that was hurried through in the final weeks before the General Election, which meant it did not become UK law.

Although the recent King's Speech included reference to a new Digital Information and Smart Data (DISD) Bill, we await the detail of what will be included. This means that for now, the UK Data Protection Act 2018 (UK GDPR) is here to stay.

So why is this relevant for Internal Audit teams within the financial services sector? Read on.

Data Processing in Context

The UK Information Commissioner's Office (ICO) is one of the most active regulators in Europe, with a range of enforcement powers at its disposal including reprimands, enforcement notices, individual prosecutions and of course financial penalties (£17.5m or 4% global turnover, whichever is greater).

In the last 12 months, the ICO has issued enforcement action to six financial services firms. Some of the infringements include:

- ▶ Making unsolicited direct marketing calls to individuals who had not provided consent. In some cases, callers were found to be persistent, aggressive, rude at times, and ignored requests from individuals not to be contacted again
- ▶ Sending direct marketing text messages to individuals without their consent
- ▶ Failure to ensure the accuracy of customer data, which was subsequently incorrectly recorded on customers' credit profiles
- ▶ Insufficient information security measures in place, meaning that personal data was compromised during a cyber-attack.

Impact of non-compliance

ICO enforcement action is publicly available, and often picked up by media outlets which can adversely affect a firm's reputation and reduce consumer trust. This can ultimately impact the bottom line, and is especially significant, given that individuals often have the option of using their purchasing power elsewhere.

It's also worth noting that the Financial Conduct Authority (FCA) also has the power to issue fines and penalties for failing to prevent data breaches. In November 2023, the FCA fined Equifax just over £11 million for failing to manage and monitor the security of UK consumer data which had been outsourced to its parent company in the US. The control environment was hit by cyber-hackers accessing the personal data of approximately 13.8 million consumers. Equifax was noted by the regulator to not have provided sufficient oversight of how personal data was managed and protected.

What should internal audit teams think about?

Internal audit teams within the financial services sector should consider the following aspects when reviewing data protection:

- ▶ Marketing activity on the basis of consent - The ICO has issued enforcement action across all sectors, but particularly for financial services firms regarding distribution of marketing information to individuals without their consent. Internal audit teams should, therefore, consider whether consent management processes are robust and transparent, that individuals genuinely exercise choice, that processes in the event that an individual withdraws consent are embedded and whether the firm could evidence consent in the event of challenge
- ▶ Cyber security - Internal audit teams need to be comfortable that there are appropriate information security arrangements in place (technical and organisational controls) to reduce the risk of a data breach
- ▶ Robust data breach management processes - Certain types of data breach must be reported to the ICO within 72 hours of discovery. Internal audit teams should consider whether internal processes for notification, assessing the severity and external reporting requirements (where applicable) are robust and fully embedded, to meet the defined time limits for reporting. Consideration should also be given to employee awareness initiatives, to ensure that breach management processes are adhered to on an on-going basis
- ▶ Increased use of Artificial Intelligence & innovative technologies - The use of AI and emerging technologies raises privacy concerns and impacts on consumer trust. Firms should be fully aware of the impact from use of AI on their data protection control environment and adherence to Data Protection by Design and Default in any new technology which poses a risk to individual rights. Given the transformative power and increased use of AI, the ICO confirmed its renewed focus on ensuring that AI technologies are implemented in a way that complies with the principles of UK data protection legislation.

06

Economic Crime Update



Vladimir Ivanov
Senior Manager

vladimir.ivanov@bdo.co.uk



James Fergusson
Manager

james.fergusson@bdo.co.uk

Economic Crime Update

The Latest Wolfsberg Group Statement on Effective Monitoring for Suspicious Activity

On 1st July 2024, the Wolfsberg Group, a prominent association of global banks dedicated to enhancing financial crime compliance standards, released a statement on effective monitoring for suspicious activity.

Whilst Wolfsberg Group publications, such as the statement evaluated, below, are typically targeted at banks, Internal Audit teams across the financial services sector should pay close attention to the guidance as it provides the basis for first and second line teams to meet regulatory requirements. It should be noted that the FCA's Financial Crime Guide cites the Wolfsberg Group's guidance as sources of information for Anti-Money Laundering (AML) controls.

This statement provides crucial guidance for firms to bolster their AML frameworks and enhance their capabilities in detecting and mitigating suspicious activities. For firms, the Wolfsberg Group's statement is more than just a set of recommendations; it's a call to action to enhance their monitoring systems. The statement emphasises the importance of a risk-based approach, where resources are allocated in line with the level of risk exposure. This means that firms must assess their own risk profiles and tailor their monitoring systems accordingly, rather than adopting a one-size-fits-all approach.

Key Points of the Statement

Holistic Approach to Monitoring

The Wolfsberg Group emphasises the importance of a holistic approach to transaction monitoring. This includes integrating various data sources, such as customer information, transaction history, and external intelligence, to gain a comprehensive view of potential risks.

Risk-Based Approach

The statement advocates for a risk-based approach to monitoring. Firms should tailor their monitoring systems based on the specific risks associated with different customer profiles, products, services, and geographies. This ensures that resources are focused on areas with the highest risk.

Advanced Analytics and Technology

The Group highlights the role of advanced analytics and technology in enhancing monitoring effectiveness. Machine learning and artificial intelligence (AI) can significantly improve the detection of unusual patterns and behaviours, enabling more accurate and timely identification of suspicious activities.

Continuous Improvement and Adaptation

Firms are encouraged to continually review and improve their monitoring systems. This includes regularly updating their systems to adapt to emerging risks, regulatory changes, and advancements in technology. Continuous improvement ensures that firms remain agile and responsive to the evolving financial crime landscape.

Collaboration and Information Sharing

The statement underscores the value of collaboration and information sharing among firms, regulators, and law enforcement agencies. Effective information sharing can lead to more robust detection of suspicious activities and enhance the overall effectiveness of the AML ecosystem.

What should Internal Audit teams think about?

Third line teams are critical to the firm's AML framework, and the Wolfsberg Group's recent statement brings with it a number of considerations for review planning:

Enhanced Monitoring Capabilities - review work should consider (where appropriate on a risk-sensitive basis given the nature, scale, and complexity of the firm's risks) leveraging technologies, such as AI and machine learning, to enhance transaction monitoring capabilities. Implementing advanced analytics can lead to more precise identification of suspicious activities, reducing false positives and improving overall effectiveness of assurance activities.

Focus on High-Risk Areas - adopting a risk-based approach allows firms to allocate resources more effectively, concentrating on high-risk customers, products, and regions. This targeted approach ensures that IA is supporting first and second line teams in mitigating the most significant threats and ensures compliance with regulatory expectations.

Continuous System Updates - internal audit teams need to establish a framework for regular review and improvement of their monitoring systems. This includes staying abreast of regulatory developments and incorporating feedback from internal audits and reviews from other assurance providers for the annual planning process.

Strengthened Collaboration - enhancing IA's combined assurance with other assurance providers is critical to maximise the third line's finite resources.

The Wolfsberg Group's statement provides a comprehensive roadmap for firms to strengthen their AML frameworks. Internal Audit can significantly enhance the firm's capabilities to detect and prevent financial crimes by adopting a holistic, risk-based approach, leveraging advanced technologies, committing to continuous improvement, and fostering collaboration with industry bodies.

Economic Crime Update

What does this mean for Internal Audit

As a result of the latest Wolfsberg Group Statement on effective monitoring for Suspicious Activity, Internal Audit functions will need to consider how to identify suspicious activities across their entire audit plan. With an increased focus on using AI and data to monitor transactions and identification of suspicious activities, Internal Audit will need to provide assurance on the accuracy and completeness of the data being used for these monitoring processes and that there are controls in place to ensure that this data is free from manipulation.

In addition, firms will need to ensure that there is a culture of doing the right thing and that individuals below senior management have an appropriate level of understanding on how to spot and report suspicious activity, Internal Audit could assess this as part of a culture audit or looking at the whistleblowing processes.

FCA calls on firms to improve treatment of Politically Exposed Persons

On 18 July 2024, the Financial Conduct Authority (“FCA”) issued its much-awaited update regarding the treatment of Politically Exposed Persons (PEPs).

This is important for Internal Audit teams within FS firms that provide assurance over risks from retail products or services provided to mass markets that could have exposure to PEPs. Considering that over 64 countries globally have, and will hold, political elections over the course of 2024 (effectively half the world’s population voting) it’s important that IA is evaluating the effectiveness of the second line’s management of PEP risks as political representatives come in and out of many offices.

As part of their initial review, the FCA contacted over 1,000 UK PEPs and received 65 responses.

The FCA then undertook data-gathering and analysis with FS firms from 5 retail sectors and commonly found that:

- ▶ some firms used definitions for PEPs and their relatives and close associates (“RCAs”) that are wider than those in the UK Money Laundering Regulations (“MLRs”) and the FCA’s guidance
- ▶ some did not have effective arrangements to assess if the PEP classification was still appropriate after the PEP had left public office
- ▶ a few did not consider the customer’s actual risk in their assessment and rating, and did not give a clear rationale for their risk rating
- ▶ firms needed to improve the clarity and detail of their communications with PEP and RCA customers
- ▶ most firms needed to improve their staff training programmes

- ▶ some firms needed to update their policies to reflect recent legislative amendments to treat UK PEPs and RCAs as having a lower level of risk than a foreign PEP, unless they have other risk factors.

Based on the feedback received and their observations, the FCA has advised firms that they must enhance their efforts to ensure that individuals with political connections and their families, are treated fairly and without undue prejudice.

According to UK legislation, these firms are required to conduct additional checks on PEPs to prevent financial crimes, in line with the international standards set by the Financial Action Task Force, which have been adopted by numerous jurisdictions globally.

The FCA has reviewed the current approach and found that while most firms are not subjecting PEPs to unnecessary scrutiny or denying them services based on their status, there is room for improvement. The FCA has advised firms to:

- ▶ narrow their definition of a PEP, as well as their family members and close associates, to what is strictly necessary by law
- ▶ reassess the status of PEPs and their associates in a timely manner after they leave public office
- ▶ communicate clearly with PEPs, in accordance with the Consumer Duty, and provide explanations for any actions taken when possible
- ▶ assess the actual risk level of the PEP and ensure that any information requests are appropriate to that risk
- ▶ enhance the training provided to employees who handle PEP accounts.

The FCA is also consulting on amendments to its PEP guidance (as outlined in FG17/6). The proposed amendments within consultation (GC24/4) include:

- ▶ clarifying that non-executive board members (NEBMs) of UK civil service departments should not be treated as PEPs
- ▶ allowing more flexibility in the sign-off process for PEP relationships while ensuring the Money Laundering Reporting Officer (MLRO) maintains oversight
- ▶ reflecting the legislative change that domestic PEPs are considered lower risk than foreign PEPs unless other risk factors are present (as of 10th January 2024, per the latest update to Regulation 35 of the MLRs)
- ▶ The FCA is seeking feedback on these proposals by 18 October 2024, and the FCA plans to publish the final amended guidance after considering the feedback received.

Economic Crime Update

In response to the FCA's review, firms are advised to:

- ▶ review and update their risk management policies, procedures, and controls for PEPs and RCAs to align with the latest legislation which considers UK PEPs and RCAs as lower risk unless additional risk factors are identified
- ▶ address any gaps in their current frameworks, ensuring policies and procedures are consistent with the updated MLRs and the FCA's Guidance, and provide staff with practical guidance for a risk-based approach to PEPs and RCAs
- ▶ communicate clearly with customers, particularly PEPs and RCAs, about the information being requested and the reasons for such requests, in compliance with Consumer Duty requirements
- ▶ provide comprehensive training to staff, using case studies and other practical tools, to ensure policies and procedures are applied consistently and effectively in line with the MLRs and the FCA's Guidance.

What should Internal Audit teams think about?

Internal Audit should consider the appropriate level coverage over the firm's financial crime framework to support compliance with the FCA's update on the improved treatment of PEP's, including review of:

- ▶ the firm's risk management framework specifically looking at the PEPs and RCAs ensuring they align with the latest legislation, provide recommendations on how any gaps in these frameworks can be rectified and help teams track progress against these; and
- ▶ the training provided by firms relating to PEPs to ensure that this is in compliance with new regulatory requirements.



FOR MORE INFORMATION:

Sam Patel

+44 (0)7970 807 550
sam.patel@bdo.co.uk

Bruk Woldegabreil

+44 (0)7467 626 468
bruk.woldegabreil@bdo.co.uk

This publication has been carefully prepared, but it has been written in general terms and should be seen as containing broad statements only. This publication should not be used or relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained in this publication without obtaining specific professional advice. Please contact BDO LLP to discuss these matters in the context of your particular circumstances. BDO LLP, its partners, employees and agents do not accept or assume any responsibility or duty of care in respect of any use of or reliance on this publication and will deny any liability for any loss arising from any action taken or not taken or decision made by anyone in reliance on this publication or any part of it. Any use of this publication or reliance on it for any purpose or in any context is therefore at your own risk, without any right of recourse against BDO LLP or any of its partners, employees or agents.

BDO LLP, a UK limited liability partnership registered in England and Wales under number OC305127, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. A list of members' names is open to inspection at our registered office, 55 Baker Street, London W1U 7EU. BDO LLP is authorised and regulated by the Financial Conduct Authority to conduct investment business.

BDO is the brand name of the BDO network and for each of the BDO member firms.

BDO Northern Ireland, a partnership formed in and under the laws of Northern Ireland, is licensed to operate within the international BDO network of independent member firms.

Copyright © 2024 BDO LLP. All rights reserved. Published in the UK.

www.bdo.co.uk