IDEAS | PEOPLE | TRUST

Internal Audit Support

Banking & Building Societies

October 2024

Welcome to your October update

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; such as 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.

Key contacts
BDO FS Internal Audit

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

Olivia Gledhill
Manager

olivia.gledhill@bdo.co.uk

Paul Gilbert
Partner

+44 (0)7890 323 336
paul.gilbert@bdo.co.uk

Bruk Woldegabreil
Director

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

Contents

01

Dear-CEO letter on APP fraud reimbursement

Dear-CEO letter on APP fraud reimbursement

In October 2024 The Financial Conduct Authority (“FCA”) issued a "Dear CEO" letter to Banks & Building Societies. The letter outlines the new requirements and expectations for Payment Service Providers (“PSPs”) regarding the reimbursement of victims of Authorised Push Payment (“APP”) fraud. The letter coincides with the implementation of the Payment Systems Regulator's (“PSR”) new reimbursement regime, which became effective on 7 October 2024 and requires PSPs to reimburse customers who fall victim to APP fraud up to £85,000 per claim.

Vladimir Ivanov
Senior Manager, FS Advisory

Vladimir.ivanov@bdo.co.uk

Key elements of the FCA’s Dear-CEO letter

Reimbursement obligations
Under the new rules, PSPs are obligated to fully reimburse victims of APP fraud. This applies to payments processed through the Faster Payments System (“FPS”) and the Clearing House Automated Payment System (“CHAPS”). Reimbursement costs are shared between the sending and receiving institutions, encouraging both parties to strengthen their fraud prevention efforts. PSPs must also maintain robust governance, systems, and controls to manage these obligations effectively.

Systems and controls
The FCA expects PSPs to implement robust fraud prevention systems and controls, including at onboarding and through ongoing transaction monitoring. The FCA emphasises that PSPs should:

- have effective governance arrangements, controls and data to detect, manage and prevent fraud;
- regularly review their fraud prevention systems and controls to ensure that these are effective; and
- maintain appropriate Customer Due Diligence controls at onboarding and on an ongoing basis to identify and prevent accounts being used to receive proceeds of fraud or financial crime.

Consumer protection and support
Under the Consumer Duty, PSPs are required to ensure that customers are well-informed and adequately supported throughout the payment lifecycle. This includes providing clear information about their rights in cases of fraud and informing them about alternative dispute resolution options, such as the Financial Ombudsman Service. PSPs must also act swiftly to rectify situations where harm has been caused to consumers, ensuring redress when appropriate. The FCA specifically refers mentions intra-firm payments which are executed through an internal channel rather than through FPS or CHAPS. The PSR’s reimbursement policies for APP fraud will only apply to payments routed through FPS and CHAPS, therefore the FCA expresses its concern regarding the potential lack of consumer understanding that the level of protection that a PSP provides against APP fraud may vary depending on the type of payment process used. The FCA places the onus of ensuring that customers understand that they may not be protected (or protected to a lesser extent only) for certain payments, depending on the payment process used, firmly on PSP firms. Any PSPs considering providing lower levels of protection for payments that are not sent through FPS or CHAPS, are encouraged to contact the FCA to explain how they intend to meet their Consumer Duty obligations in this space.

continued >

Dear-CEO letter on APP fraud reimbursement

Data collection and monitoring
The FCA, in collaboration with the PSR and Pay.UK , will actively monitor firms' compliance with the reimbursement regime. It will collect data on payment execution timings, delayed payments, and fraud reimbursements to ensure that firms are complying with the new requirements without adversely affecting the broader payments system. The data-driven approach is intended to identify any breaches in conduct and prudential standards and ensure consumer protection.

What does this mean for Banks & Building Societies

The new reimbursement rules represent a significant shift in how APP fraud cases are handled in the UK. Payment service providers, including Banks & Building Societies, must now enhance their fraud detection capabilities and improve coordination between sending and receiving institutions to reduce the risk of fraud. The shared responsibility for reimbursement is designed to encourage PSPs to take more robust preventative measures and improve their internal controls. The most notable implications for Banks & Building Societies include:

- **Enhanced fraud prevention and detection systems:** PSPs will need to invest in advanced fraud prevention and detection systems.
- **Staff training and awareness:** Ensuring that staff are well-trained to recognise and handle APP fraud is crucial. PSPs will need to provide regular training sessions and updates to keep their teams informed about the latest fraud tactics and prevention strategies.
- **Customer education:** Educating customers about the risks of APP fraud and how to protect themselves is a key responsibility for PSPs. This could involve running awareness campaigns, providing information on websites and apps, and offering advice on secure payment practices.
- **Clear reimbursement policies:** PSPs must have clear and fair reimbursement policies in place. This includes setting out the criteria for reimbursement, the process for making a claim, and the timeframe for resolving claims. Transparency in these policies will help build consumer trust.
- **Collaboration with other PSPs:** Working together with other PSPs to share information and best practices is essential. This collaborative approach can help to identify and mitigate fraud risks more effectively.
- **Regular reporting to the FCA:** PSPs will need to establish processes for regular reporting to the FCA. This includes providing data on fraud incidents, prevention measures, and reimbursement activities. Accurate and timely reporting will be crucial for demonstrating compliance with the FCA's expectations.

The financial and operational impact of these rules is substantial. Increased liabilities from reimbursement may strain resources, requiring firms to reassess their capital adequacy and liquidity strategies. Moreover, failure to comply with the FCA's expectations could result in regulatory scrutiny, fines, and long-term reputational damage. Firms will need to strike a balance between preventing fraud and maintaining the efficiency of legitimate payment processing.

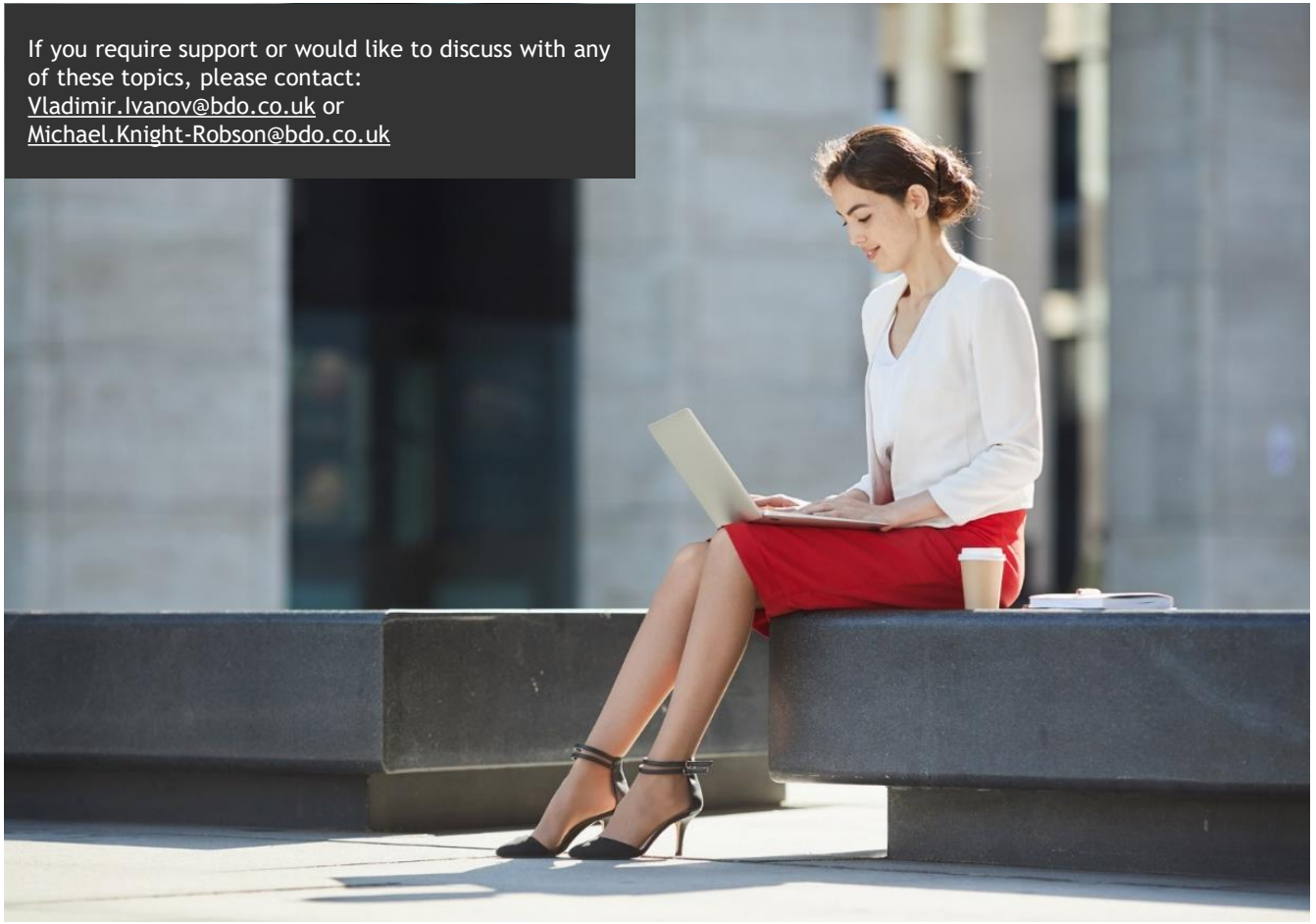
continued >

Dear-CEO letter on APP fraud reimbursement

In summary, the FCA's October 2024 Dear CEO letter underscores the importance of strengthening anti-fraud systems, sharing reimbursement responsibilities, and ensuring comprehensive customer support. The new framework demands that PSPs actively work to reduce APP fraud, not only to protect consumers but also to safeguard their financial and operational stability in a more stringent regulatory environment.

What should Internal Audit teams think about?
Internal audit will need to focus on assessing the robustness of fraud prevention systems and controls, particularly those related to onboarding and transaction monitoring, including assessing that governance arrangements, data management, and Customer Due Diligence processes are effective in detecting and preventing fraud. Internal audit should also evaluate the clarity and fairness of reimbursement policies, ensuring they align with the FCA's requirements and are transparent to customers. Additionally, there could be benefits to reviewing staff training programmes in this space to confirm that employees are well-equipped to handle APP fraud and that customer education initiatives are effective. Auditors will need to ensure that there is enough expertise within their functions to for reviewing fraud prevention measures and reimbursement processes. Internal audit plans may need to incorporate regular assessments of compliance with FCA reporting requirements, ensuring that data on fraud incidents and reimbursements is accurate and timely.

If you require support or would like to discuss with any of these topics, please contact:
Vladimir.Ivanov@bdo.co.uk or
Michael.Knight-Robson@bdo.co.uk



02

Internal Audit-led penetration testing

Internal Audit-led penetration testing

The objective of a penetration test is to check how strong an organisation's security measures are by simulating the actions of a threat actor. The importance of penetration testing has become even more topical recently due to evolving regulatory requirements.

In the UK, the Financial Conduct Authority ("FCA") and the Prudential Regulation Authority ("PRA") have introduced stricter guidelines on operational resilience and cyber security. The FCA's operational resilience framework mandates that financial services organisations identify critical business services and test their ability to withstand severe disruptions, including cyber-attacks. Additionally, the EU's Digital Operational Resilience Act ("DORA"), expected to take effect soon, will require financial institutions to regularly conduct thorough testing of their cybersecurity defences, including penetration testing, to meet compliance standards.

Traditionally, penetration tests have been managed by IT or Information Security teams however, a penetration test can also be seen as a valuable tool to provide third line assurance. Conducting a penetration test will allow an internal audit function to attempt to achieve some of the same objectives as a threat actor, thereby providing real insights as to how well the cyber security posture of the organisation is working. In essence, it can answer the fundamental question 'are we protected?' which is of key concern to senior stakeholders.

What are the benefits of Internal Audit conducting penetration testing?

Penetration testing within internal audit offers numerous advantages. Internal audit's independent role ensures that cyber security assessments remain objective, free from the potential biases that may arise when IT departments assess their own systems. By evaluating vulnerabilities in broader context of business risks and reputational impacts, internal audit offers a more strategic view of cybersecurity.

This comprehensive approach helps financial institutions not only detect technical vulnerabilities, but also understand their potential impact to the wider business. Internal Audit's experience in reporting to senior stakeholders means that internal audit is well-positioned to explain cyber security issues and risks in a way that aids evaluation of risk exposure, informs decision-making, and helps ensure that resources are effectively prioritised to address the most critical vulnerabilities.

From an efficiency perspective it can also be argued that a penetration test offers a broader deeper dive into cyber controls than a conventional audit, whilst absorbing fewer resources.

continued >

Steve Dellow
Director, Digital Risk Advisory

steve.dellow@bdo.co.uk

Internal Audit-led penetration testing

Key challenges

Despite these benefits, there are challenges when incorporating penetration testing into internal audit testing. One significant issue is the skills gap. Internal auditors may lack the technical expertise required to conduct penetration testing, necessitating investment in training or hiring specialists. This imposes resource constraints, especially for smaller organisations with limited budgets.

It may also be difficult to attach an assurance rating to a penetration test using conventional methodologies and internal audit functions may need to take a step back in order to incorporate results of penetration tests into overall assurance statements.

What should Internal Audit teams think about?

With the incoming updated CIIA Code of Practice and the increasing focus on technology and technology-led audits into the overall Internal Audit Strategy, penetration tests present an excellent opportunity for an internal audit function to demonstrate a move towards more detailed and comprehensive testing. Auditing cyber controls against good practice frameworks will continue to have its place, however, integrating penetration testing into internal audit offers financial services firms a more impartial, comprehensive, and business-aligned approach to understanding and managing cybersecurity risks. Whilst this shift introduces the aforementioned challenges, the benefits derived can make it a valuable strategy for expanding assurance across the whole three line of defence model, providing insights to first line, risk functions and internal audit alike..

If you have any queries regarding the role of Internal Audit in conducting penetration tests, or would like to discuss BDO's experience in supporting IA teams on this topic, please contact:
Sandi.Dosanjh@bdo.co.uk or
Steve.Dellow@bdo.co.uk

03

Nature related financial risks

Nature related financial risks

Three practical considerations for Financial Services firms in understanding nature-related financial risks

Nature-related financial risks will increasingly affect the economy and financial systems.

Managing nature decline is urgent. It worsens climate change, leads to biodiversity loss, limits access to water, and deepens social inequality.

Gloria Perez Torres
Associate Director, FS Advisory

gloria.pereztorres@bdo.co.uk

According to the World Economic Forum, biodiversity loss is the third most impactful risk facing the global economy, and the fourth most likely to occur. These risks arise as a result of the depletion of natural resources and biodiversity, affecting the parties and economies that depend on them. Banks, asset managers, insurers and institutions providing alternative finance are exposed to physical, transitional, liability and reputational risks if they finance business that have a major negative impact on nature or are subject to the effects.

Why Financial Institutions (FIs) need to consider nature-related financial risks?

Nature-related financial risks can impact operational cash flows, asset values and the wider economy. These manifest in several ways, including:

- **Physical risks** – these arise when natural systems are compromised due to climate, a weather event or to damage to ecosystem equilibria, which is the balance within an ecosystem, where the components - such as plants, animals, microorganisms and their physical environment – interact to maintain and sustain the ecosystem itself over time [1]. For example, deforestation could reduce local rainfall, raising operating costs for numerous sectors. Nature degradation can lead to stranded assets and credit loss. On the other hand, reducing nature degradation can help prevent climate change, wildfires, protecting property values, which are collaterals, in the case of a counterparty default.
- **Transitional risks** - these relate to the process of adjustment towards a nature-positive economy. Risks arise as a result of abrupt or disorderly introduction of public policies, technological changes, shifts in consumer or investor sentiment and disruptive business model innovation. For example, anti-deforestation legislation increases due diligence costs for lenders and buyers of soft commodities that could be connected to deforestation.
- **Liability risk** – these arise if parties that suffer loss or damage from the effects of environmental change seek compensation from those they hold responsible. These losses or damages can include potential pay-outs, fines, legal and administrative costs, insurance costs, financing costs, and litigation costs. Fines for oil spills are a prominent example of liability risk.
- **Reputational risk** - these arise when a FI is perceived as a contributor to nature decline or having a negative impact leading to negative publicity, customer loss and ultimately impacting a business' financial position.

continued >

[1] Cambridge Institute for Sustainability Leadership, Handbook for Nature-related Financial Risks: Key concepts and framework for identification

Nature related financial risks

What is good practice?

Incorporating nature-related considerations into existing climate change risk management practices. Nature-related financial risk can impact business strategy, liquidity, loan books and investments. FIs should consider nature risks through identifying exposures, assessing their materiality, testing the resilience and designing risk management controls. These could include exposure due diligence and management information which will naturally run parallel with climate change risk management practices.

Larger FIs are already implementing nature-related risk management frameworks based on their conviction that this will make their business more sustainable in the longer terms and enhance growth. Smaller and medium-size FIs are at the early stages of understanding how nature-related issues affect their financial performance and market position.

There will be challenges as this is not an easy task. Many FIs are still trying to get to grips with understanding how climate change is impacting their business, let alone biodiversity. However, having a clear view on nature-related financial risks will help FI's to quantify the actual risks and opportunities associated with their impact and dependencies.

What is on the regulatory horizon?

Currently, UK regulators do not require implementation of nature-related risk management controls. In 2022 the Bank of England indicated that it would consider specific guidance or requirements on nature-related risks, if it determines that nature-related risks are material in the appropriate time horizon, and if these risks are not already being captured by ongoing climate work and by existing prudential regimes.

The ISSB published in June 2024 its 2024-2026 work plan, which includes a project to research potential disclosures around risks and opportunities associated with biodiversity, ecosystems, and ecosystem services. This could translate in the introduction of a third Standard to complement the existing S1 and S2.

On a voluntary basis, FIs are adhering to the framework published by the Taskforce for Nature-related Financial Disclosure (TNFD), the Taskforce has published guidance on how to get started and disclose around the four pillars: Governance, Strategy, Risk Management and Metrics and Targets. Early adopters will find synergies with the Taskforce for Climate Related-Financial Disclosures (TCFD) which will facilitate understanding, implementation and reporting.

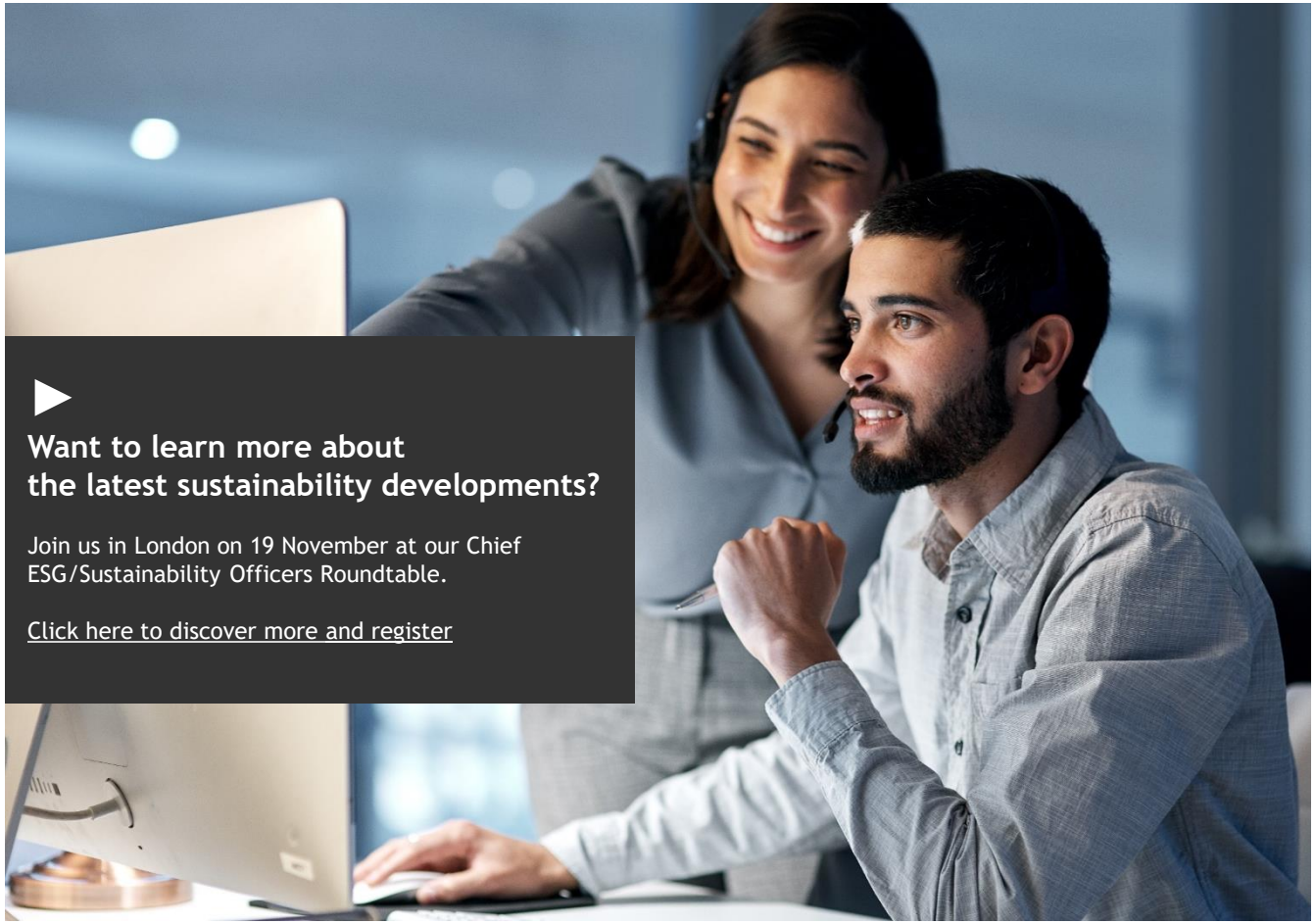
In addition, on 11 October 2024, the CFRF, a Forum established in 2019 by the FCA and the PRA published guides on how to start embedding nature risks into risk management frameworks. This shows the direction of travel for UK nature-related expectations.

What should Internal Audit teams think about?

Internal auditors will need to understand the increasing significance of nature-related financial risks and the impact these have on their business. There is potential to expand the scope of risk management reviews to include assessments of how well their organisations are identifying, managing, and mitigating risks related to nature. This includes evaluating the effectiveness of risk management frameworks, due diligence processes, and compliance with emerging regulations and voluntary guidelines like those from the TNFD. Auditors will also need to ensure that their organisations are accurately reporting on nature-related risks and opportunities, aligning with best practices and regulatory expectations where applicable. Benchmarking against industry best practices will be key, as the nature related and ESG risk landscape is ever changing, businesses need to ensure that they do not fall behind the curve of their peers. This shift will require auditors to develop new skills and knowledge in environmental risk assessment and to stay updated on evolving standards and regulations.

continued >

Nature related financial risks



Want to learn more about the latest sustainability developments?

Join us in London on 19 November at our Chief ESG/Sustainability Officers Roundtable.

Click here to discover more and register

How can we help?

BDO has expertise in sustainability and ESG-related risk management and has a team dedicated to support you. Our team are experts in financial services sustainability advisory, governance and reporting. From risk assessments to strategy development, training, programme implementation, resource augmentation and disclosures assurance, we can support you in your journey towards sustainability and resilience.

If you would like to find out more about how we can help you to incorporate nature and biodiversity risk management practices and TNFD-aligned disclosures, please contact:

Adam.Soilleux@bdo.co.uk or
Gloria.Pereztorres@bdo.co.uk

04

Appointed Representatives

Appointed Representatives

What actions should Risk and Compliance Directors be taking to assess effective oversight of Appointed Representatives?

The Financial Conduct Authority ("FCA") recently published its views on effective oversight of Appointed Representatives (ARs) and Introducer Appointed Representatives (IARs). In this article we discuss the FCA's recent publication with our insights from our Risk and Compliance Directors.

> "Principal firms must oversee their appointed representatives (ARs) effectively and are responsible for making sure their ARs comply with our rules in relation to their activities as ARs." Principal firms embedding the new rules for effective appointed representative oversight: Good practice and areas for improvement | FCA

Alison Barker
Special Adviser, FS Advisory

alison.barker@bdo.co.uk

What is the issue?

Put simply, the FCA publication concludes some effort has been made to embed requirements, but there is more to do. The FCA is holding Principals to account. Whilst ARs and IARs bring significant benefits to a business, they also pose significant risks which require mitigation and monitoring. Looked at in this way, the FCAs requirements in PS 22/11 are the basics. A culture of risk assessment and risk management should deliver a more controlled way of de-risking the benefits ARs and IARs can bring.

A recap on the background

The Appointed Representative regime has been a longstanding feature of UK financial services legislation – as far back as the original Financial Services Act 1986 for investment business. It was extended to a broader range of financial activities in the Financial Services and Markets Act 2000, including an important change allowing ARs to conduct a regulated activity independent of the principals' activities. This change in legislation has enabled some 40,000 individuals and businesses to operate in the Financial Sector without direct authorisation, which is almost equal to the number of current directly authorised firms. The requirements in PS22/11 set about clarifying expectations of principals and improving data available to the FCA to monitor risks.

A few clear themes arise from the FCA's recent review:

- Inadequate risk assessment and understanding of the AR business, both financial sector and other business, at onboarding and on an ongoing basis.
- A tick box approach to onboarding and oversight both failing to adequately cover the requirements of SUP 12.6 (Continuing obligations of firms with appointed representatives or FCA registered tied agents) and failing to adequately assess risks and information.
- Insufficient identification or monitoring of risk factors that could indicate a potential for consumer harm.
- Inadequate reporting to Boards and a lack of discussion of risks.
- Inadequate attention to contracts, such as clearly setting out the regulated activities an AR or IAR is permitted to do, and termination rights.
- Insufficient systems and controls, frameworks, reporting, MI, and documentation in place to effectively manage the AR arrangements and demonstrate action is taken when issues arise.

continued >

Appointed Representatives

Potential areas to consider

Covering all the requirements in SUP 12.6 is a good start, but understanding the inherent risks of the AR model, its role in a sector, and sufficient data about the AR population will support a more targeted and effective risk framework. Some examples are:

- AR models can be attractive to those who would not meet the FCA's standards for direct authorisation, for example individuals with poor advice records. Due-diligence should raise any issues, a strong risk appetite should guide actions to take on or reject an AR application. If taking on, additional controls and monitoring may be needed.
- Due-diligence should be thorough, for example, any evidence of prior directorships where companies have been dissolved, high numbers of complaints, or censure by any bodies should require careful assessment. ARs or IARs with overseas businesses may have higher risk profiles or may require additional effort to assess.
- Onboarding and ongoing oversight require a sufficient understanding of the ARs business (both financial sector regulated and unregulated activities, and other businesses). Good questions are what businesses does the AR operate? How does it make its money? These questions might extend to Directors of ARs and other businesses they operate. If the business is significantly larger or complex, it may present a significantly higher risk. Particularly if the principal is considerably smaller and reliant on fees from the AR. There may be other relevant regulations or regulators to consider, such as anti-money laundering regulations and ICO regulations.
- Changes to an ARs business, for example sudden growth, changes in leadership or high turnover, changes to other business activities, are all risk factors to monitor. It may trigger increased monitoring or investigation.
- Ongoing monitoring should be sufficiently regular and robust, covering a range of metrics to spot issues early. Actual testing of AR outputs such as advice, customer engagement, financial promotions, websites, or social media. Ensure consumer feedback or complaints go to the principal unfiltered.
- Relying on ARs to self-disclose, is not, as the FCA notes, sufficient as it is the principals, not the ARs duty to complete the annual assessment.
- In a three lines of defence model, onboarding, and ongoing monitoring of ARs activities should sit with the first line. A clear framework for determining risks or issues that require additional investigation, or monitoring will support clear and consistent decision making.
- A second line review may want to consider whether all elements of SUP12.6 are in place, the quality of risk identification and effectiveness of controls, and whether first line resources are sufficient (both number and competence) to conduct adequate monitoring. Monitoring is complex, those tasked with monitoring should be able to assess a broad range of information and make judgements about financial stability, business activities and potential for consumer harm.
- Governance, reporting and MI should be clear with active engagement of the Board. Evidencing active discussions and actions taken is an important discipline in demonstrating strong governance.
- Requirements for Introducer Appointed Representatives are less onerous, reflecting their more limited role. However, the risk assessment, onboarding and ongoing monitoring points are no less relevant. Principals of IARs should be equally diligent in their onboarding assessments of IARs and have sufficient resources to monitor IARs. A thorough risk assessment should determine if higher levels of monitoring are needed.

What should Internal Audit teams think about?

The FCA's recent guidelines on the oversight of Appointed Representatives (ARs) and Introducer Appointed Representatives (IARs) mean that internal auditors must ensure their organisations comply with these requirements and manage associated risks effectively. This involves internal audit performing an assessment of a firm's risk assessments due diligence, onboarding and ongoing oversight processes. Auditors should verify that monitoring mechanisms are in place, including actual testing of AR outputs and ensuring consumer feedback is directed to the Principal unfiltered. In addition, confirmation should also be sought that firms have sufficient resources and competent personnel to monitor ARs and IARs effectively, ensuring financial stability and minimising consumer harm.

If you require support or would like to discuss with any of these topics, please contact:
Richard.Barnwell@bdo.co.uk or
Nicola.Ball@bdo.co.uk

05

Corporate Governance

Corporate Governance

Addressing concerns about impending UK Corporate Governance Code changes readiness

A recent BDO survey revealed that 1 in 3 NEDs are concerned that the businesses that they represent are not sufficiently prepared for the impending changes to the UK Corporate Governance Code (the "Code"). This is a significant finding given the heightened scrutiny around corporate governance. The revised Code, aimed at enhancing transparency, accountability, and sustainability, requires businesses to act now to ensure they are not caught off guard when these regulations come into effect.

Alex Traill
Director, Digital Risk Advisory

alex.traill@bdo.co.uk

For many businesses, these concerns reflect gaps in preparedness, governance frameworks, and strategic alignment with regulatory expectations. The challenge ahead is not only compliance but leveraging governance as a driver for long-term value creation. We set out below the suggested next steps for firms to do this.

Board training and education

One of the primary reasons for the unpreparedness highlighted in the survey is a lack of awareness and understanding of the changes. The revised Code emphasises broader aspects of Environmental, Social, and Governance (ESG) factors and the role of corporate culture. There is also a new requirement for Boards to issue an annual declaration over the effectiveness of material internal controls across financial, reporting, operational and compliance aspects of the business. Many boards are not fully abreast of the requirements set out by the Code and as a result are not well positioned to oversee and drive the required transformation in the business.

Conduct a governance gap analysis

Businesses may consider conducting a governance gap analysis to identify where current practices fall short in meeting the upcoming requirements. This analysis should focus on several key areas: risk oversight, reporting obligations, board diversity, and executive remuneration policies. Given that many of the changes to the Code involve more stringent requirements around accountability, transparency, and risk management, understanding where these gaps exist is a critical first step in developing an actionable plan.

It's essential that this gap analysis is not simply a compliance exercise. Rather, it should be an opportunity for boards to reflect on how their governance structures support the company's long-term resilience and reputation.

Enhance risk management and ESG reporting

The revised Code places heightened importance on Environmental, Social, and Governance (ESG) factors. Companies should review their risk management processes and ensure they integrate ESG risks into their wider risk frameworks. It is no longer sufficient to treat ESG issues as a side concern; they need to be at the core of decision-making and strategy.

Businesses must also refine their ESG reporting processes, ensuring that disclosures meet investor and stakeholder expectations around transparency and sustainability. Strengthening these reporting frameworks will not only help businesses comply with the Code but also build trust with stakeholders who are increasingly scrutinizing corporate social responsibility.

Improve board composition and diversity

Another critical area under the new Code is Board composition. The focus on diversity and inclusion means companies should take steps to review and enhance the diversity of their boards in terms of gender, ethnicity, skills, and experience. A diverse board is more likely to foster innovation, challenge the norm, and bring fresh perspectives on governance challenges.

continued >

Corporate Governance

Strengthen stakeholder engagement

The revised UK Corporate Governance Code emphasises greater engagement with stakeholders, including shareholders, employees, suppliers, and communities. Businesses should proactively enhance their communication strategies and ensure that all stakeholders understand how the company is adapting to these changes. Effective stakeholder engagement builds trust and helps companies navigate periods of regulatory or operational change with more support and less friction.

Conclusion

The impending changes to the UK Corporate Governance Code are an opportunity for companies to not only comply with regulations but also strengthen their long-term value creation strategies. For the 1 in 3 NEDs who are concerned about their business's preparedness, the time to act is now. By prioritising board training, conducting a governance gap analysis, enhancing risk management, and improving board diversity, businesses can ensure they are ready to meet these new challenges head-on, safeguarding their reputation and future growth.

For more insights around key areas of focus for NEDs, take a look at BDO UK LLP's latest report, co-authored by Shrenik Parekh, CFA.

What should Internal Audit teams think about?

Internal audit functions should focus on several key areas to ensure businesses are prepared for the impending changes to the UK Corporate Governance Code. Firstly, they need to assess the adequacy of board training and education programmes. This includes reviewing the content, frequency, and effectiveness of training sessions, particularly those covering ESG factors and the role of corporate culture. Internal audit should also consider conducting a comprehensive governance gap analysis to identify areas where current practices fall short of the new requirements and supporting business with facilitation of their change programmes to ensure that any identified gaps are closed.

Additionally, internal audit functions should evaluate the integration of ESG risks into the wider risk management framework. This involves assessing the processes for identifying, managing, and reporting ESG risks, ensuring these issues are central to decision-making and strategy. In addition, consideration should be made to the diversity of the board in terms of gender, ethnicity, skills, and experience, examining recruitment processes and diversity targets. Finally, internal audit should evaluate the effectiveness of stakeholder engagement strategies, including communication strategies and feedback mechanisms, to ensure stakeholder concerns are addressed in governance practices.

▶ Are you grappling with "Material Controls"?

"Material Controls" in the context of Provision 29 of the new Corporate Governance Code, is a key consideration for many Boards, Audit Committees and Senior Management.

In November and December, we are running three in-person workshops, providing an opportunity to discuss with peers how they are approaching this challenge.

London - Tuesday 05 November
▶ Find out more and register

Birmingham - Tuesday 26 November
▶ Find out more and register

Manchester - Tuesday 03 December
▶ Find out more and register

If you require support or would like to discuss with any of these topics, please contact:
Alex.Traill@bdo.co.uk or
Shrenik.Parekh@bdo.co.uk

FOR MORE INFORMATION:

Paul Gilbert
Partner

+44 (0)7890 323 336
paul.gilbert@bdo.co.uk

Bruk Woldegabreil
Director

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

www.bdo.co.uk

XXXXXXX